EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

EUROPE'S DIGITAL POWER:
FROM GEO-ECONOMICS TO CYBERSECURITY

Conference Report

By Stefan Soesanto

EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

EUROPE'S DIGITAL POWER: FROM GEO-ECONOMICS TO CYBERSECURITY

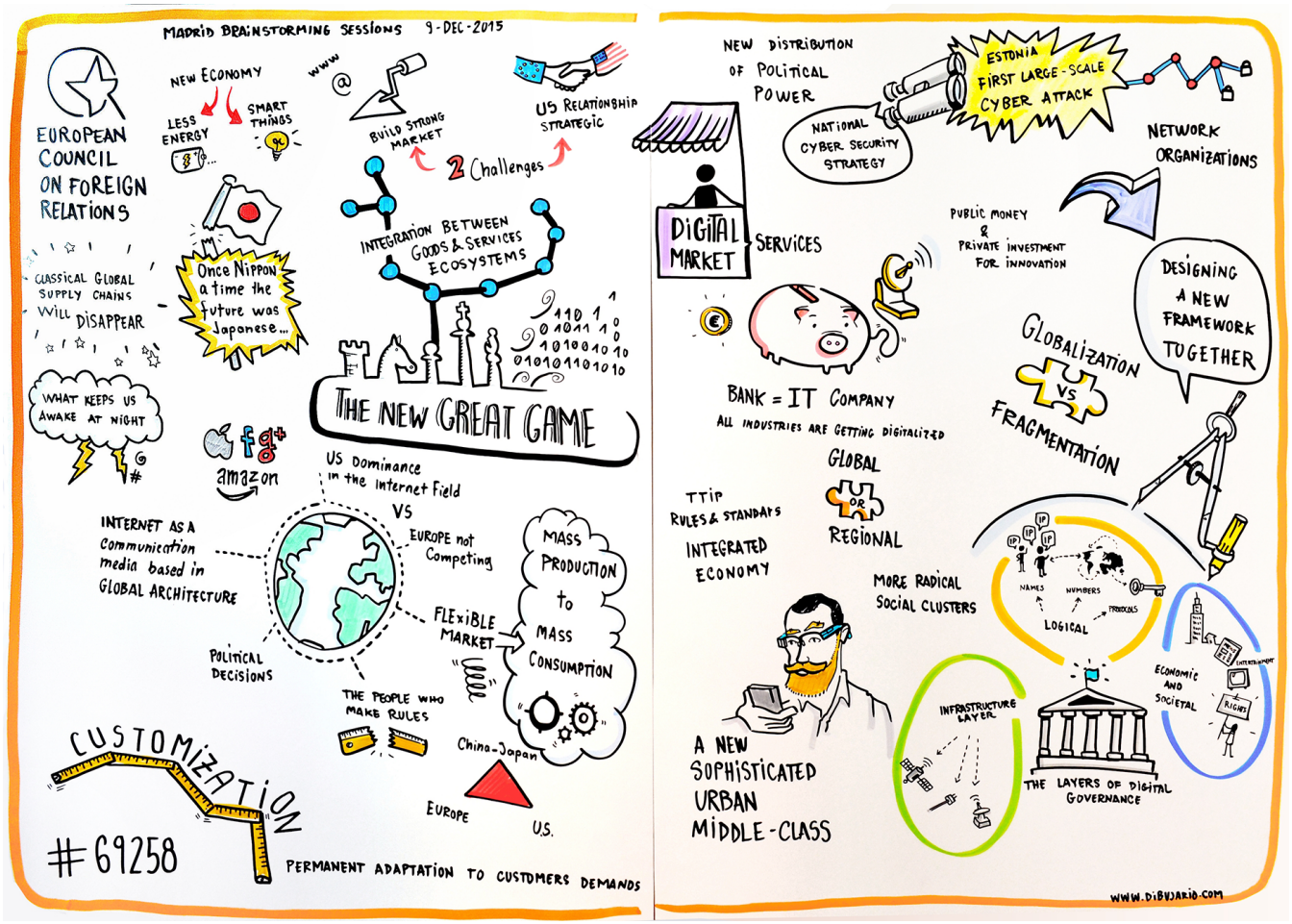
Summary

The digital space is highly contested, with many competing strands and areas of activity. In the EU and among member states there is, as yet, no clear approach to how to govern this space, let alone to how to wield power therein. This paper puts forward an understanding of digital power which rests on, first, the strength of the digital economy and, second, cyber capability.

It is clear from the workshop debates carried out as part of the Europe's Digital Power project that there is no consensus about the definition of digital power as a concept, nor any agreement on whether it should be applied to current debates in the digital sphere. Some workshop participants were adamant that the concept does not even merit further exploration.

Nevertheless, it is still the case that creating strong digital economies and strengthening cyber capability each remain important concerns for key stakeholders, and that across the European economy many growth opportunities remain to be seized. Queries over whether the emergence of 'digital champions' would genuinely increase Europe's digital power are valid; participants insisted that power and influence would not necessarily accrue to states but would, at least, be dispersed among companies and other state actors.

Whatever the precision of definitions, Europe's faltering progress towards the completion of the digital single market and its sluggish response to cyber threats are unfortunately suggestive of a reluctance to get fully to grips with digital as a medium. 'Digital power' may be a term in search of a definition, but its elusiveness does not seem likely to deter those active in the digital world from seeking to understand its potential.



The New Great Game explained – Madrid workshop storyboard
Design by dibujario.com

EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

EUROPE'S DIGITAL POWER: FROM GEO-ECONOMICS TO CYBERSECURITY

Introduction

This conference report summarises the key outcomes of the Europe's Digital Power project, undertaken by the European Council on Foreign Relations between December 2015-February 2017. The project rested on two underlying assumptions. First, that, on an international scale, economic and political power is being redistributed according to the new realities of an interconnected digital world. And, second, given that the European Union is an economic giant, but neither a political union nor a fully integrated digital market, the continent is ill-prepared to compete in the geo-economic and geopolitical spheres of today and tomorrow.

To explore this reconfiguration of power in the digital age, five workshops were conducted as part of the project. The initial brainstorming workshop was held at BBVA in Madrid and led to the publication of 'The New Great Game' thinkpiece, which drew together initial thoughts and observations into a discussion of power in the digital arena.[1] It argued that, "the digital revolution [...] ushered in a new era in which power, and the means of acquiring and retaining it, [have] been drastically redefined." The thinkpiece constituted the focus of the discussion at the project's second workshop at the Axel Springer Plug & Play Accelerator in Berlin. The third workshop was held at the NUMA start-up accelerator in Paris, to discuss 'the future of the digital industry in France' and 'the future of privacy, law enforcement, and national defence.' The fourth workshop took place at ECFR's London office and explored 'the evolving cyberthreat landscape' as well as 'the state of play of internet governance and the role of Europe.' The project's final event was held at Telefonica in Brussels, where the project team presented a draft version of this report. The workshops were attended by government and private sector representatives.

Within the confines of the project, the discussions covered a broad range of digital issues, from data protection, cybersecurity, and venture capitalism, to digital sovereignty, regulatory frameworks, and internet governance.

This report, first, considers the nature of digital power; second, touches upon topics which the majority of workshop participants felt to be of importance; and third, contextualises the views stakeholders shared during the course of the project.

