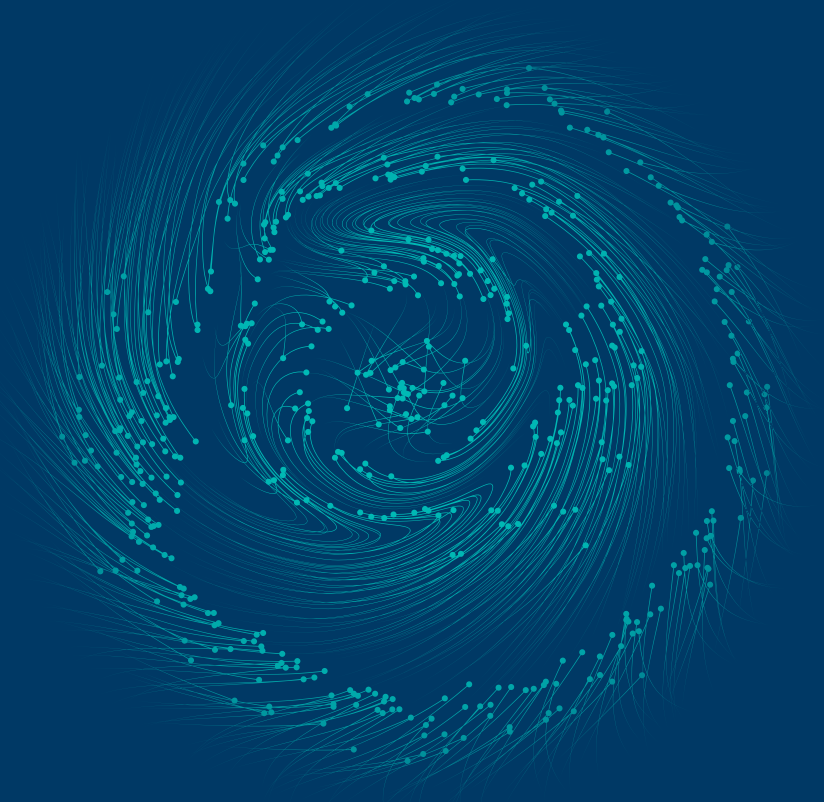
KONRAD ADENAUER STIFTUNG

The Convergence Puzzle: Australia, Germany and Emerging Cybersecurity Trends

Edited by Katja Theodorakis



THE PERISCOPE SERIES
VOLUME 3 / 2020

KONRAD ADENAUER STIFTUNG

About Konrad-Adenauer-Stiftung Australia and The Pacific

The Konrad-Adenauer-Stiftung (KAS) is a political foundation of Germany, with a mission to promote international dialogue, regional integration, sustainable development, good governance, democratic processes, social market economy and exchange of knowledge. It is named after the first Chancellor (Prime Minister) of the Federal Republic of Germany, Konrad Adenauer whose name represents the democratic rebuilding of Germany, the anchoring of German foreign policy in a trans-Atlantic community of values, the vision of European unity, and Germany's orientation towards a social market economy. Currently KAS is present in around 120 countries, with over 100 offices on six continents. With our worldwide networks and long-term partner structures, we aim to contribute to knowledge exchange and policy development in line with our values and aims.

As current global developments - such as the volatile security environment – underscore the common interests of Europe and Australia, KAS' Regional Programme for Australia and the Pacific seeks to foster durable collaboration through dialogue among parliamentarians, politicians, and representatives of leading think tanks, as well as political analysis and consultancy. For the European Union in general and Germany in particular, dialogues with Australia and New Zealand are of special relevance due to our history of strong bilateral and regional relations. Given our shared values, common beliefs and interests, there are manifold opportunities for this partnership.

About the Periscope Series

'Periscope' is the Occasional Analysis Paper series of the Konrad Adenauer Foundation's Regional Programme Australia and the Pacific. Just like the real-world sighting instrument, Periscope is meant to broaden our insights - taking in views from different angles. In this instance, it seeks to bring together perspectives from Germany, Europe and the Australia/Pacific region in order to augment our understanding of contemporary issues in the area of foreign and security policy as well as energy, economic and social policy matters. Previous editions of Periscope have focused on energy security and the geopolitical dimensions of cybersecurity challenges.

In this Edition

This edition, a collection of contributions from Australia and Germany, is concerned with emerging trends, challenges and patterns in cybersecurity relevant for both countries. The articles in this compilation – some are structured analysis pieces, some constitute more personal yet substantive reflections – were deliberately kept diverse in style, format and content to reflect a variety of perspectives and approaches. They were collected throughout 2019 and reflect dynamics at the time of writing (indicated above each contribution) –they were not intended to capture the most up-to-date developments. The only request to the authors was for them to offer their thoughts on what they perceived as an important issue or angle to the contemporary cybersecurity landscape. Interestingly, what stood out during the compilation process was that as a whole, the contributions seemed organically connected by the implied acknowledgement that an area of key importance is the way data is governed; this is due to its impact on our collective and individual freedoms, especially in an era of democratic disenchantment and contested global governance.

Titled the "**Convergence Puzzle**", this edited volume is framed by a conceptualization of cyberspace as a realm of converging and diverging forces and interests: technological, social, political, economic, institutional, cultural, ideational/ideological and strategic. These co-exist, compete and act upon each other - forming a complex ecosystem of dynamic, interlinked threat and opportunity vectors. As such, this overarching theme is premised on the recognition that viewing cybersecurity as a mainly technological matter would be reductionist and fail to capture the complexity of a space created and shaped by humans. Acknowledging the extent to which technology is used as a (geo)political and strategic tool, it is better viewed as a vehicle or force enabler/multiplier for human interests, in particular political, economic and strategic goals.

A further premise of this volume is that technology is not neutral but can act as a corrosive force for liberal values; as current developments show, technology is in fact being actively used to undermine democratic systems. With global powershifts manifesting in competing political models that seek to challenge the liberal order, 'doing cybersecurity' should hence include addressing questions of sovereignty, governmental/institutional overreach, transparency and accountability. Accordingly, what makes the space of emerging cyber dynamics a puzzle rather than just a tangle of non-linear causes and effects is the overarching goal of working out and managing the relationship between these forces in a way that aligns with the bigger picture: to make them converge in a manner that strengthens rather than undermines the foundations of liberal orders – both domestically and at the international/multilateral level. Consequently, the 'convergence puzzle' seeks to serve as a reminder of where the center of gravity should lie in debates on cybersecurity: in a commitment to the core of the liberal project as its best defense mechanism.

The Convergence Puzzle: Australia, Germany and Emerging Cybersecurity Trends

The Periscope Series
Volume 3 / 2020

Reflections

Analysis

Preface

It is with great pleasure that I introduce this latest edition of our Periscope to you. As value partners, Germany and Australia share a similar overall approach based on their common value basis but how 'cybersecurity is done' at the policy level varies – and it is important to examine the key differences in these approaches in order to capture the nuances and multi-facetted nature of these perspectives.

This focus is especially salient against the backdrop of a globalised and interdependent world, where economic well-being, political stability and security are interlinked.

After the success of our first Australia-Germany Cybersecurity Dialogue in Canberra in 2018, for the 2019 dialogue we took a stellar group of Australian experts to Berlin and Brussels. The delegation engaged in various thematic roundtables and meetings at relevant ministries and institutions to examine current challenges and explore possible solutions based on bi-lateral and multi-lateral cooperation. The focus was on how to best manage emerging challenges based on multifaceted approaches, strategic assessments and answers that are responsive to the respective geopolitical, socio-political and economic contexts from which these arise. For this end, a variety of institutions and viewpoints were selected – in Germany this included the relevant government departments, the Bundestag, think tanks and industry. In Brussels, meetings were held at the EU level, such as the European Commission (Directorate-General Communications Network, Content and Technology), with various policy experts, academics and also industry representatives as well as the Cyber Defence Section at NATO headquarters.

In particular, one key objective was to assess how Australia and Germany/Europe may take similar or different approaches, looking at the varied circumstances they may encounter in specific areas. Accordingly, the value of the meetings lies in an exchange of perspectives especially when there are diverging approaches such as for example in the German and Australian policy responses to the rollout of 5G and the management of so-called 'high/risk' vendors.

This is especially important seeing that liberal democracy is under pressure globally, from systemic challenges to existing values and orders which translates into a waning faith in multilateralism and international institutions. In responding to such challenges, there is an increased need for cooperation between like-minded nations who can work together to uphold the principles underpinning the liberal architecture.

This is done by devising frameworks and policies that reflect this normative foundation and offer solutions to the pressing problems of our time.

The delegation at the Federation of German Industries, Berlin June 2019

From right to left: Dr Beatrice Gorawantschy (Director KAS Regional Programme Australia and the Pacific), Prof Lyria Benett Moses (Director of the Allen's Hub for Technology, Law & Innovation at the University of New South Wales Sydney), Fergus Hanson (Director of the Australian Strategic Policy Institute's International Cyber Policy Centre), Rachael Falk (Chief Executive of the Australian Cyber Research Council), Amos Helms (KAS HQ), Prof Lesley Seebeck (Chief Executive of the Australian National University's Cyber Institute), Katja Theodorakis (Programme Manager Foreign/Security Policy KAS Australia and the Pacific).

On the European level, it is more important than ever that the new EU Commission has taken up its work with a clear 'geopolitical dimension' and quest for 'strategic autonomy', also having to face new regional security challenges such as climate sustainability and digital transformation. Likewise, for Australia – as a key player in the Asia-Pacific - questions of regional leadership, institution-building and integration are of paramount importance to ensure continued geopolitical and geo-economic stability, security and prosperity.

The Konrad Adenauer Foundation is committed to enhancing understanding of the drivers of these global developments and promote knowledge-sharing and dialogue among key stakeholders in the political process. It is my hope that our latest Periscope edition actively contributes to this goal.

Dr Beatrice Gorawantschy
Director KAS Regional Programme Australia and the Pacific

INTRODUCTION

The Convergence Puzzle

Katja Theodorakis, Senior Programme Coordinator Research & Analysis at the Konrad–Adenauer–Foundation's Regional Programme Australia and the Pacific

February 2020

About the Author

Katja is a national security professional with particular expertise in the areas of terrorism/extremism, jihadism and the propaganda dynamics of asymmetric/hybrid conflict. At KAS, she coordinates a portfolio that includes topics like the wider strategic relations in the Asia-Pacific, cybersecurity, European defence/security matters and the field of terrorism/extremism.

She is also a PhD candidate at the School of Humanities and Social Sciences at UNSW ADFA, where her research is concerned with insurgent ideology and propaganda narratives – in particular their strategic use in information operations. Here, she is also a founding member of the Future Operations Research Group and part of the steering committee for the accompanying Women in Future Operations (WFO) platform – multi-disciplinary initiatives dedicated to harness diverse expertise and innovative thinking around the core research themes of: Future Urban and Unconventional Warfare, Emerging Flashpoints and Future Technologies.

Katja regularly publishes and presents at seminars and appears on national TV and radio for commentary. She is currently also teaching a post-graduate course on 'Terrorism and Propaganda in Cyberspace' for the Australian Graduate School of Policing and Security at Charles Sturt University.

Note: Jackson Pollock's masterpiece Convergence has provided the creative foundation for the overarching theme and title of this volume. Known for his eclectic painting style, Pollock is seen as a trailblazer for invention and free expression, admonishing us that "the modern painter cannot express his age, the airplane, the atom bomb, the radio, in the old forms of the Renaissance or any other past culture. Each age finds its own technique."[1]

Coming across this painting by chance when thinking of a way to conceptualize cyberspace, it stood out to me for its portrayal of complexity - yet underpinned by a harmony of sorts. This seemed a fitting frame for this topic, with the dynamics of complexity evident in Convergence speaking to the complexity inherent in cyberspace - a realm of converging and diverging forces and interests: technological, social, political, economic, institutional, cultural, ideational/ideological and strategic. As such, they co-exist, compete and act upon each other, forming a complex ecosystem of dynamic, interlinked threat and opportunity vectors.

Once I discovered the inscription provided by the Albright Knox Gallery, where the painting has its home, the parallel became even stronger: "for Pollock, the process of dripping, pouring, and splattering provided him with a combination of chance and control." [2]

The dialectic between chance and control are also at play in the realm of cyberspace – how we manage them is the puzzle we are asked to solve in our own age. And, taking inspiration from Pollock once more, it requires finding our own technique.

Jackson Pollock, Convergence 1952, oil on canvas
Collection Albright-Knox Art Gallery, Buffalo, New York (Gift of Seymour H. Knox, Jr., 1956)

"Civil liberty functions today in a changing technological context."

Ithiel de Sola Pool,
Technologies of Freedom (1984)[3]

Writing in 1983, well before what we now refer to as 'cyberspace' was conceived as such, MIT political scientist Ithiel de Sola Pool mapped out the coming technological landscape as one where "most published information will be disseminated electronically", with networked computers functioning as "the printing presses of the twenty-first century". This way, he forecast a convergence of once separate modes of communication - and the dangers inherent in such 'electronic hegemony' as he anticipated an erosion of civil liberties and freedom through heavy-handed government regulation.[4]

While Pool's vantage point is bounded to some extent by its time and place – in particular traditionally libertarian concerns - his framing of the challenges of the coming information age is still a useful entry point to understand how the accelerating, disruptive nature of technology and hyper-connectivity is giving rise to a new set of socio-political, economic and especially strategic challenges.

