Energy Security in the Digital Age and Its Geopolitical Implications for Asia

Frank Umbach

The worldwide energy sector stands at the crossroads, coping with unprecedented changes and challenges: increasing deployment of renewable energy resources (RES), rising energy demand, greater energy efficiency, disinvestment in carbon-intensive industries and the US shale oil and gas revolution (together with the rapidly expanding worldwide liquefied natural gas (LNG) trade) have far-reaching impacts on the global oil and gas markets. Furthermore, digitalisation, new forms of mobility, and new consumption patterns, providers and platforms are changing established industries. The "energy transition" affects in particular the global electricity sector, which is being transformed by the reinforcing strategic trends of the "3 Ds": decarbonisation, digitalisation and decentralisation. Furthermore, electrification and digitalisation of the transport and heating sectors as well as the forthcoming "industry 4.0"-revolution, based on robotics and Artificial Intelligence (AI) systems, might result in a much higher electricity demand than currently projected. This will increase the role of electricity in final energy consumption significantly. These megatrends will affect not only the industries but also the daily life of citizens and public order as it will become ever more dependent on the stable functioning of critical (energy) infrastructures.

Increasing internet interconnectivity and a vast amount of sensitive data, as well as asymmetric conflict patterns in international relations, have dramatically amplified the risks and vulnerability of national and global energy infrastructures in

[*] This article is a short version of Frank Umbach's study "Energy Security in a Digitalised World and its Geostrategic Implications", published by KAS Regional Project Energy Security and Climate Change Asia-Pacific (RECAP)/Hong Kong. To access the study, please visit https://www.kas.de/web/recap/single-title/-/content/energy-security-in-a-digitalised-world-and-its-geostrategic-implications.

terms of sophisticated cyberattacks on services.[1] Those threats can even multiply with the next wave of digitalisation in the energy sector (especially electricity generation and distribution), the further global expansion of RES and the electrification of the transport (e.g., rapid expansion of electric vehicles) and heating sectors. It is not least due to this development of unprecedented changes, opportunities and risks that the International Energy Agency (IEA) stated in 2017,

> Every unit of the IEA – from efficiency to investment, from electricity to transportation, from renewables to modelling, from sustainability to statistics – is examining the implications of digitalisation on the energy sector. [...] The interest in this topic is strong, but the world's current understanding of the scale and scope of its potential remains limited, particularly when it comes to analytically-rigorous assessments.[2]

New (disruptive) technologies for digitalisation, AI, clouds, robotics, and industry 4.0 are even more welcomed in Asia as they promise to improve the daily lives of citizens and offer new economic perspectives for enhancing living standards and productivity.[3] Together with a growing population in ASEAN and South Asia, these technologies transform Asia into the most dynamic region in the world. Asian states and governments demonstrate in their supported programmes (e.g., Singapore's "Smart Nation Initiative" or Japan's "Society 5.0") their political will to use and adopt those new technologies which will decisively shape the worldwide digital transformation. Up to now, those programmes are developed for their entire economy and society, but do not appear to be very detailed with regard to energy transformation and future energy security.

Against the background of these dramatic forthcoming changes, at least four geopolitical implications of the digitalisation of the energy sector – alongside the other already impacting strategic energy developments – can be identified on the global and regional levels:

---

[1] See F. Umbach, "Critical Energy Infrastructure and Risk of Cyber Attack", in KAS-International Reports, September 2012, pp. 35-66; idem, "Cyber Security – Dossier", Geopolitical Information Service (GIS - www.geopolitical-info.com), August 2013; idem, "The Fog of Cybersecurity", Geopolitical Intelligence Service (GIS), 10 July 2017.

[2] See IEA, https://www.iea.org/newsroom/news/2017/april/iea-examines-critical-interplay-between-digital-and-energy-systems.html, accessed 18 January 2018.

[3] To AI see Richard Waters, "Why We Are in Dangers of Overestimating AI", FT, 5 February 2018; "Limiting the Downsides of Artificial Intelligence", FT, 22 February 2018; Rana Foroohar, "How We Can Protect Workers from AI? FT Readers Respond", FT, 21 February 2018; "The Global Policy Response to AI", FTI Consulting Inc., February 2018.