Europe's Digital Power: events

Initial brainstorming

BBVA, Madrid, Spain
9 December 2015

'The New Great Game' and 'How to Win the Game'

Axel Springer Plug & Play Accelerator, Berlin, Germany
25 April 2016

'The Future of the Digital Industry in France' and 'The Future of Privacy, Law Enforcement, and National Defence'

NUMA (Start-up accelerator), Paris, France
20 October 2016

'The Evolving Cyberthreat Landscape: From Utopia to Dystopia' and 'The State of Play of Internet Governance and the Role of Europe'

ECFR, London, United Kingdom
29 November 2016

'What is Power in the Digital Age? And How Should Europe Wield it?' and 'What Do We Need to Get Done?'

Telefonica, Brussels, Belgium
30 January 2017

1 Andrew Puddephatt, José Ignacio Torreblanca, and Nika Prislan, "The New Great Game". ECFR. 2016. Available at: http://www.ecfr.eu/page/-/The_New_Great_Game_ECFR.pdf.

Front cover icon credits, left to right: Alfredo Hernandez; Gregor Cresnar; Freepik; Gregor Cresnar.
P.12 arrow icon: Anton Saputro.
All from flaticon.com

'Digital power': A term in search of a definition

The term 'digital power' remains highly contested. Besides its usage in the private sector, where it is used to refer to the optimisation of power generation, electricity grids, and electricity consumption, it does not enjoy a generally agreed definition.[2] It is yet to even filter through into popular discourse: search online for 'digital power' and the term yields a mere 102 results on nytimes.com, 40 on arstechnica.com, 34 on theguardian.com, 18 on wired.com, and only three on politico.com.[3] And, as per its industry-specific definition, the vast majority of these hits touch exclusively on energy and electricity rather than foreign policy or internet governance.

Despite this shortcoming, a growing number of foreign policy analysts have begun to use the term. But a brief overview of different analysts' views on what the term should refer to shows that work remains to be done to complete the definition.

Antonia Colibasanu, geopolitical risk analyst at Stratfor, for example, argues that "digital power embraces and enhances the three dimensions that traditionally define national power – political, economic, and military."[4] Michael Cox, professor of international relations at the London School of Economics, describes it as, "the ability of a public or private actor to combine information on any particular individual, and use this information for comparative and analytical purposes."[5] And Josef Ansorge, author of Identify and Sort: How Digital Power Changed World Politics, explains that "digital power enables novel approaches and policies to prevent crime, control immigration, run election campaigns, combat terrorism, run development programs, and fight wars."[6]

"The concept of digital power remains highly contested"

'The New Great Game' thinkpiece advanced a set of arguments which served as a key starting point for further discussion on elaborating the concept of digital power. However, it must be said that even 'The New Great Game' refrained from proposing a single definition of 'digital power.' Instead, it depicted a digital arena within which traditional power struggles take place:

> *The digital revolution has ushered in a new era in which power, and the means of acquiring and retaining it, has been drastically redefined. As digital inexorably transforms every facet of communication and organisation, it dramatically reconfigures the political and the socioeconomic spheres. Traditional actors vying for power in this uncharted territory continue to employ traditional Great Game geo-political and geo-economic strategies in the digital world.*
>
> *This scramble to master an entity with no centralised governance nor international standards or policies for access and usage is redefining the very nature of the internet … States increasingly try to subordinate the internet and digital domains for nationally strategic purposes while a handful of economic actors swell with unrivalled market capitalisations.*

In the project workshops subsequent to the publication of 'The New Great Game', participants were sceptical of the approach adopted in the thinkpiece. Criticism principally rested on the question of whether geo-economic competition between states in cyberspace constitutes a valid analytical frame. Numerous participants argued that it is wrong to apply great power politics to the digital economy.[7] As one put it: "We should avoid a nineteenth century-inspired framing of twenty-first century digitisation which is based on wrong assumptions and leads to dangerous conclusions."[8] Another maintained that businesses – the main players in the digital world – do not at all accept that digital power as such is a relevant concern: "Why are we debating who gets which piece of the [digital] cake? In the technological sphere, most companies just see the cake getting bigger, and are interested in how the cake can get bigger, rather than who gets what piece of the cake."[9]

One contribution to the debate around the nature of digital power emerging from this project might be a simpler definition; one which bases itself on the components that workshop participants felt were important in the digital world of today and tomorrow. Their preference was to address the question of digital power less in terms of the power politics of states and more in terms of examining and understanding its component parts. On this definition, digital power may be defined as: the combination of, first, a country's digital economy (including market size) and, second, its cyberpower (including cybersecurity and offensive cyber-operations).

The first component comprises the material resources to build, expand, and improve upon the infrastructure that defines cyberspace and the absolute and potential size of a nation's digital economy. The latter component – cyberpower – has been defined as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."[10] This

2 General Electric. "Electric Value Network – Digital Transformation with GE Solutions". 2016. Available at: https://www.ge.com/digital/sites/default/files/GE-energy-electricity-value-network-in-fographic.pdf; iWatt. What is Digital Power? 2010. Available at: http://i.cmpnet.com/powermanagementdesignline/2010/09/C0638.pdf.
3 Google search parameters: "digital power" site:*.com.
4 Antonia Colibasanu. "Nation-States in the Digital World". RealClearDefense. 13 August 2016. Available at: http://www.realclearworld.com/articles/2016/08/13/nation-states_in_the_digital_world_111989.html.
5 Michael Cox et al. "21st Century Power – Dislocation, Diffusion and Decay". London School of Economics IDEAS, Panel report for the Churchill Leadership Programme. p. 8. 2015. Available at: https://www.churchillcentral.com/dms/cms-content/Panel-reports/21st-Century-Power/21st percent20Century percent20Power.pdf.
6 Josef Teboho Ansorge. Identify and Sort: How Digital Power Changed World Politics. Oxford University Press. p. 8. 2016.
7 ECFR Digital Power Project Workshop in Berlin. 25 April 2016; ECFR Digital Power Project Workshop in Brussels. 30 January 2017.
8 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.
9 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.
10 Daniel T Kuehl. "From Cyberspace to Cyberpower: Defining the Problem" p. 12. 2014. Available

ECFR Digital Power brainstorming event, BBVA, Madrid, Spain, 9 December 2015

includes everything from setting norms and standards, and governments exercising control over companies, to Denial of Service attacks and physically cutting data cables.[11]

How would this definition be applied in practice?

'Estonia versus Germany'

Following this understanding, if we compare, for instance, Estonia and Germany, we may conclude that Estonia is the stronger cyberpower. First, Estonia has a significantly smaller attack surface, namely, a smaller digital infrastructure to defend. Second, it maintains a high-readiness cyberforce and has significant surge capabilities with the Estonian Cyber Defence League (a professional volunteer force with cyberdefence skills). And, third, it has been actively pushing cybersecurity and cyberdefence as a priority, particularly within NATO and the EU. Estonian cyber expert Liina Areng describes this asymmetry very neatly by noting that "efficient, autonomous and well-trained cyber-defence forces within a limited, well-protected cyberattack space can secure victory by using innovative techniques to breach the less defensible network breadth of large state cyber-defence or cyber warfare organisation."[12]

However, as a digital power Germany is clearly the stronger of the two. The concept of digital power encompasses more than just cyber capability. We can observe this if we consider the overall size of Germany's digital economy, the size of its population and education sector, and the number of German engineering and manufacturing giants. Deutsche Telekom alone, for example, earned a net revenue of €18.1 billion in Q3 2017, while Estonia's entire GDP (constant prices) stood at €17.6 billion in 2015.[13] Indeed, by taking into account the economic dimensions of the digital revolution, we are able to more accurately connect 'digital power' to earlier conceptions of power, which proclaim that "power is epitomised in control over resources."[14]

Europe's Digital Power project did not solve the conundrum regarding the definition of 'digital power'. Neither the thinkpiece nor the workshops in Madrid and Berlin, where 'digital power' was specifically discussed, were able to settle on a single meaning or what its component parts might be. As such, the concept remains highly contested. The most important economic and cybersecurity themes that emerged across the five workshops are aggregated and grouped together in this conference report.

at: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf. In Franklin D Kramer et al. "Cyberpower and National Security". National Defense University Press. Washington, DC. p. 38. 2009.