In the past infringements on citizens' freedoms through government overreach at the hands of surveillance agencies such as GCHQ or NSA were the main fear. Today the potential for control originates from a wider array of sources: fears of rival or adversarial actors that control large parts of the technology and communications infrastructure now run alongside concerns about excessive state power – both domestically and globally. Initially, a diffusion of technology and easier accessibility had given rise to hopeful expectations of the democratizing effects of increasing connectivity, empowering individuals vis-a-vis State power.[5] Yet, the increased reach of tech-savvy dictatorships, revisionist powers and violent extremist groups highlighted the dangers of our age, soon giving way to fears of new forms of oppression and violence: technology becoming a handy enabler of greater surveillance, control, and coercion – in particular giving asymmetric and revisionist actors a potential advantage over established democracies.[6]

Geopolitically, China's One Belt One Road Initiative, especially the concept of a Digital Silk Road is being recognized not only as an instrument for greater connectivity but as a deliberate strategy to exercise control.[7] Likewise, beginning with Russia's cyber-enabled interference in the 2016 American presidential election, Chinese and Russian attempts at influencing Western politics, media organizations, and certain segments of the population illustrate the prevalence of manipulating public opinion – increasingly being considered a key national security threat amongst liberal democracies.[8]

The geostrategic threat to liberal socio-political systems in the digital age is evidenced in the 5G debates playing out in Western democracies. Europe is a current prime example: pursuing a course of 'strategic autonomy',[9] it seeks independence from the US-China superpower rivalry which it perceives to be behind the American efforts to push other nations to exclude Huawei. For this end, the stance on Huawei becoming visible in Germany and other European countries at the time of writing appears to be one of attempted 'neutral' positioning, manifested in a reluctance to endanger economic partnerships with China.[10] Along those lines, the great power rivalry between the United States and China is often described as a 'new Cold War', in terms of

Writing in 1983, well before what we now refer to as 'cyberspace' was conceived as such, MIT political scientist Ithiel de Sola Pool mapped out the coming technological landscape as one where "most published information will be disseminated electronically", with networked computers functioning as "the printing presses of the twenty-first century".

a cyber or AI 'arms race'. Even though the accuracy and usefulness of such historical analogies are contested[11], it could be argued that their frequent use points to a recognition of the fundamental nature of these challenges: as digital technologies provide adversaries with unprecedented opportunities to undermine Western democratic, social, and market institution, these are not only security issues, but more fundamentally, debates about order and global governance.

These new governance challenges for States are also illustrated by the Islamic State's strategic use of communication technologies: leveraging the opportunities afforded by social media platforms, it managed to augment its reach and incite terrorist acts against the West in a more dispersed manner. Likewise, the Christchurch attack has served as a much-needed reminder that terrorists harnessing technology is not just the purview of jihadists. It points to a bigger problem-set of how cyberspace is enabling extremists of all persuasions to more easily disseminate their narratives, recruit und inspire/instruct terrorist acts.

These development result in a new set of challenges that come with regulating the online environment, such as the complexities of responsible encryption, how to deal with AI-enabled deep fakes and the manipulation of public opinion through the use of computational propaganda (so-called political bots).[12] As these quandaries bear out through governments' relationships with tech companies, they highlight the blurred boundaries that currently exist in terms of regulation and responsibility.

Here, new points of friction emerge as tech and media companies are asked by governments to monitor the content on their platforms to impede the dissemination of extremist content or misinformation. This move has been perceived as problematic, suggesting that government intelligence gathering is being outsourced to tech companies whose business model is inherently programmed for metrics-driven growth.[13]

In this context, Facebook's regulation of activities across its platforms along a yardstick of 'truth versus falsehood' raises questions about how objective the very act of determining what is 'true' can be.[14] Even with a revamped algorithm and fact-checking measures designed to fight the spread of fake news, critics argue that it easily enables and in fact incentivizes cognitive biases, especially in a contested and polarized information environment, it is important to factor in cognitive biases as well as political and economic when assessing metrics .[15]

At the same time, the thesis has been put forward that the only way for big tech corporations to continue dominating the market is by allowing a certain extent of government regulation, resulting in what some analysts imagine as a sort of 'power sharing agreement'.[16]

What these and similar arguments reveal are the blurred lines between the power of corporations, machines and the state, which have led to questions of where power and the ability to control truly lie and what we, as citizens can do about it.

As highlighted by the debate about the validity of Cold War analogies, it has become almost a cliché these days to argue that power politics take on a new form. Yet, the argument is useful one to examine in this context. Power politics are seen as having moved away from their traditionally narrow containment lines of State sovereignty and increasingly playing out on an expanded playground that is characterized by decentralized, shifting system of networks. This idea was for example expressed by Anne-Marie Slaughter in her The Chessboard and the Web: Strategies of Connection in a Networked World, where she argued that "states still exist and exercise power, but side by side with corporate, civic, and criminal actors enmeshed in a web of networks." [17] Such developments point to an increasingly symbiotic relationship between States' digital powers/measures and corporate data collection, giving rise to debates about who is in control in an era where data apparently reigns supreme - what some have called a 'dictatorship of data'[18] or, more specifically in regards to governments wanting to protect and control their information-related companies and infrastructure, 'data mercantilism'.[19] Similarly, Shoshana Zuboff, warning of the effects of what she calls surveillance capitalism, has coined the term "Instrumentarianism", a new power constellation of the digital revolution. This "new frontier of power" is said to result from the ability to commodify human experience into 'behavioral data', by means of analysing and measuring online human activity – with the end goal of manipulating and monetizing it.[20]

Appreciating these complexities accentuates what lies center of this shift: the tricky issue of in whose hands the responsibility of ensuring the balance between privacy, free speech, 'establishing truth' and national security ultimately ends up – and if the result is a world we want to live in, a world that still reflects its founding values.

Seeking to avoid technological determinism, answering the question of 'who is in control' needs to go beyond focusing on the power of corporations or how authoritarian regimes appropriate new technological advances for their own ends: it should also entail an inquiry into the fundamental societal and political dynamics and structures that enable such abuses – with an eye on our own societies and technology's potential to weaken democracies if left ungoverned and driven by market principles. This is based on the recognition that in a hyper-connected and highly networked world, technology enables individuals, civil society, non-state actors and institutions to impact on social and political agendas more than ever before.[21] As noted in a recent report, "across social media, people participate in the creation and spread of information, misinformation, and disinformation. Society is not shielded from geopolitics here. Rather society is, wittingly or unwittingly, a participant."[22] Consequently, human action is at the core of the information age still - enabled by technology but not determined by it.

This means more technology alone can also not be the answer to help us overcome the challenges resulting from this shift. Metrics are still driven by human biases. And, in looking for a solution, common descriptors such as 'fake news contagion' are often not helpful when they remain ill-defined; equally, recourse to a 'post-truth' era gives the impression little can be done to contain the spread of falsehoods or even establish, through critical inquiry, what is true and false.

Assessing the security landscape is therefore not just a matter of simple fact-checking and metrics: how we scale risks and security threats is ultimately a function of how we perceive the world and think it should be ordered. The evolution of any system in society demonstrates this: be they military, information, political, control, economic and cultural, systems are driven not by strategic thinking alone but also firmly rooted in beliefs systems and values.[23] This makes the above questions not only deeply political and strategic ones but inadvertently also about ethics.[24] What has been termed by some as a new paradigm of 'society-centric warfare' is useful for conceptualizing this: a conflict's centers of gravity as well as the end goals of operational and technical forces are ultimately rooted in society, making factors such as identity, perceptions, emotions and motivations or beliefs paramount.[25]

Accordingly, recognizing that society and individuals have an unprecedent role in an evolving global system of knowledge, power and authority is one thing. What's more important is to acknowledge that the matter is situated in an ideational/ethical sphere rather than being a mere outgrowth of instrumental rationality. Applying the conceptual lens of French sociologist Jacques Ellul can be instructive for understanding the discursive construction of today's information age. Ellul's analysis of the forces driving liberal technological societies reveals that democracy itself, meant as the prime vehicle for the free exchange of opinion and ideas, can became an empty myth when allowed to be driven by technocratic and commercial imperatives.[26]

This is not always recognized– and when it is, the overly normative, even ideological character of the debate often obscures the real complexity of the interconnected dynamics between security matters and values or ethics. One illustration for this is how the decline/erosion of Western dominance has become a frequent talking point – evident for instance in the Munich Security Conference's engagement with the concept of "Westlessness".[27] While seeking to diagnose the challenges of our time, this is a problematic lens on several levels: the principal issue being its reification of 'the West' as the original and exclusive home of progressive values, especially when presented in triumphalist tones.[28]

Nevertheless, it highlights an important element of the global political landscape: transcending immediate security concerns, debates have been elevated to a more existential level where the future of our order is framed and questioned in ideational terms. As global power shifts have given rise to competing models of governance/political order and the way data is governed impacts on our collective and individual freedom, these questions do need to be asked and pursued. But especially in an era of democratic disenchantment, it may be more useful to address them with more humility and less self-assuredness as we reflect on how its key tenets so they can carry us into the future. The Director of Military Sciences of the Royal United Sciences Institute for instance also noted "a belief in

Western conceptual or intellectual superiority remains deeply entrenched in the Western orthodoxy; such hubris has distinct dangers."[29]

Recourses to the shared foundation of Western values, reiterating their superiority are therefore not enough to tackle the complex problems of our time. For one, maintaining the openness and trust that should be the social fabric of our society and protecting it from compromise is not an outside problem. Consequently, lamenting "Westlessness" and issuing moralistic calls for restoring Western dominance do little to alleviate the problem. What these dilemmas and complex problem-sets can alert us to, however, is the importance of how we conceptualize and address such prickly challenges of sovereignty, governmental/institutional overreach, transparency and accountability for ourselves.

To return to the starting premise, complexity is inherent in not only the technical and logical layers that make up cyberspace, but also in how 'cyber' is embedded in the socio-political, cultural and geostrategic structures.[30] Hence, recognizing this complexity as emanating from the interconnectedness of dynamically driven elements within this human-centric space or system, means that responsive policy can only be made by grappling with social and ethical complexity, rather than wanting to reduce it. In an essay titled "When Truth Becomes a Commodity", Daniel Rogers highlights a process that pinpoints the core of this challenge

> *"As long as we can click on the truths we want, as long as truth is imagined as a desire satisfied in a politically and commercially saturated market, we will have a superabundance of facts that people hold as true.*
>
> *Everyone will get what he wants, and the public — and its trust in truth — will fall apart …*
>
> *… finding our way back to the notion of truth as the result of a public process of search and debate and deliberation will not be easy…above all, it will require a renewed commitment to truth's complexity and the processes by which one searches for it."*[30]

What makes this complexity emanating from the converge of forces a puzzle rather than just a tangle of non-linear causes and effects is therefore the end goal: working out and managing the relationship between these forces in a way that aligns with the bigger picture; ultimately, it is about making them converge in a manner that strengthens rather than undermines the foundations of liberal orders – both domestically and at the multilateral level. This is tricky.

Consequently, the convergence puzzle seeks to serve as a reminder of where the centre of gravity should lie in debates on cybersecurity: in a commitment to the core of the liberal project as its best defence mechanism. The challenge is finding out what this means practically, step by step and for each problem that presents itself.

Endnotes

1 As quoted in the Albright-Knox Collection, https://www.albrightknox.org/artworks/k19567-convergence

2 Ibid

3 Ithiel de Sola Pool, Technologies of Freedom (Harvard: Harvard University Press, 1984).

4 Robert Huckfield, "The 2016 Ithiel de Sola Pool Lecture: Interdependence, Communication, and Aggregation: Transforming Voters into Electorates", P.S: Politics and Science, Vol.50, No.1, January 2017, pp. 3-11.

5 Lucas Kello, The Virtual Weapon and International Order (Oxford: Oxford University Press 201, pp. 162-4).

6 See for example https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/; https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators; Cathy Downes, "Strategic Blind–Spots on Cyber Threats, Vectors and Campaigns." The Cyber Defense Review 3, no. 1 (2018): 79-104; www.jstor.org/stable/26427378

7 Nadège Rolland, China's Eurasian Century? Political and Strategic Implications of the Belt and Road Initiative, National Bureau of Asian Research, May 2017, http://www.nbr.org/publications/issue.aspx?id=346; or more recently: https://www.economist.com/special-report/2020/02/06/the-digital-side-of-the-belt-and-road-initiative-is-growing;

8 Aaron Friedberg, The Authoritarian Challenge: China, Russia and the Threat to the International Liberal Order (Tokyo: Sasakawa Peace Foundation, 2017), https://www.spf.org/jpus-j/img/investigation/The_Authoritarian_Challenge.pdf; Christopher Walker and Jessica Ludwig, "From Soft Power to Sharp Power: Rising Authoritarian Influence in a Democratic World" in Sharp Power: Rising Authoritarian Influence (Washington, DC: National Endowment for Democracy, 2017), https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/.