(1) A further rising electricity demand, which has already been forecasted to grow much faster than the overall primary energy demand on national, regional and global levels. While the digitalisation might also promise new energy efficiency gains and energy conservation, many newly introduced and identified new technologies have proved to be very energy intensive and might lead to even higher electricity demand.

(2) Electricity supply, alongside expanding volatile renewables and advancements of battery storage technologies, becomes ever more important for future energy supply security. Advancing technologies for battery storage may cause one of the most disruptive changes and is a major game changer in the power and renewable industries.

(3) With smart meters and smart grids, the electrification of the transport and heating sectors, the internet of things (and applications) and critical (energy) infrastructures (CEIs), the energy sector becomes more vulnerable towards sophisticated cyber-attacks and blackmail attempts to disrupt a stable supply of electricity and sensitive communication flows.

(4) Renewables are often considered as indigenous energy resources, which – in contrast to fossil fuels – do not need to be imported from other producing countries, often being politically unstable. The myth suggests that renewables do not cause any inherent risks and vulnerabilities, but rather decrease import dependencies on politically unstable producers and, thereby, increases supply security. However, renewables, batteries and other "green technologies", including further digitalisation, AI systems and robotics, need many CRMs (i.e., rare earth, lithium, cobalt, platinum and others). Their production is often concentrated in few countries (e.g., China has a 90% production and export monopoly of rare earth) and huge mining companies. A stable supply and rise of global demand may have wide ranging geo-economic and geopolitical implications – particularly when future economic and military superpowers such as China will have the combined capability of being one of the future technology and R&D leaders of AI having available the much-needed CRMs as well as the production capabilities to dominate the worldwide demand and value chains of their supply.

Hence, non-energy resource security will become a major dimension in global energy security in the future. These challenges not only require a comprehensive discussion of national energy systems[4] but also more multilateral cooperation on re-

[4] See Francois Austin, "How to Solve the Energy 'Trilemma'", 27 November 2017, https://www.greenbiz.com/article/how-solve-energy-trilemma, accessed 30 January 2018.

gional and global levels to avoid new antagonistic conflict patterns and geopolitical rivalries.

Instead of analysing these four dimensions in more detail, I will explore and discuss digitalisation in the worldwide energy sector, which is offering both new economic and business opportunities, but also new risks and vulnerabilities on national, regional and global levels. In this context, I will also address some wider strategic implications for Asia.

UNDERSTANDING DIGITALISATION IN THE INTERNATIONAL ENERGY SECTOR

The energy sector has always been at the forefront of adapting technological innovations. Oil and gas companies already operate some of the world's most powerful supercomputers. The new US shale revolution 2.0 includes cloud computing services, which store and analyse an unprecedented amount of data on seismic information, drilling and production much more precisely. Digitalisation and automation, as well as new alliances between oil and IT companies, will make future operations of oil and gas drilling even safer, cleaner, and more efficient. Moreover, the industry is already coupling AI with new advanced sensors, sophisticated seismic data processes and management as well as automated drilling rigs to maximize production of tight oil and shale gas with only a few engineers and technicians.

Power utilities have proved to be "digital pioneers" since the 1970s by using technologies to improve grid management and operations, while oil and gas companies used digital technologies for modelling exploration and production assets. Today, the increasingly fast pace of digitalisation with the widespread use of "Information and Communication Technology" is changing the established energy sector and the traditional energy business models by creating new consumption patterns, providers and platforms (also from outside of the energy sector).

Digitalisation and other technology developments allow better decentralisation and distribution of renewable energies, and enable their linkages with smart grids (i.e., "microgrids") and smart metering technologies ("smart meter data hubs") as well as new battery storage solutions. Therefore, German utilities, for example, are striving to become consumer-centred and service-based organisations, but their actual market share in the digitalised retail market is still very small. New business models need to be developed to address the "3 Ds". For those energy utilities, the major challenge is not just the digitalisation itself, but the interlinkages with the other two "Ds" and its impacts on the markets, including the smart home market, and implications for their future business models and business development strategies.