11 Joseph Nye. "Cyber Power". Harvard Kennedy School: Belfer Center for Science and International Affairs. Available at: http://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf. p. 5. 2010.

12 Liina Areng. "Lilliputian States in Digital Affairs and Cyber Security". NATO CCDCOE - Tallinn Paper No. 4. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_04.pdf, p. 11. 2014.

13 Deutsche Telekom. 'Financial Results for Third Quarter 2016.' Available at: https://www.telekom.com/en/investor-relations/publications/financial-results; IMF. 2016. World Economic Outlook Database. 2016. Available at: http://www.imf.org/external/pubs/ft/weo/2016/01/weodata/weorept.aspx?sy=2014&ey=2021&scsm=1&ssd=1&sort=country&ds=.&br=1&pr1.x=66&pr1.y=12&c=939&s=NGDP_R&grp=0&a=.

14 Jelle van Haaster. "Assessing Cyber Power". p. 8. 2016. NATO CCDCOE – 8th International Conference on Cyber Conflict. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Art percent2001 percent20Assessing percent20Cyber percent20Power.pdf.

Does Europe need 'digital champions'?

'The New Great Game' points out that Europe essentially missed out on the first wave of digital innovation and therefore left Europe weaker in digital power terms. This is evidenced, as the thinkpiece argues, by the absence of any European 'digital champions' able to rival social network giants like Facebook, Twitter, Microsoft's LinkedIn, or Google's YouTube. Moreover, the rise of the sharing economy with Uber, Airbnb, and no serious European contender in the race, marked the end of the second innovation wave. To this the thinkpiece could have added a third, fourth, and fifth innovation wave missed by Europe over the years. Take, for example, the OS smartphone market which is divided between Google's Android (86.8 percent) and Apple's iOS (12.5 percent);[15] the rise of the public cloud infrastructure, which Amazon Web Service (AWS) dominates with an approximate 45 percent market share; or Google's search engine which reigns supreme with an annual global market share of 80-90 percent on desktops,[16] and over 90 percent on mobile devices.[17]

In the same vein, the European Parliament Industry Committee co-rapporteur Kaja Kallas MEP noted in 2016 that, "Europe has already missed two waves of innovation ... If we don't want to miss the next wave, we have to look to the Internet of Things, Big Data and machine-to-machine communication. They can radically transform our economy and our legislation needs to reflect that."[18]

One look at the numbers reveals that European tech companies currently lack the size to compete with their US counterparts. A 2016 report by Atomico and Slush on 'The State of European Tech' highlighted that there are 17 American tech companies with a market capitalisation of over $50 billion, and only a single European one (German software giant SAP).[19] The situation does not look any different in the start-up scene, with 'The New Great Game' reporting that "101 is the number of start-ups valued at over $1 billion in the US, 36 in China, and just 18 in Europe."[20]

However, lost within the narrative of a 'weak' digital Europe are the continent's high internet access rates and their traditionally strong telecommunication companies. Sweden's Ericsson for example holds the second largest share in the global mobile infrastructure market with 28 percent. Together with Finland's Nokia (26 percent), both capture more than half of the global market, while US companies are notably absent from this part of the global economy.[21]

When it comes to start-ups it is also not well known that there are actually more public tech companies in Europe (914), than in the United States (731) or China (650).[22] The problem is that most of these "have smaller valuations, with 615 [in Europe] commanding market capitalization of less than $100 million [...] In the US only 197 companies have market caps of less than $100 million."[23]

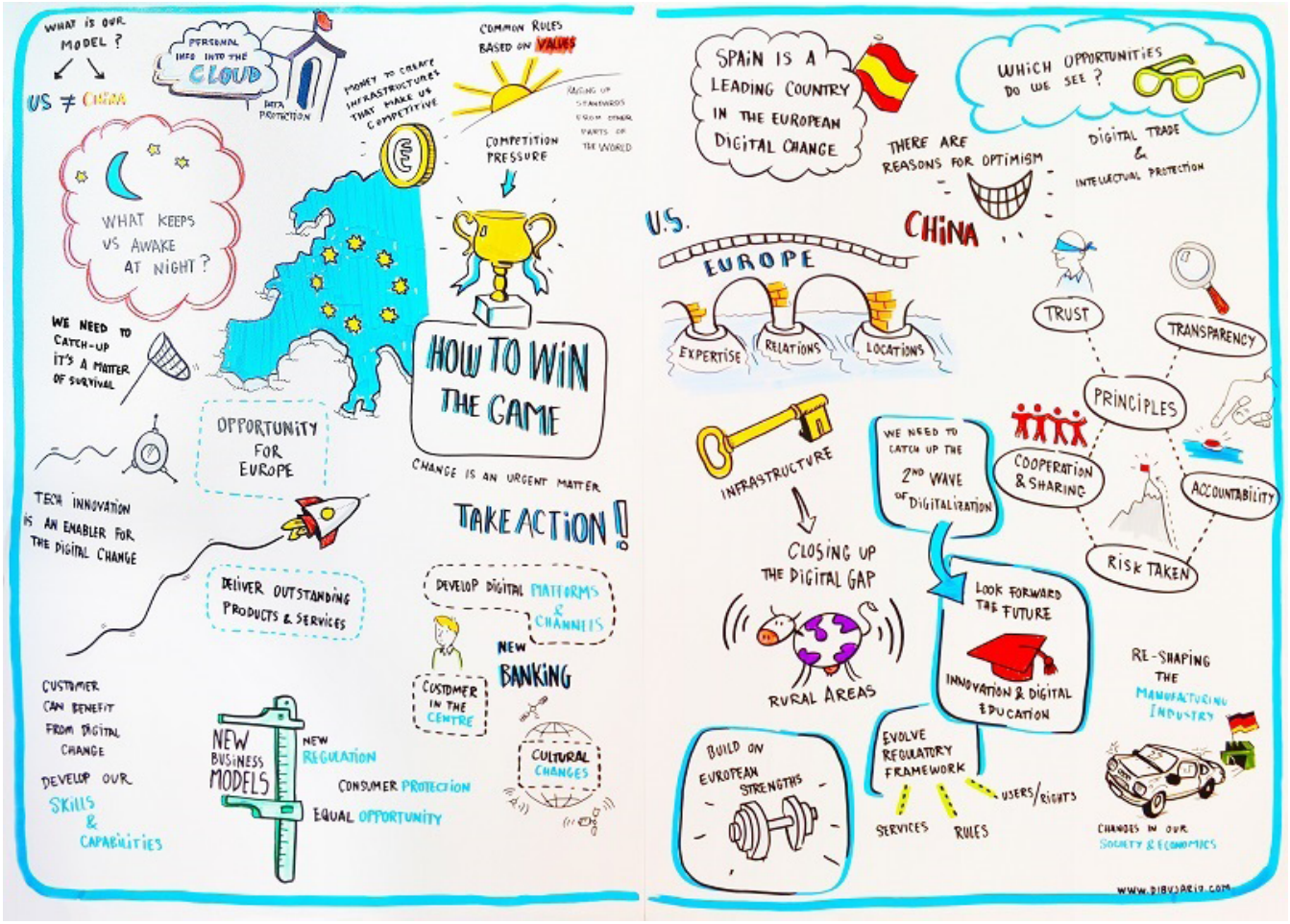
Large European corporations have woken up to this reality and are adapting their innovation models, by either investing in or directly hosting start-ups in-house. The vibrant start-up incubator/accelerator landscape in Europe is an integral part of this dynamic evolution. Accelerators like NUMA (the location of the third project workshop, in Paris; see above), for example, are maintaining open innovation programmes in which large international companies can experiment, interact, and cooperate with start-ups. Maurice Levy, head of marketing and communication at Publicis, has explained the underlying concept by stating that "[in Europe] we don't have the same ecosystem as the U.S. [...] which is why it makes sense to combine startups with the large corporate sector."[24]