9 Ulrike Franke and Tara Varma, "Independence Play: Europe's Pursuit of Strategic Autonomy", European Council on Foreign Relations, July 2019: https://www.ecfr.eu/specials/scorecard/independence_play_europes_pursuit_of_strategic_autonomy

10 https://www.ifri.org/sites/default/files/atoms/files/etnc_report_us-china-europe_january_2020_complete.pdf

11 https://tnsr.org/roundtable/policy-roundtable-are-the-united-states-and-china-in-a-new-cold-war/#_ftn5

12 See for example Samantha Bradshaw and Philip N Howard, "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation", Computational Propaganda Research Project, University of Oxford, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf; or https://www.brookings.edu/blog/order-from-chaos/2018/05/25/the-west-is-ill-prepared-for-the-wave-of-deep-fakes-that-artificial-intelligence-could-unleash/; https://www.theatlantic.com/technology/archive/2020/01/future-politics-bots-drowning-out-humans/604489/

13 David Lyon, The Culture of Surveillance: Watching as a Way of Life (London: Polity Press, 2018);

14 This is especially the case when the search is one for direct causations between what happens on social media platforms and individual actions – which cannot be easily measured - rather than inquiries into the wider strategic consequences and shifts in the information ecology, see for example https://nymag.com/intelligencer/2018/12/how-much-of-the-internet-is-fake.html; Alicia Wanless et al., "How Do You Define a Problem Like Influence?, Journal of Information Warfare (2019) 18.3: 1-14; or https://nymag.com/intelligencer/2018/12/did-facebook-cause-the-yellow-vest-riots-in-france.html

15 https://www.niemanlab.org/2019/03/one-year-in-facebooks-big-algorithm-change-has-spurred-an-angry-fox-news-dominated-and-very-engaged-news-feed/; https://www.chronicle.com/article/How-Facebook-Stymies-Social/242090

16 https://www.bloomberg.com/opinion/articles/2019-03-13/what-if-google-and-the-government-merged

17 Anne-Marie Slaughter, The Chessboard and the Web: Strategies of Connection in a Networked World (New Haven: Yale University Press, 2017).

18 https://www.npr.org/sections/13.7/2018/02/28/589477976/biometric-data-and-the-rise-of-digital-dictatorship; https://www.brookings.edu/policy2020/bigideas/placing-a-visible-hand-on-the-digital-revolution/

19 Eric Rosenbach and Katherin Mansted, "Geopolitics of Information", Belfer Center for Science and International Affairs, Harvard Kennedy School, May 28 2019; https://www.belfercenter.org/publication/geopolitics-information

20 Shoshana Zuboff, The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power (New York: Public Affairs, 2019).

21 Thomas Rid and Marc Hecker (2009), War 2.0: Irregular Warfare in the Information Age. Westport: Praeger Security International; Ofer Fridman, Vitaly Kabernik and James C. Pearce (eds.) (2018), Hybrid Conflicts and Information Warfare: New Labels, Old Politics. Boulder and London: Lynne Rienner.

22 https://www.lowyinstitute.org/the-interpreter/muddled-message-makes-harder-australias-friends-trust-us

23 Cecilia Andrews & Edward Lewis (2006), "Simulating Complexity-Based Ethics for Crucial Decision-Making in Counter Terrorism" in H Nemati (ed.) Information Security and Ethics: Concepts, Methodologies, Tools and Applications, p. 3250. Hershey, PA: Information Science Reference (an Imprint of IGI Global)

24 See Luciano Floridi, The Fourth Revolution: How the Infosphere is Reshaping Human Reality (Oxford: Oxford University Press, 2014)

25 Emile Simpson, War from the Ground Up: Twenty-First-Century Combat as Politics (New York: Oxford University Press, 2013); Ariel E. Levite and Jonathan (Yoni) Shimshoni, "The Strategic Challenge of Society-centric Warfare", Survival, 60:6 (2018), 91-118 DOI: 10.1080/00396338.2018.1542806 ;

Rupert Smith, The Utility of Force: The Art of War in the Modern World (New York: Alfred A. Knopf, 2005); Scales, R. (2006, July). Clausewitz and World War IV. Armed Forces Journal, 16–24, 48.

26 See for example Karim H Karim, "Cyber-Utopia and the Myth of Paradise: Using Jacques Ellul's Work on Propaganda to Analyze Information Society Rhetoric", Information, Communication and Society, 4:1 (2001), pp. 113-134

27 https://securityconference.org/en/publications/munich-security-report-2020/

28 US Secretary of State Pompeo's pompous 'The West is Winning' speech being a case in point

https://www.voanews.com/europe/west-winning-pompeo-tells-china-russia

29 Peter Roberts, "Designing Conceptual Failure in Warfare", The RUSI Journal, 162:1(2017), 14-23, DOI: 10.1080/03071847.2017.130151

30 https://www.chronicle.com/article/When-Truth-Becomes-a-Commodity/238866?cid=RCPACKAGE

REFLECTION

Cyber: Emerging Themes and Reflections

Prof Lesley Seebeck, Inaugural Chief Executive Officer of the Cyber Institute, Professor in the Practice of Cyber Security, Australian National University.

August 2019

About the Author

Professor Lesley Seebeck started as the CEO of the Cyber Institute, Australian National University, on 30 July 2018. Most recently, she was Chief Investment and Advisory Officer at the Digital Transformation Agency, arriving there from the Bureau of Meteorology where she served as Chief Information Officer from mid 2014 to late 2017. In March 2017, she was recognised as Federal Government CIO of the Year.

Professor Seebeck has extensive experience in strategy, policy, management, budget, information technology and research roles in the Australian Public Service, industry and academia. She has worked in the Departments of Finance, Defence, and the Prime Minister and Cabinet, the Office of National Assessments, and as an IT and management consultant in private industry, and at two universities.

Professor Seebeck has a PhD in information technology, an MBA, a Masters in Defence Studies and a Bachelor's degree in Applied Science (Physics).

The following forms initial reflections of my recent visit to Berlin and Brussels, as part of an Australian delegation sponsored through the Konrad Adenauer Foundation (KAS), and the questions our discussions subsequently raised in my own mind. I am grateful to KAS for the opportunity to engage with senior counterparts in Germany and the broader European security and economic organisations.

We've come a long way in the 30 years since the Morris worm, considered the first major attack on the internet—and not in an overwhelmingly positive direction. Cyber security is now part of any conversation about national security, economic certainty and societal well-being. And in those discussions, there are a number of common themes that lead to larger questions around cyber.

The increasing pressure on—and sense of urgency within—states to increase their cyber defences is quite evident. States typically have responded as we would expect. Government is reorganised, with new agencies emerging either as new constructs or agglomerations of the old. More often than not, they are based on or around existing security organisations, and so take on much of their progenitors' culture and worldview.

Governments also rely heavily on legislation and regulation: tools of the state. Yet legislation is tedious, slow and too often a blunt instrument, especially in new fields where the nation-state has little understanding or penetration. Good legislation takes time: concepts need to be tested; the community should be engaged and diversity of views canvassed; consequences should be fully understood and appreciated; and, critically, assumptions should be tested. While such due diligence may not be possible—especially a full appreciation of unintended consequences—it's clear that legislation rushed through in a hurry, often in response to a crisis or political pressure, rarely qualifies as good law. And poor outcomes that may have otherwise been foreseen with more forethought and caution don't merely degrade capability, they undermine trust and condemn government to a 'whack-a-mole' approach to cyber- and technology-triggered issues.

Similarly, many of the programs supported by governments reflect an internal consensus view of the problems and the skills needed to resolve a problem. Moreover, they seek to stabilise and to return to a known and understood norm. In a fast-changing world, that's less than optimal. There's a reluctance to think differently about the problem, or about how technology, society, economic drivers and the geostrategic situation may all co-evolve and fundamentally change the environment.

As a result, much of government support in cyber tends to focus on a narrow technical skill base, rather than a diversity of skills and conceptual frameworks. Proposed solutions are all too quickly reduced to a technical issue, to be resolved by technical staff with generally inadequate funds. But cyber is much more than the technology.

Those conversations mentioned above rarely touch on the technology itself. And so the deep, challenging and desperately-needed discussions about adaptation and transformation are avoided.

So it's little surprise that many of the prescribed solutions and funding aren't really hitting the mark. In some cases, that's a function of time: it takes years to educate and season graduates, for example. Government itself prefers to move slowly—and the consensus provisions required by the EU and NATO underline that preference.

There is a sense, too, that the pace of technological change and social disruption is leaving governments behind. Liberal democratic states, with rules of law, democratic processes, etc, feel increasingly vulnerable.

In contrast, illiberal and authoritarian regimes have fewer concerns about accountability and fewer qualms about using—and simply taking—technology to meet their goals, sometimes recklessly. They have also grasped, quickly and ruthlessly, the use of technology for control and suppression, just as they have understood the existential threats posed by those same technologies.

The temptation for liberal, democratic governments, is to mimic behaviours of their opponents: exerting increasing controls on their populations, decreasing transparency, and increasing means of access to the private lives and communications of citizens. Often those are incremental changes. But we should not forget is that while the changes may seem incremental, the powers and intrusiveness of the technologies, and the data collected, is increasing exponentially. As this data increases, we have tools to process it that mean that a small number of data points easily identifies individuals, even when data is de-identified. Privacy—a fundamental human need, often requiring anonymity—struggles and needs to be actively bolstered.

Continental European sensibility to such matters differs somewhat to the Anglophone world, possibly reflecting closer experience with the capriciousness and harms of authoritarian regimes. European data protection and privacy provisions offer a safeguard against over-reach, but it's not inconceivable that even European governments will bow to pressure to compromise on individual rights. Indeed, despite the EU's efforts to build consensus frameworks, those same frameworks offer sufficient scope to allow a range of behaviours and approaches across the EU.

Such diversity is good, inasmuch it is proving challenging for our governments and societies, in the West, to understand, anticipate and manage the changes being wrought on our societies by technologies and social and economic disruption.

Those challenges will increase, and the nature of current information technologies—which the West is largely responsible for creating—is such that attack is easier than defence, that tracking is easier than hiding, that replication is easier than destruction, that ambiguity is easier than integrity, and that contamination is easier than purity.

Because Western governments have had difficulty coming to terms with those fundamental changes to the economy and society, their conceptual models, and means of acting on the world are misaligned. Moreover, years of focusing on efficiencies in government, and the transfer of functions to the private sector, either as a deliberate policy (for example, the privatisation of critical infrastructure, or outsourcing of technical skills) or by being overtaken (the uptake of platforms for interaction or the democratisation of, for example,

cyber tools) have weakened government's own capacity to act.

In contrast, the scope, reach, scale and ability to act on the concerns of states—their economics, societies and security—are now available to private companies—Google, Facebook, Ali Baba, Weibo, Tencent, and others.

Where does that lead us?

First, I would suggest that there remains strength in liberal, democratic values, institutions and behaviours. They should not be discarded, and indeed should be upheld and promoted even more strongly. But they will need to be re-interpreted in this new, digital, data-heavy environment. To that end, the European efforts to protect privacy and the ownership of their own data by individuals are steps in the right direction—but only first steps.

We should not mis-interpret the nature and actions of authoritarian societies as meaning that they are inherently stronger, faster or better. Certainly, a control-heavy approach may generate short-term gains. But those controls make their society, and security, more brittle, less resilient, less adaptable and less capable over the longer-term. Fear does not create or sustain creativity, nor the questioning inherent to scientific activity, nor help build the trust that underpins healthy societies, economies or institutions.

Europe has a close acquaintance with the nature and consequence of societies that can be destroyed or created by fear. So—second—Western liberal democracies need to support the open spirit of inquiry, diversity of thought, and willingness to contest opinions, assumptions and authority that are their strengths. As Henry Farrell and Bruce Schneier argue[1], we have to be smart about how we secure open information flows and manage, dynamically, political stability, so that they benefit democracy.

There is much to share between Europe and Australia. And efforts such as those promoted by the Konrad Adenauer Foundation, including the exchange of ideas and experiences, are integral to that broader effort.

A third point. States are finding themselves on the defensive—and falling further behind. That's generated considerable concern in the business community. And so interest in counter-attacks and vigilante policies such as 'hacking back' are understandable: decision-makers are running out of options and businesses are frustrated with the inability of governments to provide a safe space for operations.

Failure to address those concerns will undermine the legitimacy of government, and of economic stability. Current efforts are falling short, and the direction of many policies in terms of simply constraining activities or undermining broader security exacerbates the problem; we need to start thinking differently about how to resolve those issues.

Fourth, we need better conceptual models around cyber in the geo-strategic context. Tropes such as 'cyber as nuclear', and even 'cyber as the fifth domain', fall short of the reality of technologies densely embedded in evolving civilian contexts. They also evoke unhelpful scenarios and reactions—especially the cyber-as-nuclear analogy.

Warfare has typically been a matter for states—at least since the Peace of Westphalia. But cyber offers means of coercion, control, and disruption that may be both deniable and available to actors other than nation-states.

Just as Mahan found that few of Jomini's principles of war on land were applicable to sea, we should not expect a direct translation of existing concepts and doctrines into the cyber world. There are no heartlands here, as per Mackinder, nor rimlands, as per Spykman, at least that translate easily in the physical sense. Clausewitz's centres of gravity are diffused and changeable, though cyber is no less a political issue than any other use of force. Vauban's fortresses won't help here; counter-insurgency may offer some insights into the dynamic interplay of populations and politics. In no other—forgive the term—domain do both protagonists and bystanders constantly change the shape of the contested environment as they work, play, build, steal and corrupt.

Finally, time in Europe and more recently in Asia, has left me with some reflections specifically on Australia. Australia has the opportunity to recreate itself and its positioning in this new digital world. It has an educated and multicultural population, offering the benefits accruing to diversity, it can build on the density of its urban centres while also taking advantage of its vast distances and resources, and it has a reasonably stable political system that advocates meritocracy, transparency, accountability, the role of the individual and the rule of law.