Furthermore, expanded robotics and AI promise that half of the activities (not jobs) traditionally carried out by workers can be automated.[5] "Deep learning systems" are using artificial neural networks and real-time data to predict demand trends on a hyper-regional basis.[6]

Figure 1: Recent and Forthcoming Changes in the Global Energy Sector.

Energy market changes and impacts

Recent changes in global energy markets	*Forthcoming changes due to:*	*Impacts*
• Expansion of renewables • Energy efficiency technologies and strategies • Decarbonization/disinvestment in fossil fuels • U.S. shale oil and gas revolution • LNG revolution • Rising cyberattacks on critical energy infrastructures • Decreasing public acceptance of energy infrastructure investments (i.e. in fossil fuels)	• Electrification of the transport and heating sectors • Digitalization – Energy utilities and electricity/power sectors (smart grids, smart metering, internet of things/smart home etc.) – Fossil fuel production • Blockchain technology • Decentralization • Battery storage solutions • Quickening decarbonization	• Energy prices and competition between fossil fuels and renewables • Additional rise of worldwide and European electricity demand (already growing much faster than global primary energy consumption) • Increasing need for battery or other storage solutions • Rising cyber risks and vulnerabilities of critical energy infrastructures due to internet linkages and digitalization • Socioeconomic and political stability of oil and gas producers • Risks and vulnerabilities of the rising critical raw material demand for supply security

Source: Dr. Frank Umbach

GIS GEOPOLITICAL INTELLIGENCE SERVICES www.GISreportsonline.com

Source: Dr. F. Umbach/GIS, 2018.

Digitalisation and electrification have also led to rising competition among energy companies which face at the same time new competitors from outside (e.g., IT companies). This is even true for the oil and gas companies, which have created strategic alliances and partnerships with IT companies. Renewables, as well as energy storage solutions, have become much cheaper and competitive. This also offers oil and gas companies new options to diversify their energy sources and businesses and has led to a new class of hybrid energy enterprises, reconciling fossil fuels with renewables. In Europe, Royal Dutch Shell and Total have also begun to invest in further expansion into the electricity supply chain and building a retail energy business in Europe for an integrated power supply chain from generation to retail supply, challenging traditional power companies. But the barriers and challenges to implementing the full spectrum of new digital technologies – ranging

[5] See also Patrick McGee, "Auto Bosses Accused of Failing to Train Workers for AI Revolution", FT, 17 June 2018.

[6] See also Richard Waters, "'Deep Learning' - the Hot Topic in AI", FT, 14 May 2018.

from adequate timing of capital-intensive large projects, the existing infrastructures, risk-averse management perspectives toward introduction of new disruptive technologies, high fragmentation along the supply chains, and long-term demand trends, to dependence on a up-to-date information technology support infrastructure – might slow their fast implementation and full exploitation of the new disruptive technologies.

The electricity sector is expected to undergo the greatest digital transformation as it will break down the traditional boundaries between various energy sectors, increase flexibility, blur the distinction between generation and consumption as well as increase the rate of integration across entire systems. Since 2014, global investments in digital (electricity) infrastructure and software have jumped by 20% per year up to US$47bn in 2016. Around 90% of the world's data have been created in just over the past two years! While the digitalisation is at first glance primarily a technology revolution, its impacts for companies and governments will change markets, business models, organisational structures and companies' cultures substantially in the forthcoming years. The potential savings in costs and investments in the worldwide power sector due to digitalisation by reducing operation and maintenance costs, improving the efficiency of the power plants and networks, decreasing unplanned outages and downtime, and extending operational lifetimes of assets has been estimated at around US$80bn between 2016 and 2040. The current electricity model is increasingly being disrupted and undergoing major change. Even fundamentals are increasingly questioned: (1) electricity prices are always based on usage-based prices (i.e., negative electricity prices); (2) only energy companies will generate and sell electricity; (3) all private and industrial customers need an electricity and wider grid connection as well as a regional system operator; and (4) local distribution companies will necessarily function as a stable and profitable source of funds to local governments owning them. All these traditional assumptions will change in the forthcoming years.