"Workshop participants were very divided over whether any rise of European digital champions would translate into an increase in Europe's digital power"

But not everyone shares the positive take on this 'idea farming' approach to harnessing innovation. Jon Evans at Techcrunch has argued that "this strategy stands in striking contrast to the Silicon Valley ethos that startups should devour and replace legacy dinosaurs, not prop them up", adding, "Can you imagine an early-stage Airbnb excitedly trumpeting a joint venture with Marriott, or a young Uber desperately seeking a partnership with Yellow Cab?"[25]

One way or the other, as Tom Wehmeier, principal and head of research at Atomico, has optimistically predicted, "over the course of the next 10 years [...] we will see Europe produce a company on the scale of Google and Facebook".[26]

15 IDC. "Smartphone OS Market Share, 2016 Q3". 2016. Available at: http://www.idc.com/promo/smartphone-market-share/os;jsessionid=8480E0E68BDFEAF397544E8A6E319E2D.
16 Netmarketshare. "Desktop Search Engine Market Share". Available at: https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0; Statista. 2016. Worldwide desktop market share of leading search engines from January 2010 to October 2016.' Available at: https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/.
17 Netmarketshare. "Mobile/Tablet Search Engine Market Share". 2015. Available at: https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=1.
18 European Parliament. "Stop geo-blocking and boost e-commerce and digital innovation, says Parliament". Press release. 19 January 2016. Available at: http://www.europarl.europa.eu/pdfs/news/expert/infopress/20160114IPR09903/20160114IsPR09903_en.pdf.
19 Atomico. "The State of European Tech 2016: the future is being invented in Europe". 2016. Available at: http://www.atomico.com/news/the-state-of-european-tech-2016.
20 These numbers were taken from Fortune's unicorn database, which is yet to be updated. Available at: http://fortune.com/unicorns/.
21 Mike Dano, "Huawei pulls ahead of Ericsson, Nokia in overall RAN market share, Dell'Oro Group reports". FierceWireless. 10 August 2016. Available at: http://www.fiercewireless.com/wireless/huawei-pulls-ahead-ericsson-nokia-overall-ran-market-share-dell-oro-group-reports.
22 Atomico. "The State of European Tech 2016: the future is being invented in Europe". p. 96. 2016. Available at: http://www.atomico.com/news/the-state-of-european-tech-2016.
23 Arjun Kharpal. "European tech start-ups are on for a record year and US investors want in". CNBC. 30 November 2016. Available at: http://www.cnbc.com/2016/11/30/european-tech-start-ups-are-on-for-a-record-year-and-us-investors-next-facebook-google.html.
24 Mike Butcher. "Vivatech concentrates France's booming tech scene, and its minds". Techcrunch. 1 July 2016. Available at: https://techcrunch.com/2016/07/01/vivatech-concentrates-frances-booming-tech-scene-and-its-minds/.
25 Jon Evans. "Vive la France! Vive la Tech!… But do these two great tastes taste great together?" Techcrunch. 5 June 2016. Available at: https://techcrunch.com/2016/06/05/vive-la-vive-la-vive/.
26 Arjun Kharpal. "European tech start-ups are on for a record year and US investors want in". CNBC. 30 November 2016. Available at: http://www.cnbc.com/2016/11/30/european-tech-start-ups-are-on-for-a-record-year-and-us-investors-next-facebook-google.html.



Discussion input: How to win the New Great Game?
Madrid workshop storyboard
Design by dibujario.com

Given that this is very much a live debate, what was the sense on this in the project's workshops, which brought together government and private sector representatives?

The view from the workshops

Workshop participants were very divided over the question of whether any rise of European digital champions would actually translate into the creation of or an increase in Europe's digital power. As one participant put it: "Europe needs to attain digital power, not to counter US technological might but for the sake of matching it and finding areas of potential cooperation."[27] Some agreed that a strong digital economy is central to this.

But others were cautious about the tendency of the 'digital power' debate to pit the United States against Europe. As one participant warned, we should avoid "translating a fundamental transformation of the economy [the digital revolution] unnecessarily into an issue that could bring harm to transatlantic relations."[28]

In fact, most workshop participants pointed to the fragmented nature of power when considered in geo-economic terms. Few saw a strong correlation between power and the digital economy, given, first of all, that current internet companies are inherently multinationals, and second, even US-headquartered internet companies do not assist the US in foreign policy terms, because they need to adhere to numerous national jurisdictions and have to protect their own branding on a global scale.

The project's first two workshops gave direct consideration to whether Europe needs to strategically create its own digital champions to rival those from across the Atlantic. Several participants in the workshops voiced serious concerns that large US-headquartered internet companies will, despite the number of competition rulings against them, continue to

27 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.

28 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.

dominate the European market by simply outspending, out-innovating, or outgrowing any serious competition.

But the situation is not quite as straightforward as it might first appear. One workshop participant was keen to explain that, "often in Europe there is this attitude that [US internet companies] figured out their thing and can now lean back and wait for the profits to come in, but there is a lot of nervousness in these companies [...]. The notion that winners will always be winners and losers will always be losers is not how we see the dynamics playing out." As such even the large US internet companies are facing the same innovation pressures as everyone else in the market.[29]

The overarching challenge, as one workshop participant explained, is to find a healthy balance on innovation and competition. On the one hand, large companies do not want to be 'Uberised' and are interested in building up start-ups to push innovation. On the other hand, not all start-ups want to be acquired, and nor are they easily integrated into a large company.[30]

"Many workshop participants warned against treating the digital world as an arena of power competition"

Many workshop participants warned against treating the digital world as an arena of power competition. Doing so could impact on the benefits that European consumers enjoy from the digital economy.[31] One workshop participant stated that, "it all comes down to whether we accept the politicisation of the internet [...] and accept that Europe simply has to compete because that is the direction the internet is moving toward. Or whether the thrust of European policy should prevent this politicisation, to depoliticise it, to regulate the internet, and avoid controlling it."[32]

***

This project took place in the context of a highly contested debate about why Europe lacks digital champions. It was clear from the views expressed in the workshops that there remains disagreement about how to create digital champions. There was further disagreement about whether the lack of champions means that Europe wields less digital power as a result. Many participants maintained that there is no necessary correlation between the size of a country's digital economy and the size of its digital power. A larger digital economy may be beneficial in a general sense but participants disagreed about the extent to which this allows digital power to be wielded directly.