All this means that we cannot easily reduce the challenges presented by cyber, or digital disruption, to a mere technology issue – as much as governments, perhaps understandably, would like to do so. We need to foreswear hastiness, and to move with greater deliberation: there's much to be gained from a more patient and careful response, not least a deeper understanding of the issues and greater scope to bring people on board. We need to embrace and encourage the diversity we have in our community—we know that cognitive diversity in groups yields better decisions. And we should avoid the temptation of continuously yielding to a single controlling voice. Such voices prevail by firepower. And under fire, a unit will scatter, then regroup, adaptively—just as in nature.

Nor is cyber simply about security. Cyber is about adaptiveness, and resilience. Doing cyber well means strategy, not simply security. Strategy emphasises the proactive; security the reactive. Cyber is fundamentally about the world we want to live in, the societies we want our children to grow up in, the nature of economic growth, and the nature of fundamental human rights and the values we hold dear. And that means contemplating deeply what those values are, and reflecting them through the people we educate, the institutions we shape, and the elections we run to ensure that they are, in turn, reflected by those we elect as our representatives.

Endnote

1 https://bostonreview.net/forum-henry-farrell-bruce-schneier-democracys-dilemma

REFLECTION

Reflections on a Cyber Study Tour

Fergus Hanson, Director International Cyber Policy Centre at the Australian Strategic Policy Institute

October 2019

About the Author

Fergus Hanson is the Director of the International Cyber Policy Centre. He is the author of 'Internet Wars' and has published widely on a range of cyber and foreign policy topics. He was a Visiting Fellow at the Brookings Institution and a Professional Fulbright Scholar based at Georgetown University working on the uptake of new technologies by the US government.

He has worked for the UN, as a Program Director at the Lowy Institute and served as a diplomat at the Australian Embassy in The Hague.

While working for philanthropist Andrew Forrest he led the establishment of the Freedom Fund in London and the Global Fund to End Modern Slavery in Washington D.C. He has been a Fellow at Cambridge University's Lauterpacht Research Centre for International Law and the Centre for Strategic and International Studies, Pacific Forum. He is a member of the board of directors of the Catherine Hamlin Fistula Foundation and Art Monthly Australasia. He is an Advisory Board member of the Cyber Peace Institute in Geneva.

Living in Australia at the epicentre of the most serious geopolitical upheaval since the Cold War focusses the mind. Sometimes too much. As China rises and President Xi Jinping pursues an increasingly assertive foreign policy, states in the region are feeling the pinch. Suddenly, 'win–win' has been replaced with the militarisation of the South China Sea, the arbitrary arrest of foreign civilians as punishment for hurt feelings and economic coercion to bully smaller states into submission.

For those living in the Indo-Pacific, the shift in posture is now part of our everyday reality. But for a while it seemed like the rest of the world thought this might just be a regional problem that did not concern them.

A deep dive with German and European Union policy makers, business leaders and officials suggested if this was ever the case, it is no longer the dominant view. On the other side of the world China's ambitions are increasingly being viewed as global, with consequential implications for policy-making. One notable example was in the area of intellectual property, of which Germany has much. After years of its theft, German industry has begun to step up its public response.

A leading force in this change has been Germany industry itself. Doing away with a previously cautious approach that favoured quiet diplomacy over telling it like it is, Germany's peak industry group, BDI, characterised the relationship with China bluntly: "systemic competition." It also urged German firms to "keep an eye on the possible risks of a commitment in China".

This stepped-up concern with some of the Communist Party's more negative actions has spread to the European Union where there are early indications the implications of China's actions are also being considered through a more strategic lens. It recently labelled China a "systemic rival" and critiqued Italy for its engagement in the One Belt One Road initiative. For the machinery of Brussels this was bold stuff. It also reflected the success of German industry in moving this to a multilateral issue that the whole EU can tackle.

Listening to discussions in Europe was a little like déjà vu – many of the issues like whether to let high risk vendors build your most important piece of critical infrastructure – had already been debated and resolved in Australia. But there were also noticeable differences in the debates in Australia and Germany. Discussions in Germany, with its powerhouse manufacturing, focussed much more sharply on the theft of intellectual property. And while in Australia foreign interference is rife and is widely debated, Germany's geographical distance from China (and perhaps its language) means foreign interference is much less of a concern (although not from Russia).

This difference of experience and stages of decision making opens up strong opportunities for deepening an already strong two-way dialogue. Around the world China has largely succeeded up until now in ensuring issues are dealt with bilaterally where it is easier for it to get its way. With the issue

There is significant scope to expand the number of issues that states like Germany and Australia could collaborate on when it comes to China. The theft of intellectual property and 5G are great places to start. But there will inevitably be more as China continues to pursue its ambition to be a global power that weighs as heavily on Europe as it already does in Asia.

of intellectual property theft things briefly turned the other way, with the US leading a global effort to put this issue on the agenda of multilateral groups like the G20.

There is significant scope to expand the number of issues that states like Germany and Australia could collaborate on when it comes to China. The theft of intellectual property and 5G are great places to start. But there will inevitably be more as China continues to pursue its ambition to be a global power that weighs as heavily on Europe as it already does in Asia.

The KAS-sponsored visit to Germany and Brussels was a wonderful opportunity to hear first hand how Germans and EU officials are seeing the rise of China. While there are still marked differences, the trend is very clear. Everyone is starting to reassess China's trajectory and its willingness to play by the accepted rules. There is much that liked-minded states could do to ensure the rules-based order is protected and strengthened through this tumultuous period.

ANALYSIS

Germany's Responses to Large Scale Malicious Cyber Incidents and Opportunities for AUS–GER future cooperation

Julia Schuetze, Project Manager Stiftung Neue Verantwortung, Berlin

November 2019

About the Author

Julia Schuetze is the Project Manager for International Cyber Security Policy at Stiftung Neue Verantwortung e.V. Her research focus is on joint responses to malicious cyber activities, specifically on cyber diplomacy of the European Union with the United States and Japan as part of the EU Cyber Direct project. She is a Cybersecurity Policy Fellow at New America Foundation. She has organized several workshops and events with cybersecurity experts from the U.S., EU, Japan and Germany in Washington D.C., Berlin and Tokyo to enhance international cooperation on cybersecurity. Prior to SNV, she worked at Wikimedia Deutschland e.V. and has researched at the Berkman Klein Center at Harvard University. She holds the Euromaster Transatlantic Track degree from University of Bath with stops at UW Seattle and HU Berlin. Her bachelor thesis at the University of Stirling, 'Germany's cyber security awareness programme: Lessons from the US', was tutored by the German Federal Office for Information Security (BSI). She was also an intern at the Washington DC office of the Konrad-Adenauer-Foundation in 2014.

Large scale malicious cyber incidents have been on the rise. Classified as such are malicious activities with "significant impact[1]" that seek to undermine political integrity, national security and economic competitiveness, with the eventual risk of conflict.

Germany's Federal Office for Information Security (BSI) brings out a report about the state of IT-security every year. In 2019[2] it presented a threat situation affecting Germany, highlighting the increased risk of such large scale malicious activities that mirror two of the most consequential cyber incidents of 2017 WannaCry and NotPetya. Take NotPetya, a Ransomware attack[3] that exploited a widespread vulnerability in Microsoft affecting countries around the world and caused huge financial damage globally[4] and impacted Germany and Australia[5]. Since then, as BSI highlights in its 2019 report, more vulnerabilities were discovered, such as in a widely used chip hardware[6]. Ransomware attacks are still on the rise, a new form called Emotet has already affected German businesses and cities, halting services and production[7]. Moreover, digitalisation and digital dependability increase the effects of large scale attacks and widespread vulnerabilities. The effects are made worse due to the automation of attacks and therefore they could spread even more quickly globally and create massive economic damage; or in case of autonomous driving or attacks on medical devices, risk the health of people[8]. Moreover, the wider use of AI as a technology also bears new risks as AI can be hacked and has its own unique vulnerabilities[9].

Recognizing this threat landscape, governments have found different answers to respond to large scale malicious cyber activities, such as NotPetya. Most governments focus on the one hand on addressing the vulnerabilities and aim to increase resilience and cybersecurity, so those incidents cannot cause that much damage. On the other hand, governments are trying different strategies to influence the behavior of threat actors to punish them or prevent them from executing such incidents in the first place. The discussion on responses to malicious cyber activities spans the whole field of cybersecurity policy and becomes more and more part of the traditional security and foreign policy debates. This is because governments use a whole range of different policy instruments (military, regulatory, financial, technical, organizational and diplomatic) to respond to malicious cyber activities. Countries cannot do this in silos. Especially threats and vulnerabilities that cause large scale incidents, like NotPetya are global and therefore affect the cybersecurity of many countries. Accordingly, the global cybersecurity environment can be strengthened or weakened by actions taken by other governments. It can be weakened, for example if governments are using cyberspace as a means to achieve strategic geopolitical goals, such as damaging another country through a cyber attack as was found to be the case with NotPeyta[10]. This can weaken cybersecurity globally, since the vulnerabilities that are exploited for such an attack are in soft- and hardware that is used worldwide and thus

makes other actors vulnerable. Moreover, if attacks are not targeted or executed as a targeted attack, the attack can spread quickly on its own, as was the case in NotPetya, soon affecting many businesses and public services in other countries. The global cybersecurity environment can however also be strengthened through international cooperation. For example, countries can assist each other in becoming resilient by sharing information about a threat quickly, working across borders with businesses on closing vulnerabilities that could be exploited for an attack. Those are just a few of the examples why it is important to think about the cybersecurity challenge with an international perspective.

Most countries therefore have by now set up a cybersecurity strategy that includes their international engagements and guides actions taken for cybersecurity or in cyberspace (see Australia, USA, Japan).

Understanding Germany's responses to large-scale malicious activities allows us to identify how Germany could work together with Australia as the strategic goals governments pursue as well as the policy instruments that they are using can offer opportunities and challenges for cooperation affecting bilateral and multilateral relations with other governments and international organisations.

The difference in the Australian and German government responses to malicious cyber activities can be best highlighted in the NotPetya incident that triggered many different political and especially foreign policy responses. Although both countries were affected, their foreign policy responses differed. This paper will examine Germany's responses (and how it does not respond) in comparison to other countries when it comes to large scale attacks like NotPetya. The focus of the analysis is Germany's domestic architecture[11] as well as the operational and foreign policy responses taken individually and jointly with other countries. Looking at this closer improves the understanding of what Germany's approach to cybersecurity is and its measures taken in case of a large scale cyber incident. It will moreover show some divergences to Australian responses but also opportunities for future cooperation with Australia.

Germany's responses to large scale malicious cyber activities

Germany takes a whole of government approach. This means that almost every federal governmental actor has some role in Germany's cybersecurity architecture[12]. The Federal Office for Information Security (BSI), responsible for Germany's IT-Security, specifically aims to complement this approach with a whole-of-society approach as a form of governance that engages the private sector, civil society, communities and individuals through different actions, such as information platforms or institutional dialogues. In the BSI's case, this approach was chosen to strengthen resilience and increase it-security for society and businesses more broadly.

When looking at the German government's responses to large scale malicious cyber activities, such as NotPetya in 2017, the main government agency at the centre of Germany's cybersecurity architecture, the **Federal Office for Information Security (BSI) is first and foremost responsible for the prevention and operational response of such large scale incidents**. To prevent large scale malicious cyber activities the German government focuses on the protection of critical infrastructure as well as government agencies' IT. This resulted in a regulatory response by implementing

the IT Security Legislation[13] which demands a certain **set of standards and reporting mechanisms by critical infrastructure providers**. In order to facilitate a close and trustworthy relationship with its core stakeholder groups, such as businesses and governmental agencies, the BSI uses an **institutionalized dialogue** in the form of a public private partnership, the Alliance for Cybersecurity (AfCS/ACS). The AfCS is a network to share information on threats and protection mechanisms. In the case of NotPetya, BSI shared warnings and information on how to handle such an incident publicly as well as targeted by the AfCS[14]. It also does this preventatively as can be seen in a recent example when the BSI sent out a warning about the hardware chip vulnerability to all members of the Alliance for Cybersecurity and gave instructions for protection[15]. Ideally, this is to prevent the success of a large scale malicious activity that could use this vulnerability.

Another important element of Germany's response structure is the **National IT Situation Center (LZ) situated in BSI that is tasked to create an analysis of the threat environment for Germany and evaluate cyber incidents for state and private sector entities 24/7**. In a situation where an incident occurs experts at LZ react and distribute their analysis accordingly. In case of a large scale malicious activity, the LZ can become a crisis center. BSI may also gather and distribute information **via their Computer Emergency Response Teams or Mobile Incident Response Team that** in some very special cases may also provide technical assistance on the ground. For NotPetya and other larger incidents, another institution becomes very important for mitigating and reacting to the incident - the **Cyber Defense Center (NCAZ/ Cyber-AZ)**. It is housed by BSI but includes other government agencies, such as the federal police, the intelligence services, the armed forces -- mainly aiming to ensure a whole-of-government approach in operational response. Hence if a cyber threat occurs it is the place where the **operational response among different governmental bodies is coordinated**. Any information about the incident would be accumulated there and every government body represented would take appropriate steps, such as investigation, information gathering, technical assistance. This also occurred during the NotPetya incident[16].

Germany works with international partners on prevention of large scale incidents. For example since NotPetya the German BSI has published together with its counterpart in France, the National Cybersecurity Agency of France (ANSSI), a **common situational picture** that aims to inform the public but also helps the two countries be **better prepared and learn from each other**. It goes way beyond just information sharing. Such joint technical analysis can build a common understanding of threats and may be used by policymakers as a tool to inform their political analysis of the situation and ultimately the responses taken jointly. In their own words, the press statement reads as follows: "Both agencies agree that the threat situation concerning Ransomware is still alarming" and further it states "the impact, however is different in France and Germany, especially regarding global WannaCry and NotPetya ransomware campaigns in 2017. These different experiences regarding the consequences of the same attacks in the two countries emphasize the need to cooperate even closer, e.g. sharing information and jointly analysing cyber threats."[17] Hence joint technical analysis is used in response to large scale incidents with the aim to prevent and learn from other governments.