In consequence, the whole electricity industry needs to adopt radical changes in its business models. Many won't survive and/or be able to compete in fundamentally different future markets. The greatest potential for the digitalisation in the energy sector might be the elimination of traditional segmentation and boundaries between various energy sectors as well as with other sectors and industries. They will enforce the integration of entire systems and the creation of new ones. In this context, connectivity becomes the most important driver factor for the digitalisation of the industrial and electricity sectors.

GEOPOLITICAL DIMENSIONS

In contrast to the years before 2010, the world is no longer confronted with any scarcity of fossil fuels, which had sparked debates of a near "peak oil"-era with ever increasing fossil fuel prices. Instead, the present world has now to cope with fossil fuel oversupplies and rapidly decreasing fossil fuel prices, which have changed the overall geo-economic and geopolitical balance of power between consumer and producer countries, leading to new "buyers' markets".

Traditionally, geopolitical risks and vulnerabilities due to supply disruptions have been considered as exclusively linked with fossil fuels as renewables are immaterial and available almost everywhere ("no one can ever embargo the sun"). Their expansion has also promoted the overall decentralisation of energy supplies – widely perceived as enhancing energy security. They may not just reduce the dependence on politically unstable fossil fuel suppliers (both state and corporate), but also their political and geo-economic power in international relations. The loss of their previous geo-economic and geopolitical influence translates into the emergence of global "buyers' markets" instead of the traditional "sellers' markets". The creation of "prosumers" (energy consumers becoming simultaneously energy/electricity producers) and the redistribution of economic as well as political power offers new participation, investment and strategic influence to new centralised powers (e.g., internet giants such as Facebook, Amazon, Netflix, Google and others, which become either energy producers themselves or are digital technology partners of energy companies) as well as to new players on the local level as a result of the decentralised energy supplies. According to this logic, expanding RES and "energy abundance" will "depoliticise markets" by decreasing the traditional geopolitical risks of supply disruptions and, therewith, enhancing national, regional and global energy supply security in our traditional understanding and defined concepts.

While traditional supply risks such as supply disruptions due to political instabilities in producer countries or attempts at political blackmail (i.e., Russia) indeed will decrease and be marginalised in the mid- and long-term future, new geopolitical risks and vulnerabilities will arise with the expansion of renewables and the rapid introduction of new disruptive technologies (including smart meters, smart and super- as well as micro-grids etc.) in the context of digitalisation, electrification of the transport and heating sectors, robotics and Artificial Intelligence systems. Up to now, supporters of RES have hoped that power generation will become more dispersed and decentralised, while regions may become more self-sufficient in energy supply, triggering a process of "energy democratisation", in contrast to the traditional centralised energy systems. Enhanced energy access via mini-grids and rooftop solar panels in Africa, South and Southeast Asia as well as other regions has offered new energy options for reducing "energy poverty" alongside the further growth of the global population. But the changing energy systems, from the traditional one, coping with scarcity challenges, to abundant RES, will inevitably produce losers such as the currently leading oil and gas producer superpowers in the mid- and long-term future.

It is indeed true that a more diversified energy mix increases energy supply security and renewables decrease those traditional geopolitical risks of supply disruptions. But it has largely been overlooked that the expansion of renewables also creates new geopolitical dependencies, risks and vulnerabilities.[7] The worldwide electrification of the transport and other industry sectors, the development of a new generation of batteries for electricity storage as well as the digitalisation of the industries, including the spread of robotics and Artificial Intelligence systems in the industry ("industry 4.0") will further boost the worldwide demand for CRMs such as lithium, cobalt, rare earths and others.[8] As a result, this might create new, unprecedented challenges, including bottlenecks and supply shortages, for the global supply chains of the CRMs at each stage, ranging from mining to processing, refining and manufacturing. The challenge again is not so much physical scarcity of those materials, but rather timely sufficient investments and their concentration in production in even fewer producer countries as well as companies. Compared with the conventional oil and gas resources, the production of CRMs is geopolitically even more challenging and problematic – particularly when the future rise of the global demand is taken into consideration.