Becoming a stronger digital power: regulation, protectionism and infrastructure

There is a live debate around the rules which govern the digital sphere in Europe, the way these are used, and the extent to which they attract or put off investment. There is further significant overlap with the debate about how best to upgrade the necessary infrastructure to support the digital economy in the future.

No less a figure than Barack Obama spelt out the feeling, most pervasive in the US, that Europeans have not only failed to compete on the international stage, but have retreated into the comforts of protectionism to make up for this failure. In his interview with Recode in 2015, he said that, "we have owned the Internet. Our companies have created it, expanded it, perfected it in ways that [the Europeans] can't compete. And oftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests."[33]

But US accusations of protectionism against the EU go beyond the presidency and have included alleged excessive data protection and privacy rules; taxation issues; and the number of anti-trust complaints filed against US companies. The cases are indeed numerous, stretching from the European Parliament's vote in favour of 'breaking up Google' in November 2014, to the fall of the 'Safe Harbor' data security agreement, and the quick assembly of the EU-US Privacy Shield. Other prominent matters include the European Commission's charge against Apple to pay back the Irish government €13 billion in illegal state-aid.[34]

Europeans reject these charges, but they are not unfounded. European governments have long sought to protect their industrial base companies and are even trying to shield social cohesion from market disruption. Banning Uber and Airbnb, clamping down on Google, and increasingly trying to police or even legislate social media content, are just a few recent examples. Peter Terium, chief executive of Innogy, noted that "[European governments] try to think of all the excesses that are possible and try to regulate them away. [While] the US approach is: let's first roll out the market, then legislate the excesses that we see and not the ones we can theoretically think of."[35]

29 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.
30 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.
31 ECFR Digital Power Project Workshop in Brussels. 30 January 2017.
32 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.

33 Kara Swisher. "White House. Red Chair. Obama Meets Swisher". Recode. 15 February 2015. Available at: http://www.recode.net/2015/2/15/11559056/white-house-red-chair-obama-meets-swisher.
34 Samuel Gibbs. "European parliament votes yes on 'Google breakup' motion". The Guardian. 27 November 2014. Available at: https://www.theguardian.com/technology/2014/nov/27/european-parliament-votes-yes-google-breakup-motion; Amar Toor. "French taxi drivers clash with police in anti-Uber strike". The Verge. 26 January 2016. Available at: http://www.theverge.com/2016/1/26/10832204/french-taxi-uber-strike-paris-vtc; European Commission. "European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows". Press release. 12 July 2016. Available at: http://europa.eu/rapid/press-release_IP-16-2461_en.htm; European Commission. "State aid: Ireland gave illegal tax benefits to Apple worth up to €13 billion". Press Release. 30 August 2016. Available at: http://europa.eu/rapid/press-release_IP-16-2923_en.htm.
35 Guy Chazan. "Why Germany needs to accelerate into the digital fast lane". Financial Times. 25

Indeed, regulation inside Europe itself – and the extent to which it has failed to keep pace with the nature of the modern economy – constitutes a further source of active debate.

Some European companies complain that they are unable to innovate while being constrained by existing regulations and compliance systems – unlike, for example, new entrants such as Uber or WhatsApp, which have disrupted their respective sectors without being subject to the same rules as their competitors. In the banking sector, for example, companies are currently trying to understand how to apply blockchain technology to its infrastructure, without creating a transparent and decentralised network that would violate privacy regulations and unravel the existing central bank focused monetary system.[36] As such, Huw van Steenis, analyst at Morgan Stanley, noted that "not one bank nor policymaker that we have met with on blockchain gives even a second thought to an unpermissioned public network."[37]

Meanwhile, despite the flourishing European start-up ecosystem and a positive shift in attitudes toward tech globally, there are still several barriers that complicate Europe's stronger advance in the digital field. In Europe only one-fifth of venture capital is available to start-ups when compared to the situation in the US, something which pushes numerous start-ups to move either to London, Silicon Valley, or New York, or try their luck in various EU member states that have lower living costs. The same outward trajectory is visible when it comes to the large number of European expatriates who either studied in the US or moved there to successfully launch companies in Silicon Valley.

The view from the workshops

In the light of US internet companies' dominance of the global digital market, some workshop participants went so far as to make the case for Europe to actually follow the Chinese model to kickstart growth of its own domestic industries. One participant argued that, "it may not be politically correct, but Alibaba would never have grown as much, if Amazon were allowed to operate in China."[38]

But as one participant noted: "our protectionism is not protecting emerging digital champions, but our 19th century companies. We have protectionism, but it's the wrong one."[39] Indeed, several workshop participants warned that replicating China's protectionism cannot be the answer to a problem that is inherently about the agility of governments and companies to adapt to fundamental market changes and the speed of innovation.[40] Indeed, this is easier said than done, but as one workshop participant recommended, policymakers need to re-examine existing regulations, set up clear limits of what is allowed and what is not, and enable markets to experiment within these new parameters.[41] Another participant explained that the fundamental policy issue comes down to "outdated regulations, or the lack of rules implementation, which have created a situation in which regulators are tackling the same services differently."[42] Telecommunications industry representatives in particular strongly backed the idea that "consumers deserve the same protection regardless of the company providing the service, its legal settlement location, or the location where the consumer is accessing the service from." As such a "level playing field across the digital ecosystem is a prerequisite for guaranteeing users' rights while providing fair competition between companies and services."[43]

There was entrenched scepticism in the workshops about the attractiveness of Europe as an investment destination and location for digital business. One workshop participant explained that, "in the long run [start-ups] will realise that it is not in their interest to expand to other EU member states, as the costs and risks simply outweigh the benefits of just moving to the United States."[44] Another pointedly remarked, "There are a lot of really good French coders in the digital industry. The main problem is that the majority of them are working in the United States."[45] However, one participant also highlighted that "the European Commission and national governments are doing a much better job now of putting digital education and the fostering of entrepreneurial spirit on the top of the agenda."[46]

> "The European Electronic Communications Code needs to be bolder in its vision by bringing about full spectrum harmonisation"

As a partial solution to reverse this 'brain drain', workshop participants were at pains to stress the importance of the European Digital Single Market (DSM). They viewed it as a priority to provide European corporations and start-ups with the breathing space to compete in the digital arena of tomorrow. Overall, the underlying hopes are that a DSM of 500 million European consumers will spur innovation and competition, prevent the outflow of European talent and ideas to the other side of the Atlantic; attract substantial venture capital from across the globe; and introduce common standards to allow for market scale. One workshop participant highlighted that, "market size is the overarching concern when it comes to competing on the digital playing field."[47] Completing the DSM would help companies to grow and develop within a large market, and would promote a

January 2017. Available at: https://www.ft.com/content/31469796-dcd1-11e6-9d7c-be108f1c1dce"
36 Kadhim Shubber. "Banks find blockchain hard to put into practice". Financial Times. 12 September 2016. Available at: https://www.ft.com/content/0288caea-7382-11e6-bf48-b372cdb1043a.
37 Philip Stafford. 2016. "Banks struggle to make blockchain fast and secure". Financial Times. 26 September 2016. Available at: https://www.ft.com/content/e0a32840-4f68-11e6-8172-e39ecd3b86fc.
38 ECFR Annual Council Meeting in The Hague. 28 June 2016.
39 ECFR Annual Council Meeting in The Hague. 28 June 2016.
40 ECFR Annual Council Meeting in The Hague. 28 June 2016. ECFR Digital Power Project Workshop in Berlin. 25 April 2016. ECFR Digital Power Project Workshop in Brussels. 30 January 2017.
41 ECFR Digital Power Project Workshop in Berlin. 25 April 2016; See also: Christoph Steck. "Policy challenges of the digital economy". ECFR. 28 July 2015. Available at: http://www.ecfr.eu/article/commentary_policy_challenges_of_the_digital_economy3082.
42 ECFR Digital Power Project Workshop in Brussels. 30 January 2017.
43 ECFR Digital Power Project Workshop in Brussels. 30 January 2017.
44 ECFR Digital Project Workshop in Paris. 20 October 2016.
45 ECFR Digital Project Workshop in Paris. 20 October 2016.
46 ECFR Digital Power Project Workshop in Brussels. 30 January 2017.
47 ECFR Digital Project Workshop in Paris. 20 October 2016.