Due to the rise of cyber incidents despite the development of norms, the European Union has established a set of response mechanisms, including most prominently the so-called EU Cyber Diplomacy Toolbox which Germany supported through the Council decision adopted in June 2017.

Looking specifically at Germany's foreign policy responses, its engagement and diplomatic efforts on cybersecurity, is centred traditionally around developing norms to increase the stability of cyberspace, freedom of expression and building capacity in other countries. For this, the German Federal Foreign Office (AA) created an International Cyber Policy Coordination Staff in 2011[18]. The AA is also involved in the German Cybersecurity Council that governs Germanys' strategy. Notably, the AA is not part of the Cyber Defense Center (Cyber-AZ) and thus has no part in the operational response in a large scale incident, like NotPetya. It rather aims to **prevent a large scale incident and increase the stability of cyberspace**, by engaging in **international fora for norm building, such as United National Group of Governmental Experts (UNGGE) and the Open Ended Working Group on Cyber Norms (OEWG)**. This foreign policy response is done jointly with other countries, for example since 2012 in strategic cooperation with Australia noted in the Berlin-Canberra Declaration of Intent on a Strategic Partnership where it states in Article 11: "Australia and Germany underline the importance of the Internet's security, its freedom and its potential for development, and share the view that there should be an appropriate balance between cyber security and access to information, freedom of expression and the protection of privacy. With a view to developing norms of state behaviour and confidence and security building measures for cyberspace, they will work closely together in international forums, particularly in the UN Group of Governmental Experts."[19] Hence, the foreign office's work has thus far mostly concentrated on prevention of large scale cyber incidents through norms in coordination with other countries.

Due to the rise of cyber incidents despite the development of norms, the European Union has established a set of response mechanisms, including most prominently the so-called EU Cyber Diplomacy Toolbox which Germany supported through the Council decision adopted in June 2017[20]. The EU Cyber Diplomacy Toolbox includes measures suitable for an immediate response to incidents as well as elements to encourage cooperation, facilitate the mitigation of immediate and long-term threats, and influence the behavior of potential aggressors in the long term. These measures range from diplomatic and political to economic actions to prevent, detect or react to malicious cyber activities, including those that do not rise to the level of internationally 'wrongful acts' but are considered as 'unfriendly acts'. This toolbox includes foreign policy tools including restrictive measures. Importantly, all those responses can only be implemented if all member states agree. With reference to

NotPetya, the Council passed the following conclusion[21] that Germany supported. The conclusion reads: "The EU firmly condemns the malicious use of information and communications technologies (ICTs), including in Wannacry and NotPetya, which have caused significant damage and economic loss in the EU and beyond. Such incidents are destabilizing cyberspace as well as the physical world since they can be easily misperceived and could trigger cascading events".

Because getting all member states to agree is not the easiest task, countries have also chosen bilateral and multilateral coordinated or joint responses. Joint responses can be defined as an action that two or more countries take together in order to prevent, detect or react to malicious cyber activities including diplomatic instruments. A joint response to a specific threat or vulnerability or major incident includes the implementation of policy instruments. Here, beyond the European Union - level response to NotPetya, there are more and more responses by 'coalitions of the willing and capable' in reaction to major incidents where countries that agree to take further join together. Germany has so far not taken joint or coordinated bi- or multilateral responses in reaction to a major incident beyond supporting the EU Council's decision. Examples of a coordinated response by a coalition of the willing and capable was seen, most prominently after NotPetya, where Australia led a coordinated attribution effort. In February 2018, within days of each other, seven nations including Australia attributed the NotPetya cyber attacks to Russia. It was no coincidence, according to Australia's Ambassador for Cyber Affairs, Dr Tobias Feakin that "[NotPetya] represented the largest coordinated attribution of its kind to date," Feakin he said in April 2018 at the Australian Cyber Security Centre (ACSC) Conference in Canberra[22]. The governments of the US, the UK, Denmark, Lithuania, Estonia, Canada, and Australia called out Russia in official statements. Official statements of support came from New Zealand, Norway, Latvia, Sweden, and Finland. "That had followed also an additional coordinated calling-out of DPRK [North Korea] as responsible for the WannaCry incident," Feakin said[23]. Germany did not join this coordinated attribution effort and there was also no official attribution by the German government individually done before or after the coordinated attribution. The German government was criticized in a news article for this as Handelsblatt had learned that the White House had shared confidential insights into the attack's origins with German intelligence. A German government spokesman said the administration confined its statements on intelligence matters to the "responsible secret bodies of the German Bundestag"[24].

The German government has so far not been on the forefront of attribution. The only public attribution after a cyber incident was done by the Minister of Foreign Affairs in a press statement about the expulsion of Russian diplomats due to Scripal incident, an effort led by the United Kingdom. Here the Minister of Foreign Affairs added that the expulsion was also done due to the cyber incident that affected the foreign office in 2018, saying that it was most likely Russian actors that were responsible for the incident[25]. This was not a large scale cyber incident like NotPetya but a targeted attack infiltrating the foreign office. Public attribution to Russia had also been done frequently by the former Head of Germany's Domestic Intelligence[26]. However, it can be disputed whether this is an actual public attribution by the German

government as it was only communicated through media channels by himself and followed up by or embedded in embedded in other political actions or in a foreign policy approach towards Russia in an official German government statement.

Conclusion: Germany's responses to large scale malicious cyber incidents

Thus when it comes to foreign policy cooperation in reaction to a large scale incident, Germany is not cooperating openly or using the same response as Australia which has attributed frequently and is heading an international deterrence strategy right now. The German government, through its responses focuses mostly on prevention of large - scale cyber incidents and therefore its cooperation with other countries appears to be centred on that, too. Germany's foreign policy approach is still focusing on norms-building. Cyber incidents are not yet addressed as part of a broader foreign policy or security policy towards a country, for example with Russia. Germany has not yet published a cyber diplomacy strategy that would include or signal the use of diplomatic instruments as a response to cyber incidents. In case of non-existence of such a strategy, this may explain why Germany is not using diplomatic instruments, such as attribution, sanctions and more in response to a large scale incident. Therefore, Germany is not joining bilateral or multilateral cooperation to respond yet, like the coordinated attribution effort led by Australia. Strategically this could prove difficult in a world where cyber incidents are increasingly becoming part of broader geopolitical conflicts and are used as just another tool by some countries to undermine other countries' economies, national security and political integrity[27]. Unlike Germany's well-developed operational response which are also done together with other countries, like the join technical analysis that BSI and ANSSI put out, using other responses that are more political are underdeveloped. This is even more confusing in light of current debates on the use of offensive cyber means for defensive purposes, so-called active cyber defense, and attribution in Germany[28]. Without a clear international strategy that installs Germany's approach to cybersecurity and specific cybersecurity goals within its broader foreign and security policy goals, it would make the implementation and signalling of use of those instruments very unpredictable for like-minded governments and bad actors alike.

Opportunities for AUS-GER future cooperation

Taking into account the current state of Germany's responses to large scale incidents, there are three opportunities that emerge for further cooperation among Australia and Germany.

1. Firstly, Germany and Australia should **continue the dialogue on responses as it would help the understanding of options that are available to Germany and Australia** and will increase the awareness about under what conditions Germany may respond on EU level or on its own or potentially join a coalition of countries. This could help to coordinate responses in the future.
2. Secondly, Germany and Australia could **focus on threat analysis to prevent large scale cyber incidents.** Here both could learn from each other. starting with a common concern and common goal can assist in identifying options of closer cooperation. A specific common concern is for example threats to critical

infrastructure, and more specifically threats from cyberspace that could halt the successful implementation of energy transition that both countries have in common. In Australia, renewable energy is growing at a per capita rate ten times faster than the world average. The next fastest country is Germany[29]. The assumption made by the German government that energy transition "means that access to them is less likely to lead to conflicts[30]" and further that "it will also be more difficult for states to use energy sources to exert pressure" should be discussed again taking into account the unique vulnerabilities that renewable energy systems have[31] and that in general energy infrastructures are becoming increasingly the target of cyber attacks[32]. Since Germany and Australia have an interest in a successful energy transition, a common goal could be to address the cybersecurity implications in this context and analyse specifically threats to energy transition and evaluate what responses may be useful to mitigate them.

3. Thirdly, Germany and Australia should start **working together not just on norm development but on norm implementation and aim to support global governance cooperation platforms to achieve the implementation of norms**. Many norms have been/are being developed in different fora. For example the UN established two intergovernmental processes on cybersecurity – the Open Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, and the sixth Group of Governmental Experts (GGE) on developments in the field of information and telecommunications in the context of international security. Germany and Australia are members of both groups. Then multi-stakeholder initiatives, such as the Global Commission on the Stability of Cyberspace (GCSC) recently launched its final report, which offers a cyber stability framework, principles, norms of behaviour, and recommendations for the international community and wider ecosystem. Further there is the Paris Call for trust and security in cyberspace that was signed by Germany and Australia. What is necessary now, is an initiative that oversees the implementation of norms worldwide and identifies actions to ensure norm implementation. As both countries support the multistakeholder approach to internet governance, a pledge to support a global digital cooperation architecture as a way to support norm implementation could aid bringing stakeholders together. The High-level Panel on Digital Cooperation was convened by the UN Secretary-General to advance proposals to strengthen cooperation in the digital space. Three ways of achieving this goal were proposed in the report and are now being further developed and discussed worldwide. All have strengths and weaknesses as a German multi-stakeholder group has identified in a workshop in October 2019[33]. The Australian government put out a public statement commenting on the recommendations[34]. A beneficial next step for norm implementation could be to use those two discussions, one on digital cooperation architecture and one on norms for cyberspace and identify what sort of architecture Australia and Germany would pledge to support to implement norms or develop norms further.

Endnotes

1 EU definition that governs the implementation of EU Cyber Diplomacy toolbox that Germany passed in Council with all other member states. Council of the European Union (2019) Cyber-attacks: Council is now able to impose sanctions

2 BSI (2019) Die Lage der IT-Sicherheit in Deutschland 2019

3 Greenberg (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History

4 Greenberg (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History

5 BSI (2017) Update: Cyber-Angriffswelle Petya – Bedrohung größer als bekannt or Scherchel (2017) BSI-Warnung: Nach wie vor hohe Gefahr durch NotPetya-Backdoor in MeDoc or Minister for Law Enforcement and Cyber Security (2018) Australian Government attribution of the 'NotPetya' cyber incident to Russia

6 Reichert (2019) Hardware vulnerability bypasses Spectre and Meltdown patches

7 Westernhagen (2019) Trojaner-Befall: Neue Emotet-Welle legt Neustädter Stadtverwaltung lahm

8 BSI (2019) Die Lage der IT-Sicherheit in Deutschland 2019

9 Herpig (2019) Attack surface of machine learning

10 Russia used NotPetya incident to and then it spread

11 Herpig and Bredenbock (2019) Cybersicherheitspolitik in Deutschland. Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum

12 See Germany's cybersecurity architecture here: https://www.stiftung-nv.de/sites/default/files/cybersicherheitspolitik_in_deutschland.pdf

13 Bundesanzeiger (2015) IT-Sicherheitsgesetz

14 BSI (2018) Die Lage der IT-Sicherheit in Deutschland 2018

15 BSI (2019) Windows-Schwachstelle: BSI warnt vor möglichen wurmartigen Angriffen

16 BSI (2018) Die Lage der IT-Sicherheit in Deutschland 2018

17 BSI (2018) ANSSI and BSI present their first "Common situational picture"

18 Federal Foreign Office (2019) International cyber policy

19 Australian Government Department of Foreign Affairs and Trade (2012) Berlin-Canberra Declaration of Intent on a Strategic Partnership

20 European Council (2017) Cyber attacks: EU ready to respond with a range of measures, including sanctions

21 Council of the European Union (2018) Council conclusions on malicious cyber activities

22 Stilgherrian (2018) Blaming Russia for NotPetya was coordinated diplomatic action

23 Stilgherrian (2018) Blaming Russia for NotPetya was coordinated diplomatic action

24 Koch (2018) Germany is just fine with the NotPetya cyberattack but its allies aren't

25 Auswärtiges Amt (2018) Bundesregierung zum Fall Skripal

26 Reuters (2018) German intelligence sees Russia behind hack of energy firms: media report or Russia 'was behind German parliament hack' or Reuters (2017) Germany challenges Russia over alleged cyberattacks

27 See for example: Center For Strategic International Studies (2019) Significant Cyber Incidents and Tallait (2019) Disrupt and restraint: The evolution of cyber conflict and the implications for collective security

28 Herpig (2019) Aktive Cyber-Abwehr: Innenminister schaltet bei IT-Sicherheit schrittweise von Verteidigung auf Angriff

29 https://theconversation.com/australia-is-the-runaway-global-leader-in-building-new-renewable-energy-123694

30 Maas (2019) Speech by Foreign Minister Heiko Maas at the opening of the Berlin Energy Transition Dialogue

31 Stamper et al (2017) Distributed Energy Systems: Security Implications of the Grid of the Future und Idaho National Laboratory (2016) Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector

32 See: Sanger und Perlroth (2019) U.S. Escalates Online Attacks on Russia's Power Grid, E-ISAC (2016) Analysis of the Cyber Attack on the Ukrainian Power Grid and Cimpanu (2019) Ransomware incident leaves some Johannesburg residents without electricity

33 Heumann, Göhlich, Schuetze (2019) Workshop Documentation UN High-Level Report – discussing Architectures for global digital Cooperation

34 Australian Government Department of Foreign Affairs and Trade (2019) IGF Consultation: Report of the UN Secretary-General's High-level Panel on Digital Cooperation

ANALYSIS

The Cold Wind of Exclusion

Rachael Falk, CEO Cyber Security Cooperative Research Centre

January 2020

An earlier version of this article has been published in condensed form as “Can the ‘core’ and ‘edge’ of a 5G network really be separated?” on the ASPI Strategist[i].