The production of CRMs is geopolitically – compared with the concentration of conventional oil and gas resources – more challenging and problematic as currently 50% of CRMs are located in fragile states or politically unstable regions. Moreover, security of supply risks are not just confined to primary natural resources and CRMs but also include the import of semi-manufactured and refined goods as well as finished products. Manipulated prices, restricted supplies and attempts at

[7] See also Megan O'Sullivan, Indra Overland, and David Sandalow, "The Geopolitics of Renewable Energy", Columbia/SIPA, Belfer Center/Harvard and Norwegian Institute of International Affairs (NPI) 2017; Daniel Scholten, "Renewable Energy Security", EUCERS-Newsletter, Issue 64, April 2017, pp. 2-4; Daniel Scholten and Rick Bosman, "The Geopolitics of Renewables: Exploring the Political Implications of Renewable Energy Systems", Technological Forecasting & Social change, 103/2016, pp. 273-283; Meghan L. O'Sullivan, "Renewables Won't End Geopolitics of Energy", Japan Times, 24 August 2017, and Ian Morris, "Imagining a World after Fossil Fuels", Stratfor, 22 March 2017.

[8] See also Walt Patterson, "How Renewables Will Change the Geopolitical Map of the World", www.energypost.eu, 9 February 2018.

cartelisation of CRM markets with wide-ranging negative economic consequences are not just restricted to producing and exporting countries. Powerful state and private companies have also been responsible for non-transparent pricing mechanisms for many precious CRMs. Global supply chains have become ever more complex with blurred boundaries between physical and financial markets and weakly governed market platforms. These market imperfections lead to the manipulation of prices, thus threatening the stability of the future security of supply of CRMs.

Given China's strategic interest to become the world's largest battery producer and market for electric mobility as well as the worldwide interest (i.e. South Korea, Japan, the EU's and U.S.) in new industrial battery storage options, the dependence on CRMs such as lithium, cobalt, graphite, rare earth and others will equally rise. Those geopolitical impacts have already been highlighted during 2010–2011 when China, in the midst of an escalating diplomatic conflict with Japan, stopped all exports of Rare Earth Elements (REEs) to the world's biggest importer and blackmailed Tokyo diplomatically by instrumentalising its status as the world's largest producer and exporter of REEs. It sent a troubling message to the world that the new rising Asian economic and military power might not respect international law or the existing global rules of the WTO and cast doubt on the political willingness of Beijing to accept the regional and global responsibilities that go with its emerging superpower status. During the last months, China has further strengthened its efforts to control the entire global supply chain of lithium, from owning international mines to production, up to manufacturing of batteries and electric vehicles (EVs).

The future CRM supply security depends largely on timely investments, and alternative strategies such as (1) the re-use of CRMs; (2) reduced use; (3) substitution; and (4) recycling. Using these strategies would allow reducing the imports of CRMs from a long-term perspective. These options need also to be an integral part of the development of "circular economies" as a response strategy, by using CRMs more economically, efficiently and environmentally, thereby reducing their mining demand in order to strengthen their security of supply.

The present energy transition[9] and the digitalisation have fuelled a global race for the best and most disruptive technologies and competition in access to as well as strategic control of critical raw materials, such as rare earth, lithium, cobalt and others. These strategic developments have wider geo-economic and geopolitical impacts and may transform international energy relations between countries and

[9] Quoted following Quinn Connelly, "Energy Transitions? Not so Fast", RealClear Energy, 18 April 2018.

regions. The heightened competition for global technology-industrial leadership has already led to a growing technology race between the US and China, which is shaping the present and will determine future geopolitical competition between the two superpowers of the 21st century.[10] Those technology transformations could also lead to a new "securitisation" of raw materials alongside the monopolisation of political *and* economic power, strengthening the autocratisation of political systems inside countries as well as internationally.[11] In this context, China's worldviews and geopolitical strategies – such as the "Belt and Road-Initiative" (BRI), formerly known as "One Belt One Road" Strategy (OBOR) – and its nationalist tendencies in its domestic policies under President Xi Jinping are of utmost strategic importance for the West and global stability.