Don't forget to check out the Europe's Digital Power **web portal**

ecfr.eu/digitalpower

virtuous circle which attracts talent and investment, and further strengthens Europe's digital economy through increased competition, better products and user experience.

Yet much needs to done in order to bring about such a positive set of circumstances, and some of the changes on the horizon may be extremely disruptive. As one workshop participant noted, the primary challenge for Europe's existing industries is to transition into the digital age, while at the same time maintaining their labour force and old factories.[48] Emerging competitors such as Tesla are unsurprisingly able to outflank car makers that still have to invest in technology, such as the clean combustion motor, which will be redundant in 10-15 years.[49] As one participant noted, "sometimes you have to think about a clean break which is very difficult to do, [...] but thinking along those lines is very useful."

Workshop participants further stressed the importance of transmission capabilities, meaning broadband and wireless networks. Indeed, if data is the new currency for innovation and economic prosperity, as one workshop participant argued, then common sense dictates that getting more and more data faster and faster from A to B is a natural development process to sustain a modern digital economy. Indeed, without these continuous modernisation efforts, the cloud, streaming media services such as Netflix and Spotify, or the Internet of Things (IoT), would have been impossible to achieve.

According to one workshop participant, the European Commission's 2016 proposal to establish a European Electronic Communications Code is a first step in the right direction to correct Europe's underlying structural deficiencies. Among other issues, the code proposes better use of radio frequencies through "long licence durations, coupled with more stringent requirements to use spectrum effectively and efficiently."[50] And it puts forward a new business model by "selling wholesale network access to retail operators [which] can reduce competition risks, attract 'patient' capital which supports longer-term investment in very high-capacity networks and thus push out the dividing line between commercial and non-commercial deployment areas."[51]

However, as another participant highlighted, the European Electronic Communications Code needs to be bolder in its vision by bringing about full spectrum harmonisation. In the participant's view, predictable licensing frameworks with traceable renewal mechanisms need to be established in order to incentivise network investment.[52] The EU cannot afford to drop the ball again by repeating mistakes with the next generations of communication networks.

Another workshop participant also noted the importance of enhancing the scope of net neutrality, by including the accessibility to physical networks, which would help unbundle the telecom sector and ease restrictions to real competition. The overall vision, as put forward by the participant, ought to be an environment in which service- and content-operators can utilise and maximise transport network capacity, which in turn is being supplied by neutral telecom infrastructure operators.

> "The EU is missing is an overarching and compelling narrative that sets out a comprehensive vision of the internet, cyberspace and the digital economy"

A further recommendation made by several workshop participants was to implement the DSM faster and manage its progress in a coordinated and coherent fashion.[53] They argued that, if the DSM is elemental to the future of the European digital economy, and is deemed essential to create a gravitational pull on tech, talent, and capital, toward the continent, then putting an emphasis on establishing coordinated regulation criteria is a key to success.[54] One workshop participant therefore argued that the Body of European Regulators for Electronic Communication (BEREC) could, for example, expand its current role and strengthen cooperation between the national authorities to drive an overarching agenda.[55]

Overall, as one participant put it, what the EU is missing is an overarching and compelling narrative that sets out a comprehensive vision of the internet, cyberspace, and the digital economy. Indeed, the global battle cry, regularly head in the digital world, for a 'free, open, and secure internet'[56]

48 ECFR Annual Council Meeting in The Hague. 28 June 2016.
49 ECFR Annual Council Meeting in The Hague. 28 June 2016.
50 European Commission. "Commission welcomes political agreement to boost mobile internet services with high-quality radio frequencies". Press Release. 14 December 2016. Available at: http://europa.eu/rapid/press-release_IP-16-4405_en.htm?locale=EN.
51 EUR-Lex. 2016. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions: Connectivity for a Competitive Digital Single Market – Toward a European Gigabit Society. COM/2016/0587 Final. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX percent3A52016DC0587.
52 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.
53 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.
54 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.
55 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.
56 "Internet Policy and Governance Europe's role in shaping the future of Internet Governance". European Commission. 12 February 2014. Available at: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52014DC0072.

– values that the EU itself has subscribed to – are wholly insufficient and ring rather hollow, when on the one hand EU member states are advocating digital sovereignty, strategic autonomy, and data localisation strategies, while on the other hand authoritarian governments like China and Russia, are actively pushing concepts such as the Digital Objects Architecture (DOA), which could be misused to track user activity online, control the free flow of information, and facilitate government censorship.[57] As one participant noted, "the EU is not up to speed [on the DOA issue], and the US and the UK are in political turmoil currently."[58] Another participant, however, highlighted that "the economic and legal culture differs from one region to another. Europeans, for example, determine their laws on the basis of what they deem permissible in view of our traditions. These might not be exactly the same issues, like privacy or competition, as they are in other parts of the world."[59]

Particularly worrying, according to several workshop participants, is that currently very few, if any, European government officials are actively involved in internet governance forums, and have been pretty much outside these discussions for the past decade.[60] On top of this, other workshop participants noted that Europe would do well to mobilise competencies in the various government agencies to raise awareness of these critical deliberations, otherwise the balance of power on internet governance and other digital issues will pivot away from the liberal narrative and shift toward adopting authoritarian policies.

***

Europe has been accused of adopting a protectionist attitude to its digital economy, and some voices even call for it to go further down this road. However, many more caution against such a strategy and instead urge the completion of the DSM as the key means of attracting – or just simply retaining – talent, investment, and new technologies. In terms of regulation, the question is how to find a workable approach between the changing dynamics of the market and existing regulations, while ensuring regulations are both as up to date as possible and conducive to nurturing digital economic development.

Data protection: An urgent transatlantic dialogue needed

Data protection has, more by accident than design, turned into an important vector in Europe's ambition to promote its norms and values. Indeed, most of the current EU data protection legislation stems from a pre-internet era which did not envisage the vast commercialisation of cyberspace.[61] Yet, with the fall of the 2006 Data Retention Directive, the implementation of the EU-US Privacy Shield, and the General Data Protection Regulation (GDPR), the EU has built a broad narrative on protecting the data and online rights of its citizens.

But not all is as rosy as it seems. The failure to find an agreeable solution to harmonise data retention across Europe has prompted governments and telecom/network providers across the EU to find national solutions in harmony with the European Court of Justice ruling in 2014. The EU's treatment of the UK's investigatory powers bill and that country's adequacy assessment in light of Brexit will be a critical litmus test on whether national security will trump trade and data privacy in the larger context of future EU-UK relations.