About the Author

Ms Rachael Falk is the Chief Executive Officer of the Cyber Security Cooperative Research Centre (Cyber Security CRC). Ms Falk comes to the Cyber CRC with a strong commercial and cyber security background having practiced as a lawyer for 15 years both in leading law firms in Australia and the UK and also in-house at Telstra Corporation Limited. Ms Falk became Telstra’s first General Manager of Cyber Influence. Ms Falk is a regular commentator on topical cyber security issues in Australia.

There can be no doubt that the Australian government's decision to ban 'high risk vendors' from its 5G network build caused ripples not just through the Five Eyes community but in key markets where these 'high risk vendors' already has key customers. One of those such customers was Germany.

No specific 'high risk vendor' was named by the Australian government[1], however, the media swiftly named Huawei after the then director-general of the Australian Signals Directorate (ASD) noted in a public speech in October 2018:

> *"It would be naive to think we can manage these strategic and technology risks by holding back change. Like everything, it is a question of finding the right balance between leveraging all the advantages that these new shifts bring – and protecting Australians, our values and our way of life.*
>
> *These twin themes of technological and strategic economic shifts can be seen in the government's recent decision to prohibit telecommunications carriers from using high-risk vendors in 5G networks."*[2]

In a visit to Germany in June 2019, it became apparent that this was a country that was grappling with a multitude of tensions when it came to opening the door to a potential 5G vendor that other key countries had considered to be a risk. The Five Eyes' decisions (or deliberations, at least) have also slowly become public.

Australia's position with respect to Huawei was hardly new. And risk based decisions when it came to network operators were not new.

In 2012, the Australian government famously banned Huawei from taking part in the National Broadband Network (NBN) build. However, 2012 was a long time ago and the public narrative (from government, at least) around restriction of such vendors was quite different: there was none. No public statement, no intelligence official publicly talking about it. Nothing. The news dribbled out and was confirmed by the then National Security Advisor, Dr Margot McCarthy before a Senate Estimates Committee hearing in 2013. Importantly, she noted that 'it was a risk based decision to exclude Huawei from the National Broadband Network.'[3]

Trust and trading partners are also a huge influence in when or if decisions like excluding a vendor from building a piece of critical infrastructure should be made public. In 2012, Australia's largest trading partner was China. The lack of public narrative could be explained away in the context of a trade relationship. Or it could be explained in the context of a different time. A time when the public narrative tended to be less direct.

The 2012 NBN decision also didn't really spook our Allies and certainly not Germany. The only 'spooking' (if there were such a thing) came from the US House Intelligence Committee which had issued a damning report on Chinese vendors and trustworthiness. The wave of distrust may have been quiet here in Australia but it was building up in the United States of America. The arguments of trust were often

interwoven with theft of intellectual property and several indictments for the arrest of Chinese nationals accused of spiriting out highly sensitive US secrets and / or of commercial espionage.

However, the NBN decision was 7 years ago and even then there were questions in the US about Chinese law compelling its citizens to cooperate with requests from the Chinese government.

> *"..under Chinese law, ZTE and Huawei would be obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security."* [4]

Chinese law and how it operates is important when it comes to extraterritoriality. According to the Australian Strategic Policy Institute summary of Chinese law:

'For Chinese citizens and companies alike, participation in 'intelligence work' is a legal responsibility and obligation, regardless of geographic boundaries.

This requirement is consistent across several laws on the protection of China's state security. For instance, Article 7 of the National Intelligence Law (国家情报法) declares:

> *Any organisation and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work.'* [5]

This can be summarised by '*For Chinese citizens and companies alike, participation in 'intelligence work' is a legal responsibility and obligation, regardless of geographic boundaries*.'[6] In short, that can mean the ability for the Chinese government to influence/ interfere with/ have access to key assets of national interest and in this case, it would mean Australia's 5G network.

At the same October 2018 National Security Dinner, ASD's Director-General spoke publicly about the risk assessment that ASD carried out as part of their risk assessment for government. In short, according to ASD, once a vendor was embedded in the actual network, then for a high risk vendor, it then just becomes a matter of capability and intent[7]. The ability to interfere with or cause harm (at the direction of their government) exists irrespective of the wishes of that company's leadership. Since then, there has been much talk of the 'core' and 'edge' in a 5G network.

In contrast, ASD's UK equivalent, the General Communications Head Quarters (GCHQ) seemed to form a different view[8] and consequently, the UK government's approach as to 5G vendors was different. And perhaps not surprisingly, the UK also had agreed (many years ago) to having a Huawei 'cell' that assesses Huawei code before it is used[9]. The 5G network build decision is a matter for the UK government and they are perfectly entitled to take a different decision to other Five Eyes partners. It seems, according to news reports, that the 5G decision was subject to heated debate in Cabinet and there was no uniform view as to where the United Kingdom sat with respect to excluding high risk vendors. However, in terms of a public narrative it was the start of the 'core versus edge' narrative. It could be said that Australia was not in this camp.

Was the 'core versus edge' camp looking for convenient nuance in order to justify their decision or to soften the blow for Huawei?

So where did all of this leave Germany in June 2019? It appears somewhat in the middle. Germany did not seem to want to

adopt the direct Australian approach with one organisation we visited saying that "Germany would never directly exclude a company in a procurement process". Some German organisations labelled the Australian decision as "geopolitical". Often talk moved to China being regarded as less of a threat because it was not close geographically which is ironic given the conduit of cyber has no borders.

Overwhelming, we heard that Germany wanted to be in a position to 'trust and verify' and that it would prefer to be able to ascertain (or perhaps exclude or control?) its vendors on that basis. However, when pressed to explain how an approach of trust and verify when even the best run Chinese company can be subject to its domestic law and no German company would be the wiser, they struggled to articulate how this might actually achieve greater security. Some shifted uncomfortably when we asked why a ban on high risk vendors could not occur. There was also talk of a broader European strategy and that one country could not dictate the procurement process. Although apparently these decisions are made a 'national level' and not at the EU level.

The sense was when we left Berlin on a very warm Summer afternoon that they were no closer to a 5G network build procurement decision that enabled the German government to effectively manage the risks of allowing a high risk vendor as part of the 5G build. There was a sense of unease coupled with the tension of knowing they had to act decisively.

Now in early 2020, the leaves have long since fallen and the cold wind of pressure to act would no doubt have been felt in the Bundestag. While the situation with respect to the build of the 5G network remains very fluid at the moment - and there are dissenting factions within the party on this matter - it appears the CDU would lean towards deciding to allow Huawei to take part in Germany's 5G bidding[10]. Such a move has been labelled a 'Faustian bargain' in that it is suggested the Chancellor can put Germany's economic interests first but potentially jeopardise international security in the long term[11].

It is important to look at the actual 'decision' the CDU leadership proposes to make. So far, what we seem to know is that Huawei would be included in the 5G network build procurement process.

According to a document apparently endorsed by the CDU leadership[12], it appears they might advocate for adopting a variant of the 'core versus edge' approach. The document notes that '*the core network must fulfill the highest security requirements… the government should also have increased security requirements for the peripheral 5G network without jeopardising the immediate transition to 5G*' and that '*…no company should have a presence in the network infrastructure no higher than 50% by 2025. In the case of foreign suppliers, a maximum of 30% of the periphery (edge) of the network*.' It is implied that all core network suppliers should be European.

It has also been suggested that the decision to not exclude Huawei from the 5G German build is based on commercial and trade interests that have prevailed over security interests. According to *Foreign Policy*, Germany is heavily reliant on the Chinese market and according to unnamed 'German Officials' that 'Merkel was warned by Chinese leaders that an exclusion of the Shenzhen - based group from the German 5G network would have serious consequences for bilateral economic ties'.[13]

What is clear is that Germany wants to pursue a different path, and that is its choice. To let many vendors compete in the procurement process for any critical infrastructure build is inclusive and this is in keeping with the organisations we spoke with in June 2019. The sense that direct exclusion was not seen as the right thing to do. Or possibly, the impact upon German / China trade relations was too great? Another factor could be that Huawei has partnered with Deutsche Telekom and other carriers in Germany for many years so the cost of replacing such equipment would be considerable.[14]

Germany's possible decision to let Huawei take part in the 5G procurement process feeds into a broader EU issue about security as a whole (as in, the EU) rather than individual member States deciding what is in their national interests. There does seem to be a tension between the German way, and the EU way and it is unclear whether there can really be a unified approach to building of a 5G network particularly because each EU member state may have different incumbent providers who in turn have relationships with many overseas vendors like Huawei.

It will be interesting to see as Germany moves through the 5G procurement process how it will (or will not) be influenced by the different approaches other nations have taken. Similarly, whether it will be influenced by a broader EU approach to national security.

Will Germany decide that it is neither the 'core' or the 'edge' that matters - and the security risks will be managed by limiting foreign network operators as suggested in the CDU document? Irrespective of which path Germany takes, it is bound to attract attention and be closely watched.

Endnotes

i See https://www.aspistrategist.org.au/can-the-core-and-edge-of-a-5g-network-really-be-separated/

1 https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers

2 https://www.asd.gov.au/publications/speech-ASPI-national-security-dinner Speech by the director-general ASD, ASPI National Security Dinner, 29 October 2018

3 https://parlinfo.aph.gov.au/parlInfo/download/committees/estimate/bbcdc742-8b94-4a59-952b-08a9c3964c43/toc_pdf/Finance%20and%20Public%20Administration%20Legislation%20Committee_2013_02_11_1661_Official.pdf;fileType=application%2Fpdf [pages 149-151]

4 US House of Representatives, Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, https://fas.org/irp/congress/2012_rpt/huawei.pdf, page 3

5 Samantha Hoffman and Elsa Kania, ASPI, The Strategist, 'Huawei and the ambiguity of China's intelligence and counter espionage laws' https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/

6 ibid

7 https://www.asd.gov.au/publications/speech-ASPI-national-security-dinner

8 https://www.bbc.com/news/technology-48035802

9 Similar offers (or suggestions for a cell) as far back as 2012 had been made by Huawei in Australia which have never been accepted by the Australian government.

10 Theresa Fallon, 'Germany's Faustian Bargain with China', The Diplomat, November 8, 2019

11 Ibid

12 Tweet from Noah Barkin, 18 December 2019 noting 'The CDU leadership in parliament adopted this paper on #5G yesterday evening. It is softer in key areas, paving the way (by my reading) for a #Huawei role in the German network…'

13 'Europe's Backlash Against Huawei has Arrived, Foreign Policy, November 27 2019

14 The Diplomat, Germany's Faustian Bargain with China, Theresa Fallon, November 8, 2019

ANALYSIS

5G and beyond: A test for "technological sovereignty" in Europe?

Isabel Skierka, Researcher at the European School of Management and Technology Berlin; PhD candidate at TalTech University, Estonia; non-resident fellow at GPPi, Berlin

December 2019 [This article was submitted in late December 2019. Therefore, developments after that point in time are not considered in this article.]

About the Author

Isabel Skierka is a researcher with the Digital Society Institute at ESMT Berlin, where she focuses on cybersecurity policy in Germany and Europe (including IoT security and safety), electronic identity management, and the intersection of geopolitics and technology. She is also pursuing a PhD at the Ragnar Nurkse Department of Innovation and Governance at Tallinn University of Technology in Estonia in which she explores cybersecurity crisis management. She is a non-resident fellow with the think tank Global Public Policy Institute (GPPi) in Berlin, and serves as a member of multiple multi-stakeholder organizations in the field of digital policy. Prior to joining ESMT, Isabel worked with GPPi, NATO, at the European Commission's DG Connect (as a Bluebook trainee), and as a visiting researcher at the Institute of Computer Science of the Free University of Berlin. Isabel holds a master's degree in international conflict studies from the War Studies Department of King's College London and a bachelor's degree in European studies from Maastricht University, including an exchange at Sciences Po in Paris.

In the heated debate over Chinese vendors' participation in the roll-out of 5G mobile networks, Europe has so far refrained from a black-and-white stance on the issue. For months, the United States has pressured European allies to exclude Chinese vendors such as Huawei from 5G networks on national security grounds.