CYBER SECURITY REQUIREMENTS

The expansion of renewables is linked with other disruptive technologies (such as smart meters, smart grids, batteries and other new storage options), the further digitalisation of the energy sector, the electrification of the transport and heating sectors as well as robotics and Artificial Intelligence. As the future energy sector in general and the electricity generation, supply and distribution networks in particular will be linked to the internet, cyber security challenges in the energy sector will dramatically increase the risks of national or transnational electricity blackouts, threatening the overall functioning of all critical infrastructures, as they are dependent on a stable electricity supply and a functioning access to a reliable Internet.

Given this internet interconnectivity of the energy and other industrial sectors, the existence of a vast amount of sensitive data and asymmetric conflict patterns have dramatically increased the risks and vulnerability of "Critical Energy Infrastructures (CEIs)" to sophisticated cyberattacks by national hacker groups, transnational crime organisations and state-supported secret services.

In recent years critical infrastructures have increasingly been the target of cyberattacks. In 2009, viruses were discovered in the US electricity grid that

---

10 See also Richard B. Freeman and Wei Huang, "China's 'Great Leap Forward' in Science and Engineering", NBER Working Paper, No. 21081, 2015; "The Tech Giants Growing Behind China's Great Firewall", Stratfor.com, 6 February 2018, and Kai-Fu Lee; Paul Trioto, "China's Artificial Intelligence Revolution. Understanding Beijing's Structural Advantages", Eurasia Group, Sinovation Ventures, 2017 and "The Coming War Tech War with China", Stratfor.com, 6 February 2018.

11 See also Peter Hefele, "Of Streams of Data, Thought, and other Things", KAS-International Report 1/2018, pp. 56-63 (58).

supposedly originated from China and Russia. It could have made the US a victim of blackmail if relations between the two countries had soured. While the knowledge of creating computer viruses is expanding exponentially, many industrial computer systems that control power plants (via Supervisory Control and Data Acquisition/SCADA-systems) as well as other CEIs are often old and outdated even in Western countries, making them very vulnerable to cyberattacks.

As all critical infrastructures (CIs) are dependent and directly or indirectly connected to the regular internet, and dependent on a stable supply of electricity, the energy and in particular electricity sectors of highly industrialised countries may be considered as the Achilles heel of their political, social and economic stability.

Digitalisation of the electricity sector is also linked with the digitalisation of the building sector and "smart home" technologies such as smart thermostats, smart lighting and various IoT-devices. By 2020, more than 20 billion connected IoT-devices, and nearly 6 billion smartphones are expected to be online. By 2040, 1 billion households and 11 billion smart appliances could be an active part of a highly interconnected electricity system. Their "smart demand response" has been estimated to provide 185 GW of inherent flexibility to the system (the presently installed electricity supply capacity of Italy and Australia combined). It could save up to US$270 bn of investment in new electricity supply infrastructure needed to ensure energy supply security. The roll-out of "smart charging" of electric vehicles, shifting the charging to off-peak times, could save another US$100-280 bn by avoiding the need to build new electricity infrastructure by 2040.

But the widespread introduction and use of digital technologies and devices, as well as their benefits, are dependent on overcoming the manifold challenges in regard to technical and economic considerations (cost-benefit calculations of private consumers and industry), safety and security risks (against cyberattacks) and concerns regarding private data security and timely as well as adequate political guidelines (introducing new regulations and defining new standards). Critical questions about how much information people are willing to share with electricity and internet service providers, how private and commercial confidentiality can be best protected, and who owns, collects and uses consumer-specific data (including for prosumers), including for third parties, need to be answered. A new regime of close and trust-infused collaboration in the form of public-private partnerships (PPP), involving the energy and internet industry as well as governments in institutionalised PPP discussions, has yet to be created.