Additionally, the case of the US Department of Justice trying to force Microsoft to turn over customer emails stored outside the US, has, for the moment, found an end with the US Court of Appeals for the Second Circuit, quashing the case in July and declining a rehearing on 23 January 2017.[62] However, as the court noted in its 4-4 decision, "it is overdue for a congressional revision that would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs and service provider obligations in the global context in which this case arose."[63] Depending on how Congress moves forward on this, the repercussions could either unravel European data protection regulations, push US email-service providers out of the European market, or simply cut-off EU-US data transfers. Indeed, the EU-US Privacy Shield may already be standing on increasingly weak pillars depending on how the Trump administration implements national security policies going forward.

The implementation of the GDPR is also facing significant challenges across Europe. According to Dell's 2016 global survey of 871 IT professionals, "80 percent said they knew little or nothing about the GDPR, while 97 percent said their companies didn't have a plan in place to implement the new law."[64]

57 Winston Maxwell and Mathilde Gerot. "Ignoring GDPR, French Senate Votes for a Data Localization Amendment'. Hogan Lovells. 1 June 2016. Available at: http://www.hldataprotection.com/2016/06/articles/international-eu-privacy/ignoring-gdpr-french-senate-votes-for-a-data-localization-amendment/; Eli Dourado. "How Russia and the UN are actually planning to take over the internet". The Hill. 12 September 2016. Available at: http://thehill.com/blogs/congress-blog/technology/295320-how-russia-and-the-un-are-actually-planning-to-take-over-the.
58 ECFR Digital Project Workshop in London. 29 November 2016.
59 ECFR Digital Power Project Workshop in Brussels. 30 January 2017.
60 ECFR Digital Project Workshop in London. 29 November 2016; Andrew Puddephatt, "Governing in the digital marketplace". ECFR. 22 July 2015. Available at: http://www.ecfr.eu/article/commentary_governing_in_the_global_marketplace3077.
61 ECFR Digital Power Project Workshop in Brussels. 30 January 2017.
62 Grant Gross. "Court denies U.S. government appeal in Microsoft overseas email case". Computerworld. 24 January 2017. Available at: http://www.computerworld.com/article/3161165/security/court-denies-us-government-appeal-in-microsoft-overseas-email-case.html.
63 Susan L Carney. "SUSAN L. CARNEY, Circuit Judge, concurring in the order denying rehearing en Banc. 24 January 2017. Available at: http://www.politico.com/f/?id=00000159-d0ff-de52-a95b-fcff8f3d0000.
64 Jeff John Roberts. "Firms Are in Denial About the EU's Coming Privacy Law, Survey Suggests". Fortune. 11 October 2016. Available at: http://fortune.com/2016/10/11/gdpr-dell-survey/; "GDPR: Perceptions and Readiness." Dell. September 2016. Available at: https://software.dell.com/docs/

Europe's Digital Power event, Axel Springer Plug & Play Accelerator, Berlin, Germany, 25 April 2016

The European Commission's proposal for a new ePrivacy Regulation, which leaked in December 2016, also aims to further enhance data protections in the realm of electronic communications, by tackling, for instance, the processing of metadata and overhauling the banner-fatigue for cookies.[65]

Given the EU's active position on data protection, some analysts have even put forward the notion of pushing EU data protection standards as an instrument of industrial policy and protectionism. Sebastian Dullien, senior policy fellow at ECFR, for example notes that "the EU could legislate that companies should be fined €500,000 for each case in which they hand over personal data of an EU citizen to foreign law enforcement or secret services without a valid EU court order. [And] given the US rules on how internet companies have to cooperate with US agencies, this would make any kind of engagement by US companies in the EU highly risky and would most likely lead to a withdrawal of a number of US companies from the EU market."[66] Yet, the idea of pushing US companies out of the European market is potentially a dangerous one. Russia, for example, used regulatory powers in November 2016 to block Microsoft's LinkedIn after "a local court ruled [...] that it had breached the country's data protection rules."[67] And in early January 2017, Russian authorities even required Apple and Google to remove LinkedIn from their app stores.

"The debate is only happening in the US, while Europe is almost silent"

gdpr-global-survey-white-paper-23599.pdf.
65 Jennifer Baker. "European Commission proposes formal ePrivacy Regulation". IAPP. 10 January 2017. Available at: https://iapp.org/news/a/european-commission-proposes-formal-eprivacy-regulation/.
66 Sebastien Dullien, "Creating European digital champions". ECFR. Available at: http://www.ecfr.eu/digitalpower/blog/creating_european_digital_champions.
67 Mark Scott. "Russia Prepares to Block LinkedIn After Court Ruling". New York Times. 10 November 2016. Available at: https://www.nytimes.com/2016/11/11/technology/russia-linkedin-data-court-blocked.html?_r=0.

The view from the workshops

One workshop participant noted that, "over the past two decades, only 11 countries have achieved 'adequacy status' by the European Commission, and none of them are global economic players."[68] Matters are complicated further because "the standards and requirements the EU demands of third countries to receive personal data from Europe are perhaps unsustainable, as illustrated by the ongoing legal challenges, e.g. to 'standard clauses,' which many European firms rely on to export data from the EU to the world."[69]

Other workshop participants noted that "we need to reinforce judicial tools and regulations, particularly in view of the Internet of Things and the numerous sensors that will be deployed in a person's home. The GDPR is only one among a range of possible answers, as it makes data controllers, data processors, and cloud providers responsible for the protection of a user's privacy. However, we also need better privacy awareness among the public, which in turn will naturally fuel the demand for more comprehensive privacy protections."[70]

Indeed, numerous workshop participants from national governments pointed to several pieces of legislation on data protection, privacy, and online rights being taken forward. Yet on encryption, for example, one participant noted that, "the debate is only happening in the US, while Europe is almost silent."[71] Even on government access to cloud data, Washington is far ahead of the debates in Brussels, because "10 out of 10 cloud providers are headquartered in the US – and again Europe is silent." Indeed, several participants

68 Commission decisions on the adequacy of the protection of personal data in third countries". European Commission. 24 November 2016. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm).
69 ECFR Digital Power Project Workshop in Brussels. 30 January 2017.
70 ECFR Digital Project Workshop in London. 29 November 2016.
71 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.

queried why European governments are unable to proactively engage in transatlantic debates that are happening right now.[72] Given these issues, one participant stressed the urgent need for a comprehensive and in-depth transatlantic dialogue on data protection and cross-border data transfers.[73]

As another participant added, digital statecraft is still very much misunderstood by European governments. In the data protection context, the participant cited as evidence the fact that, particularly in Germany, "consent is seen as the tool to raise protection levels in Europe. Empirically, however, the opposite is true. People give consent to anything you put in a pop-up in front of them."[74] As a result, the participant concluded that, "governments have not really understood how to effectively shape [digital] markets and shape [online] behaviour in the long term."[75]

***

No consensus emerged in the workshop discussions about whether it would be prudent for the EU to leverage data protection regulations as an element of digital power. On the one hand, data protection regulations have the potential to positively shape the digital economy and benefit European consumers. On the other hand, any heavy-handed data protection policy has the potential to impede transatlantic data flows, and significantly stifle the European digital economy.

72 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.
73 ECFR Digital Power Project Workshop in Brussels. 30 January 2017.
74 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.
75 ECFR Digital Power Project Workshop in Berlin. 25 April 2016.