In the end, European Union (EU) member states have been navigating a 'middle way' between an outright ban, following countries like the United States or Australia, and a completely vendor-agnostic approach. In October 2019, the EU Network Information Security (NIS) cooperation group (composed of representatives from EU member states, the European Commission and the EU's cybersecurity agency ENISA) published a joint risk assessment which provides a thorough overview of the technical, but also the non-technical, political challenges related to securing 5G networks.[1] The report emphasizes the need for robust IT security risk management and other technical measures, but also warns member states of deploying equipment from suppliers that are likely to be "subject to interference from a non-EU country" due to respective legislation and a lack of "democratic checks and balances". It also names "non-EU states or state-backed actors" as a primary threat to 5G network security. The wording's code for the Chinese tech giant Huawei and China itself is hard to miss. A set of Council Conclusions published in early December 2019 echoed these concerns.[2] On this basis, the EU is poised to publish a 'toolbox' of technical, legal, and political risk mitigation measures by 31 December 2019.[3]

The challenges that the EU faces with 5G go beyond cyber and national security threats. For Europe, the rollout of the 5G infrastructure has become a geopolitical test on several levels. Will Europe be a shaper or taker of 5G technology and the new era of industrialization it promises to propel? How will it be able to control the security and reliability of such key digital infrastructures in the long-term? Eventually, how should EU member states manage their dependencies on foreign technologies and strengthen their "technological sovereignty" – a political priority of the incoming EU Commission led by Ursula von der Leyen?[4] The latter might be the most important strategic issue the EU will need to tackle in the long-term and will be decisive for the Union's ability to shape its own future in the digital age.

It is against this wider geopolitical backdrop that EU member states will need to decide the handling of 5G security risks and potential dependencies on Chinese suppliers, like Huawei, in their telecommunications networks. The precondition for a unified approach is unity among EU member states.

The German debate – a precedent for Europe?

In Germany, the question of Huawei's involvement in the rollout of 5G networks has perhaps triggered the most intense public debate of all countries in Europe. The

While the inclusion of Huawei in the rollout of 5G networks carries significant political and economic risks, German industry also has a lot to lose. Excluding Huawei from the network would likely result in some form of retaliatory action from Beijing that could harm the German economy

country's decision about 5G security will send an important signal to other EU members – Germany has the largest national economy and largest telecommunications market in Europe. While the inclusion of Huawei in the rollout of 5G networks carries significant political and economic risks, German industry also has a lot to lose. Excluding Huawei from the network would likely result in some form of retaliatory action from Beijing that could harm the German economy and specific industries, such as the car industry. Chinese officials and more recently, the Chinese ambassador to Germany, have already hinted at this possibility.[5]

In this context, the German government had originally planned to adopt a purely technical approach to 5G security. Days after the EU's join risk assessment's publication on 9 October 2019, the German government released a catalog of draft telecommunications security requirements. Drafted by two lower level government agencies – the Federal Network Agency (BNetzA) and the Federal Office for Information Security (BSI) – the catalog argued that security would be guaranteed above all by the technical certification of software and hardware from 5G technology providers and inspection of the source code.[6] In addition, operators of public telecommunications networks would have to request a "declaration of trustworthiness"[7] from the equipment vendor. The equipment vendors' corporate structure and the context of the legal and political environment in which it operates – key aspects raised in the EU joint risk assessment – would not have to be evaluated. Under these conditions, network operators would have been able to source the majority of 5G network components from Chinese equipment manufacturers such as Huawei and ZTE.

However, the German government's approach did not consider the non-technical political and economic risks of a long-term dependency on Chinese suppliers. Local intelligence legislation allows the Chinese government to coerce companies like Huawei or ZTE into cooperating with national intelligence agencies and potentially facilitate espionage or sabotage of 5G infrastructures abroad. Apart from the frequently emphasized risks for national security, relying on a foreign tech giant entails considerable economic and industrial disadvantages. European competitors like Nokia and Ericsson will have difficulties surviving in the face of an increasingly powerful Chinese tech giant that is likely subsidized[8] by its national government. The absence of any strategy for 5G security and industrial policy from the German government's approach from fall 2019 was striking. By delegating the decision on 5G security

to the technocratic level, the German government evaded political responsibility for an issue of high geopolitical significance.

According to media reports[9], the German chancellor herself intervened in order to prevent restrictions against Chinese suppliers. Likely motives include the fear of Chinese retribution against German companies such as Volkswagen, Siemens, or BASF, which heavily rely on the Chinese market. This approach remarkably differs from that of other European countries. France or Italy, for example, have awarded government ministers or security services with the powers to examine and decide over network operators' plans to roll out 5G on the grounds of national security concerns.[10]

Yet, the tides have been turning in Germany and triggered a vivid parliamentary debate which could, after all, lead to a de facto restrictions of Huawei equipment in Germany. Not long after the draft guidelines' publication, a group of parliamentarians rebelled against the government and demanded the chancellor to submit the decision on 5G to the German parliament instead of declaring it a fait accompli.[11] Among them were a number of prominent members of Merkel's own party, the Christian Democratic Union (CDU), thereby also turning the debate into a leadership test for the chancellor. Throughout the months of November and December, various coalitions, both among governing parties and opposition parties, formed in parliament, all debating and working on new 5G security criteria.[12]

At the time of writing (mid-December), the government coalition has been deliberating to adopt tougher criteria for vendors to participate in the 5G network rollout, including the political and legal conditions that any given vendor is exposed to in its country of origin.[13] Such language and propositions made into a public position paper by the Social Democratic Party (SPD) coalition partner and an informal paper from members of the CDU/CSU parties would allow a de facto ban of Chinese vendors, at least from critical parts of future 5G networks.[14] Merkel's CDU is expected to explore a common position in January.[15]

Meanwhile, Telefónica Deutschland, which is Germany's second largest telecoms operator confirmed that Huawei would help build its network. Vodafone, the third largest operator, warned that an exclusion of Huawei would delay its 5G rollout up to five years, and Germany's largest and partially state-owned operator Deutsche Telekom will freeze spending on new 5G equipment due to political uncertainty.[16]

Whatever the final outcome will be, the German case is an example for how decisions on the deployment of strategic technologies and issues of national security as well as 'technological sovereignty' can be openly and democratically debated by the

According to media reports, the German chancellor herself intervened in order to prevent restrictions against Chinese suppliers. Likely motives include the fear of Chinese retribution against German companies such as Volkswagen, Siemens, or BASF, which heavily rely on the Chinese market.

legislative and executive. Despite the long time it took decision makers to grasp the importance of the issue and engage in a serious debate, it could set a precedent for future similarly strategic discussions.

Decisions in other EU member states as well as the EU 5G cybersecurity toolbox to be published by the end of December will give further impetus to the development of a common, or divided, EU position on the geopolitics of 5G.

Beyond 5G: "Technological sovereignty" in Europe

Although on the surface, the debate about 5G security centers around cyber security and national security concerns, its major strategic dimension is that of what the European Commission refers to as "technological sovereignty".[17] Technological sovereignty is a widely used political term that remains yet to be defined, let alone operationalized. In European political discourse, it refers to the ability of an actor (a state, a company or an individual) to act and decide independently in the digital realm. A precondition for technological sovereignty is a certain degree of control over key competences and technologies as well as the ability to decide among alternative technologies and capabilities provided by trustworthy partners, and the ability to further develop these, if necessary.[18] In this context, sovereignty does not equal autarky. Rather, it consists precisely in the ability of entering into dependencies while being able to master them through the capacity to assess and (to a certain degree) control technologies and capabilities.

Hence, how can Europe "strengthen its technological sovereignty" – a proclaimed goal by the new European Commission? Since European countries are increasingly dependent on foreign technology suppliers, particularly in the areas of cloud and data infrastructure and software, mobile and desktop operating systems, as well as semiconductors and microprocessors, this will be no easy task. Ironically in the context of the 5G debate, one of the few technology fields in which European companies are still leading, is that of mobile communications equipment. Two of the three Radio Access Network market leaders, Ericsson and Nokia, are European and competitors of Huawei. In the context of the 5G debate, a first step should therefore be to strengthen European manufacturers and to level the playing field for them on the European market. This will require not only security guidelines, but, in the long-term, competition and industrial policy measures.

Enhancing its members' capacity to act more independently in the digital realm will require the EU to strengthen its own industrial base in key technology sectors, as well as managing necessary dependencies in an interdependent and global economy and supply chain through trade and diplomatic tools.

As a first step, decision-makers in Europe should therefore determine which key technologies and competencies they themselves should produce and command, and in which areas they can enter into dependencies. This must be accompanied by a strategy for managing dependencies on foreign technology providers, which inevitably arise in the global value chain. With which partners can and should EU member states cooperate in the long term, and in what frameworks? The trustworthiness of the political and legal system as well as previous experience with partners within an alliance should play an important role as part of this assessment.

Although on the surface, the debate about 5G security centers around cyber security and national security concerns, its major strategic dimension is that of what the European Commission refers to as "technological sovereignty"

Moreover, governments should actively promote innovation and strengthen their own industrial base in key technology fields, such as robotics, artificial intelligence capabilities (talent and technologies), and edge computing. States should invest into research and development and applied innovative projects (also in cooperation with the private sector), leverage their role as procurer to promote selected technologies and create legal certainty for the use of new technologies. The Union has already started with the Important Projects of Common European Interest (IPCEI) tool in the field of microelectronics, or the European Network of Competence Centers in Cybersecurity under the Horizon 2020 tool.[19] In order to strengthen transparency and control possibilities of IT, but also innovation possibilities, EU legislators could oblige manufacturers and suppliers to open up technologies and achieve greater interoperability. EU member states should also examine and strengthen competition law and other instruments that level the playing field for companies on European market.

On the external dimension, Europe will need to level the playing field by adapting rules for trade, foreign direct investment, and procurement. All while safeguarding the principles of an open and competitive European economy, the EU might need to extend state-aid control beyond EU companies, support European firms with investment funds -both in the fields of research and development as well as implementation -, and strengthen its foreign direct investment screening tool.[20]

If Europe wants to retain its ability to shape its own digital future more generally, these are essential steps to take in the near future. The region's long-term command over digital technologies will perhaps be its most strategic asset and a precondition for the assertion of political and economic influence in the future.

Endnotes

1 EU NIS Cooperation Group, "EU coordinated risk assessment of the cybersecurity of 5G networks", 9 October 2019, Brussels. Retrieved from: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

2 Council of the European Union, "Council Conclusions of the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G", 3 December 2019, Brussels. Retrieved from: https://www.consilium.europa.eu/media/41595/st14517-en19.pdf

3 European Commission, "Press release - EU-wide coordinated risk assessment of 5G networks security", 9 October 2019, Brussels. Retrieved from: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

4 European Commission, "The von der Leyen Commission: for a Union that strives for more", 10 September 2019, Brussels. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_5542

5 Noah Barkin, "Europe's Backlash Against Huawei Has Arrived", Foreign Policy, 27 November 2019. Retrieved from: https://foreignpolicy.com/2019/11/27/europe-huawei-backlash-merkel-germany-summit/

6 Bundesnetzagentur, "Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung von personenbezogenen Daten nach § 109 Telekommunikationsgesetz – Stand 09.10.2019", 9 October 2019. Retrieved from https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen2.pdf?__blob=publicationFile&v=2

7 In principle, this amounts to a "no spy clause" between vendor and network operator. In that clause, suppliers would have to assure that they are legally and effectively able to refuse the disclosure of confidential customer information to third parties. However, the "declaration" mechanism lacks any verification, enforcement or evaluation mechanisms.

8 Ellen Nakashima, „U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible", 29 May 2019, The Washington Post. Retrieved from: https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html

9 Moritz Koch, Dietmar Neuerer, Stephan Scheuer, „Merkel öffnet 5G-Netz für Huawei", 14 October 2019, Handelsblatt. Retrieved from https://www.handelsblatt.com/politik/deutschland/netzausbau-merkel-oeffnet-5g-netz-fuer-huawei/25107766.html

10 Wei Shi, "French parliament passes "Huawei Law" to govern 5G security", 26 July 2019, telecoms.com. Retrieved from: https://telecoms.com/498728/french-parliament-passes-huawei-law-to-govern-5g-security/. Reuters, "Italy approves use of special powers over 5G supply deals", 5 September 2019, Reuters. Retrieved from: https://www.reuters.com/article/us-huawei-tech-5g-italy/italy-approves-use-of-special-powers-over-5g-supply-deals-idUSKCN1VQ1YG

11 Noah Barkin, "Europe's Backlash Against Huawei Has Arrived", Foreign Policy, 27 November 2019. Retrieved from: https://foreignpolicy.com/2019/11/27/europe-huawei-backlash-merkel-germany-summit/

12 See: Moritz Koch, Stephan Scheuer, "Außenminister Maas stellt sich in der Huawei-Frage gegen Kanzlerin Merkel", 20 November 2019, Handelsblatt, retrieved from: https://www.handelsblatt.com/politik/deutschland/5g-mobilfunknetz-aussenminister-maas-stellt-sich-in-der-huawei-frage-gegen-kanzlerin-merkel/25244378.html; Guy Chazan, "Merkel under pressure over Huawei's role in German 5G rollout", 13 December 2019, Financial Times. Retrieved from: https://www.ft.com/content/372c1da6-1d98-11ea-97df-cc63de1d73f4;

13 Guy Chazan, "Merkel under pressure over Huawei's role in German 5G rollout", 13 December 2019, Financial Times.

14 At the time of writing, the SPD has published its position paper, the CDU/CSU has not yet published a common position. See: SPD-Fraktion im Bundestag, "Ein digital souveränes Europa mit sicheren 5G-Netzen", SPD-Position Paper, 17 December 2019, Berlin. Retrieved from: https://t.co/WxTQSFKfb5?amp=1; noahbarkin, "The CDU leadership in parliament adopted this paper on #5G yesterday evening. It is softer in key areas, paving the way (by my reading) for a #Huawei role in the German network. This is significant! Key elements:", 17 December 2019 [Twitter Thread]. Retrieved from: https://twitter.com/noahbarkin/status/1206926297357832192

15 Moritz Koch, "5G-Ausbau: Kanzleramt will vollständiges Huawei-Verbot verhindern", 17 December 2019, Handelsblatt,retrieved from: https://www.handelsblatt.com/politik/international/mobilfunkstandard-5g-ausbau-kanzleramt-will-vollstaendiges-huawei-verbot-verhindern

16 Guy Chazan, "Merkel under pressure over Huawei's role in German 5G rollout", 13 December 2019, Financial Times.

17 The following is based on parts of: Isabel Skierka, "Stellungnahme zur Anhörung des Ausschusses Digitale Agenda zum Thema ‚IT-Sicherheit von Hard- und Software als Voraussetzung für Digitale Souveränität", 11 December 2019, Deutscher Bundestag. Retrieved from: https://www.bundestag.de/resource/blob/672536/b2b63aeeaffe54e40f8c62571cc628c4/Stellungnahme-Skierka-data.pdf; European Commission, "The von der Leyen Commission: for a Union that strives for more", 10 September 2019, Brussels. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_5542. Sometimes, the term is also referred to similarly as "digital sovereignty" or "digital strategic autonomy".