STRATEGIC PERSPECTIVES

The geo-economic and geopolitical megatrends outlined above are impacted by the global ascendancy of a rising number of autocratic states with a (combined) unprecedented economic power and the political will to use their economic-financial soft power to divide and weaken Western democracies. The share of “not free” and “partially free” countries in global income has grown from 12% to 33% nowadays – a level not seen since the early 1930s and the rise of fascism in Europe.[12]

China, for instance, has proclaimed a “digital silk road” and announced investments in overseas fibre-optic cables, telecommunication and internet infrastructures, data and cloud computing services, global positioning, wireless communications, and smart city sensors, all of which have attracted Asia’s and worldwide attention, but also increasing concerns. The potential insertion of backdoor viruses and mechanisms could increase China’s industrial and political espionage, intelligence and propaganda missions in BRI partner countries. Beijing is suspected of being willing to export its worldwide unrivalled internet censorship and its comprehensive political control of data collection and traffic with its “Belt and Road Initiative”. It raises basic questions in regard to human rights by undermining personal freedom, privacy as well as anonymity as granted by liberalised Western democracies and their constitutions.[13]

For Asia’s energy sector and other industrial sectors, digitalisation offers new perspectives for enhancing energy efficiency, expanding renewables with new storage options, boosting productivity and decreasing the costs of production as well as business operations. New risks are primarily perceived with cyber security, but – with the exception of Japan and South Korea – not so much in regard to the supply security of CRMs. In Southeast Asia, Singapore has been at the forefront as a “smart city state” in addressing various cyber security challenges nationally and enhancing cyber security cooperation as well as coordination within ASEAN. The initiated project of a Japan-ASEAN Cyber Centre not only serves the enhancement of resilience of cyber security on both sides, but also growing interregional cooperation and new global governance initiatives for international standards and norms. But perceived state-supported “offensive cyber operations” have, not only in the US but also in Asian countries, caused increasing cyber security concerns. The “Five Eyes”

[12] See also Yascha Mounk and Roberto Stefan Foa, “The End of the Democratic Century”, Foreign Affairs, 16 April 2018, here p. 2.

[13] See also Stewart M. Patrick, “Belt and Router: China Arms for Tighter Internet Control with Digital Silk Road”, Council of Foreign Relations, 2 July 2018 and Kenny Liew, “Belt & Road Bolsters China’s Technological Clout”, CSIS-Reconnecting Asia Project, 24 September 2018.

intelligence alliance between Australia, Canada, New Zealand, the UK and the US has not only deepened security consultation and coordination to combat perceived Chinese and Russian cyber threats and investments, but the member countries are also willing to share their intelligence with European partners such as France and Germany as well as Japan and other countries in the future. The real challenge in regard to the future global governance of the internet and digitalisation between Western countries and China (and Russia) is clearly linked with their respective different political systems as China's understanding of "cyber sovereignty", for instance, makes the global internet a battlefield for domestic political stability (i.e., control of the world's largest online population) and wider-defined national security interests inside and outside the country.

Although not all implications for and impacts on the worldwide, regional and national energy sectors can already be identified and analysed in regard to digitalisation challenges in detail or are even fully understood, it has already become clear that those unprecedented technological changes in the worldwide energy sectors will also have wide-ranging geo-economic and geopolitical implications. Many geopolitical implications are still being overlooked as current discussions concerning digitalisation alongside the other developments still centre on the economic changes, the management of the perceived short-term challenges of the energy transition to a non-fossil fuel age and the risks for traditional business models and strategies as well as company cultures rather than on the long-term implications for the worldwide energy and raw material supply security as well as on an adequate global governance system for it.

Dr. phil. Frank Umbach is Research Director at the European Centre for Energy and Resource Security (EUCERS), King's College, London (www.eucers.eu); Executive Advisor, ProventisPartners, Munich (M&A; proventis.com); Adjunct Senior Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyan Technological University (NTU), Singapore (www.rsis.edu.sg), and Visiting Profssor at the EU-College at Natolin (Warsaw) on EU energy (foreign) policies (https://www.coleurope.eu/about-college/welcome-natolin). He has also done various consultancy projects on behalf of European and Asian governments/ministries, international organisations (i.e. NATO and EU), the international energy industry and consultancy companies on international energy security, geopolitical risks, cyber security and critical (energy) infrastructure protection/CEIP, as well as (maritime) security policies in Asia-Pacific. He was also Co-Chair of the European Committee at CSCAP (2002-2007); Dr. Umbach is the author of more than 500 publications in more than 30 countries worldwide; contract author of the *Geopolitical Intelligence Service (GIS)*, Liechtenstein since 2011, and Co-Editor of the (monthly intelligence reports on) *Energy and Geopolitics (E&G)*, Berlin.