Cybersecurity: time to get it right

In the domain of cybersecurity, digital power rests on two pillars. First, data-, information-, and network-security are increasingly becoming matters of national security, social stability, and economic prosperity. Evidence of this changing threat-environment includes: cyber-enabled fraud, which in 2016 (in conjunction with computer misuse) overtook all other crime in the UK for the first time ever;[76] IoT botnets leveraging unprecedented denial-of-service attacks against crucial components of the internet infrastructure;[77] numerous cyber-attacks against the Ukrainian electricity grid in late 2015, which were the first publicly acknowledged cyber-incidents to result in power outages;[78] and Russian government agencies' involvement in the 2016 US election process, which compromised the emails of "US persons, and institutions, including [those] from US political organizations."[79]

Second, cybersecurity companies themselves have become a source of national pride and evidence of a country's cyberdefence capability. Given that the market for cybersecurity solutions is booming, they also represent an important stronghold for a nation's digital economy. Take, for example, Thales in France, BAE Systems in the UK, F-Secure in Finland, Avast in the Czech Republic, Bitdefender in Romania, or Panda Security in Spain.

The view from the workshops

In this context, workshop participants noted that it is eminently important that, despite the EU's emphasis on privacy and data protection, the EU not ignore the concerns and challenges law enforcement agencies across Europe are facing, ranging from: targeting individual cybercriminals without compromising the security and privacy of digital users; overcoming the big data challenge by having the right tools, technology, and the right workforce to distil meaningful data to go after cybercriminals; overcoming the low level of cyber-incident reporting (which hopefully the NIS Directive and the GDPR will fix); engaging with hard-to-reach jurisdictions by accessing volatile data and pursuing criminals abroad; and, finally, identifying emerging cybercrime threat areas and identifying socioeconomic indicators for cybercrime.[80] Currently, however, as one participant noted, "there are no real guidelines when it comes to security, and it is thus very difficult for vendors and operators to know what they actually need to secure."[81] Another participant noted that,

76 NCA Strategic Cyber Industry Group. "Cyber Crime Assessment 2016". 7 July 2016. Available at: http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file.
77 "Hacked Cameras, DVRs Powered Today's Massive Internet Outage". Krebs On Security. 21 October 2016. Available at: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.
78 Kim Zetter. "Inside the cunning, unprecedented hack of Ukraine's power grid". 3 March 2016. Available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
79 "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security". 7 October 2016. Available at: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.
80 ECFR Digital Project Workshop in London. 29 November 2016.
81 ECFR Digital Project Workshop in London. 29 November 2016.

"it would be in everyone's best interest if the private sector could have an open conversation with governments across Europe, to assess which cybersecurity strategy we ought to use and what security standards we need to set."[82]

Participants proposed many ideas for fixing the cybersecurity problem, including: better security management, such as having the right method to update and integrate IoT devices; facilitating multi-stakeholder models and creating industry consortiums for cybersecurity; policing national domain allocations to tackle dummy registrations and deanonymising proxy services; accelerating the adoption of Internet Protocol version 6, as well as mitigating services for Internet Protocol version 4 – such as Secure DNS; and strengthening partnerships between the northern and southern European countries and their industrial sectors to harmonise the level of cybersecurity maturity; and, finally, strengthening encryption.[83]

Apart from the underlying challenges of cybersecurity per se, participants also identified two overarching deficiencies within the current European debate. First, the number of politicians actually knowledgeable about cybersecurity issues is too small. And, second, governments are unable to match private sector wages to attract and retain cyber talent.[84]

When it comes to the cyber skills gap, one participant highlighted that organisations are currently too focused on "hiring pieces of paper" and demanding unreasonable job qualifications. Instead, companies should start looking for character traits: for tenacity, parallel thinking, and natural inquisitiveness, and be encouraged to support their employees to attain new knowledge and certificates while on the job.[85] Additionally, current recruitment models need to become more flexible to retain personnel over time and mitigate the loss of knowledge. As one participant put it, "overall it should be easier to move between government, the private sector, and academia. One way to mitigate this is for government agencies to build up specialists that can come back and consult in less formal ways, as trialled by UK law enforcement."[86]

The very live issue of cybersecurity and nation-state intrusions was not discussed at these particular workshops. However, this issue will only continue to grow in importance and future research will also seek to examine and discuss digital power from this perspective.

***

Workshop participants proposed numerous ideas to shape and inform the cybersecurity policy debate. Of particular importance was the notion of getting more politicians involved on cybersecurity issues and finding a workable approach for law enforcement agencies to fight cybercrime without compromising the privacy of digital users.

82 ECFR Digital Project Workshop in Paris. 20 October 2016.
83 ECFR Digital Project Workshop in London. 29 November 2016; ECFR Digital Project Workshop in Paris. 20 October 2016.
84 ECFR Digital Project Workshop in London. 29 November 2016.
85 ECFR Digital Project Workshop in London. 29 November 2016.
86 ECFR Digital Project Workshop in London. 29 November 2016.

Conclusion

The digital space is highly contested, with many competing strands and areas of activity. From Europe – both the EU and member states – there is not as yet any single clear approach to how to govern this space let alone to how to wield power therein. This paper has put forward an understanding of digital power which rests on, first, the strength of the digital economy and, second, cyber capability. It is clear from the workshop debates carried out as part of the Digital Power Project that there is no consensus about the definition of digital power as a concept nor whether it should be applied to current debates in the digital sphere. Some workshop participants were adamant that the concept does not even merit further exploration. Nevertheless, it is still the case that creating strong digital economies and strengthening cyber capability each remain important concerns for key stakeholders, and that across the European economy many opportunities remain to be seized to grow and strengthen the economy. Queries over whether the emergence of 'digital champions' would genuinely increase Europe's digital power are valid; participants insisted that power and influence would not necessarily accrue to states but would, at least, be dispersed among companies and other state actors. Whatever the precision of definitions, Europe's faltering progress towards the completion of the digital single market and its sluggish response to cyber threats are unfortunately suggestive of a reluctance to get fully to grips with digital as a medium. 'Digital power' may be a term in search of a definition, but its elusiveness does not seem likely to deter those active in the digital world from seeking to understand its potential.

About the author

Stefan Soesanto is the digital policy fellow at the European Council on Foreign Relations. He took charge of the project in July 2016. Prior to this engagement he worked at RAND Europe and in the European Parliament.

Acknowledgements

I would like to thank Dina Pardijs for her support, out-of-the-box thinking, and being an invaluable part of the digital power project. I would also like to thank my predecessor, José Ignacio Torreblanca, for starting the project and opening up the discussion on digital power. Special thanks go to Andrew Puddephatt, Sebastian Dullien, Nika Prislan, Susi Dennison, and Jeremy Shapiro for their research input and continuous project support. Thank you to Tara Varma, Lucie Fabiano, and Manuel Lafont Rapnouil for organising the Paris workshop; Alexia Gouttebroze, Edin Dedovic, and Olivia Graham for the event in London; and to Alexander Harding, Iva Kopraleva, and Marisa Figueroa for their support to the Brussels event.

Thanks to Adam Harrison and Gareth Davies for their wizardry in editing the conference report.

Particular thanks also go to all the participants for attending the workshops and openly sharing their critical thoughts, provocative ideas, and valuable insights.

And finally, I want to express my sincere gratitude to the teams at BBVA, Cellnex, and Telefonica for their support.

***

With thanks to our partners:

ECFR/207
ISBN 978-1-911544-07-4