18 Bitkom, „Digitale Souveränität, Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa", 2015; Forschungszentrum Informatik, Accenture, Bitkom Research, „Kompetenzen für eine Digitale Souveränität", 2015.

19 European Political Strategy Centre of the European Commission, "Rethinking Strategic Autonomy in the Digital Age", EPSC Strategic Notes, July 2019, Issue 30. Retrieved from: https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf

20 Mark Leonard, Jean Pisani-Ferry, Elina Ribakova, Jeremy Shapiro, and Guntram Wolff, "Redefining Europe's Economic Sovereignty", June 2019, European Council on Foreign Relations. Retrieved from: https://www.ecfr.eu/publications/summary/redefining_europes_economic_sovereignty

ANALYSIS

Responding to Cyber Security Threats in Critical Infrastructures – Challenges for Australia and Europe

Prof Helge Janicke, Director of Research Cyber Security Cooperative Research Centre and Edith Cowan University

November 2019

About the Author

Prof. Helge Janicke is the Research Director of the Cyber Security Cooperative Research Centre, Australia. He is affiliated with Edith Cowan University and holds a visiting Professorship in Cyber Security at De Montfort University. Prof. Janicke's research interests are in the area of cyber security, in particular with applications in critical infrastructures using cyber-physical systems, SCADA and Industrial Control Systems. Prof. Janicke's current research investigates the application of Agile Techniques to Cyber Incident Response in Critical Infrastructure, Managing Human Errors that lead to Cyber Incidents, and research on Cyberwarfare & Cyberpeacekeeping. Prof. Janicke established DMU's Cyber Technology Institute and its Airbus Centre of Excellence in SCADA Cyber Security and Forensics Research. He has been the Head of School of Computer Science at De Montfort University, before taking up his current position as Research Director for the Cyber Security CRC. Prof. Janicke founded the International Symposium on Industrial Control System Cyber Security Research (ICS-CSR) and contributed over 100 peer reviewed articles and conference papers to the field that resulted from his collaborative research with industry partners such as Airbus, BT, Deloitte, Rolls-Royce, QinetiQ, and General-Dynamics.

Critical infrastructures are organisational and physical infrastructures essential to our nations' economy and the well-being of its citizens. A disruption or degradation of these infrastructures directly impacts on key responsibilities of the state to provide essential services to its citizens.

Whilst definitions as to what constitutes essential services vary across nations, they all share a common understanding as to the importance of a mature approach to their cyber security.

The European Union (EU) identifies Energy, Transport, Banking, Financial Market Infrastructures, Health, Water, and Digital Infrastructures as critical in its Network and Information Systems (NIS) directive [1]. This directive came into force in May 2018, but leaves the concrete implementation and identification of Operators of Essential Services (OES) to its member states, whilst providing guidance and advice on the assessment methodologies to create consistency in approach across the EU. The NIS thus balances the need for a consistent and coordinated approach across its member states with the individual member states operational realities and their local governance structures with the overarching aim to establish a coordinated approach to the response to major cyber security incidents. Similarly, the Australian Government recognises 8 critical infrastructures: banking & finance, government, communications, energy, food & grocery, health, transport, and water in its Critical Infrastructure Resilience Strategy[2]. It specifically identifies operators of critical infrastructure assets in its Cyber Security of Critical Infrastructure Act 2018[3], in particular regulating reporting requirements and powers with respect to critical electricity, gas, ports, water assets. In its draft Cyber Security Strategy 2020[4] Australia is consulting on the adoption of additional measures similar to the European NIS directive.

The impacts of a degradation or disruption of essential services on a nation's economy can be significant, and are difficult to quantify. Work by Schmidthaler and Reichl [5] provides computer based models to estimate the economic impact of power outages across the EU using a power outage across Italy as an example. They estimate the economic impact of this 3-16h (depending on region) outage on Sunday the 28th February 2003 across Agriculture, Manufacturing, Services and Households to have been €1182 million. Given the significant losses, understanding the impact and the potential for cascade failures due to long term disruptions is important to prepare for cyber incidents[6].

Whilst disruptions of essential services due to cyber attacks remain comparatively rare in comparison to functional failures or natural disasters, they are a real and significant risk. Recent examples of sophisticated cyber incidents are the 2015 BlackEnergy attack[7,8] on the Ukrainian energy sector, disrupting power supply to over 200,000 households. Whilst the earlier 2010 Stuxnet attack[9] on an Iranian nuclear enrichment plant already alerted to the potential of cyber warfare[10] and the vulnerabilities

of Industrial Control System components to cyber attacks. The BlackEnergy incident highlighted the increasing connectivity between corporate Information Technology (IT) systems and frequently vulnerable Operational Technology (OT) that controls the physical infrastructure. It also demonstrated the increasing sophistication and coordination of cyberattacks to impact on critical infrastructures.

Not all attacks are specifically targeting OT used to deliver essential services. In 2017 the WannaCry ransomware[11] impacted significantly the operations of the UK's National Health Service, until systems could be restored. WannaCry clearly demonstrated the vulnerabilities and direct impact on public services, especially if these are already operating under stress. Whilst the response and the recovery from backups was swift, it exposed significant risks associated with the maintenance and secure use of large corporate IT networks. This incident also affected thinking in the OT space - where a recovery from a large scale ransomware infection would in many infrastructures be harder, and more time-consuming. That this is a persistent threat to many organisations is clear: the global shipping company Maersk[12] suffered significantly from the NotPetya[13] ransomware in 2017, and is still in legal proceedings with its insurers over the incident.

These examples illustrate some of the cyber security risks that industries face today. Over the last decades many industries benefited from increased IT/OT integration and automation, without sufficiently addressing the increasing cyber security risks, to the extent that for many of these industries a fall-back to more manual processes is either incurring large losses or is simply infeasible. These risks are balanced with the cost of implementing better security, and investment in upgrading the OT infrastructure to offer better security. For industries that operate critical infrastructures the situation is more complex, as regulators and national interests are exerting influence on the management of cyber security risks.

A complicating issue when protecting essential services are the intertwined responsibilities for the protection of critical infrastructures. At a macro level these typically involve a variety of stakeholders that influence the development and operation of these services. Whilst the state has regulatory oversight of critical infrastructures, the delivery of the service is typically the responsibility of a private corporation. To increase competition and disrupt monopolies, governments frequently favour a separation of the provision of a service from the underpinning distribution networks with complex interplays between these systems. An example of this is Network Rail, which owns the majority of the UKs rail infrastructure through its "devolved routes" business model but works with a variety of train operators to deliver a transport service to the UK's population and businesses. Similar examples exist in other essential services. Combatting any disruption due to a cyber attack hence requires significant coordination between a number of (potentially competing) organisations that together make up the service.

At a micro-level, there is often a disconnect between the IT focused Cyber Security expertise and the coordination with other stakeholders in the business and the engineers on the shop-floor, making a coordinated and effective response to attacks on OT difficult to achieve. Whilst most nation's security strategies for critical infrastructures emphasise the need for Operators of Essential Services to coordinate and

This pace of technology adoption makes protecting large scale infrastructures a herculean task. Many installations have been operational for 20 years or more, and evolved over time as they needed to integrate with newer technologies in an increasingly digital world.

collectively prepare for cyber attacks, the adoption of cyber security controls in critical infrastructures is clearly outpaced by the development of IT/OT connectivity and integration of new technologies such as 5G and modern Industrial Internet of Things (IIoT) infrastructures.

This pace of technology adoption makes protecting large scale infrastructures a herculean task. Many installations have been operational for 20 years or more, and evolved over time as they needed to integrate with newer technologies in an increasingly digital world. These legacy installations make it difficult to overcome security vulnerabilities that are often inherent in their architecture and the details of their implementation. Overhauling this infrastructure en-mass can be very costly. It is also typically is not planned in the original business case and thus negatively affects the return on investment and hence profits of the organisations providing the service. Updating infrastructure brings further risks and disruption as large scale tests are often infeasible and whole-sale technology change has a history of overrunning in time/cost and causing severe disruption to services.

Given these difficulties, it is clear that we need to better understand these complex systems[14] and equip organisations that are contributing to their operation with the capability and capacity to manage cyber attacks. It also raises the question how we quantify cyber security risks as part of business decision making in this sector – what effect has the fast-paced evolution of IT on the traditionally longer life-times of OT infrastructure. The IT world is ahead in its maturity to deal with cyber security threats, regular patching regimes, secure by default device configurations, strong authentication and encryption, firewalls, DMZ, Intrusion Detection systems and the swift recovery from backups (in the case of Ransomware) are all part and parcel of any modern IT heavy organisation.

In the OT sector the ability to deploy these mechanisms is far more limited, as legacy systems cannot be easily replaced without (expensive) re-certification of safety cases; for similar reasons patching is often not feasible. The introduction of tried and tested IT security controls bears dangers[15] as they can negatively affect the functioning of the system especially when additional network latencies are critical and can jeopardize the safe operation of the system[16], e.g. in energy distribution networks. These additional challenges for securing OT infrastructure are however not only technical in nature, there still is a lack of awareness and understanding in how to architect secure OT infrastructures with many large organisations relying on a small number of skilled individuals. The majority of reported cyber attacks on critical infrastructures reached the OT infrastructure through cyber security breaches of corporate IT networks

– whilst this should not be a reason to be complacent about OT security it shows that even the more mature IT protections were the first to fail, typically through simple human errors[17].

For future technologies, underpinning our increasingly smart infrastructures and smart cities, Artificial Intelligence (AI) techniques and scalable Big-Data analytics[18] will undoubtedly play a role in helping to overcome some of these issues. However, they are not a panacea for all our critical infrastructure cyber security ills. AI technologies can assist to manage the large amounts of sensor data and help in the identification of system anomalies[19] as well as improving the immediate response to cyber incidents through automation. However, it is important to recognise that cyber security is an arms-race and many of the tools that help us defend our systems equally can be used to subvert them. Data-Analytics in the form of open source intelligence and automation are already tools of the trade in sophisticated Advanced Persistent Threats (APTs) and aid in the targeting and execution of cyber-attacks. The idea that an AI that is deployed to protect a system can be subverted and used sparked a whole area of AI research called adversarial machine learning[20]. It is clear that technological innovation in newer, better cyber security tools is part of the solution, but it clearly alone cannot rise up to the challenge.

Securing the critical infrastructures that underpin our daily lives and well-being requires a coordinated approach and a long-term vision and strategy to provide direction and support to providers of essential services such as the National Cyber Security strategies of many nations in the industrialised world. Their implementation must challenge current organisational structures, employee behaviours, and at times business models that prioritise efficiency savings and productivity increases over the prudent management of critical cyber security risks. Many of the cyber security challenges are not rooted in technology but its effective use and the organisational structures that surround it. This means that education and awareness across all walks of life and professions that develop, operate and indeed use our critical infrastructures is an essential tool in combatting cyber attacks in our increasingly digitised world.

Endnotes

1 European Commission, "The Directive on security of network and information systems (NIS Directive) | Digital Single Market," Eur. Comm., 2016.

2 Australian-Government, "Critical Infrastructure Resilience Strategy: PLAN," 2015.

3 Australian-Government, "Cyber Security of Critical Infrastructure Act 2018," 2018.

4 Australian-Government, "Australia's 2020 Cyber Security Strategy - A call for views," 2019.

5 M. Schmidthaler and J. Reichl, "Assessing the socio-economic effects of power outages ad hoc," Comput. Sci. - Res. Dev., 2016.

6 G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, G. Lykou, and D. Gritzalis, "Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures," Int. J. Crit. Infrastruct. Prot., 2016.

7 R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer, "Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid," 2016.

8 Department for Homeland Security, "Cyber-Attack Against Ukrainian Critical Infrastructure | ICS-CERT," ICS-CERT, 2016. .

9 R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," IEEE Secur. Priv., 2011.

10 M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," Comput. Secur., vol. 49, 2015.

11 National Audit Office, "Investigation: WannaCry cyber attack and the NHS - National Audit Office (NAO)," National Audit Office, 2017. .

12 L. Matthews, "NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million," Forbes, 2017.

13 S. Mansfield-Devine, "Ransomware: the most popular form of attack," Comput. Fraud Secur., 2017.

14 C. Islam, M. A. Babar, and S. Nepal, "A multi-vocal review of security orchestration," ACM Computing Surveys. 2019.

15 A. Cook, H. Janicke, L. Maglaras, and R. Smith, "An assessment of the application of IT security mechanisms to industrial control systems," Int. J. Internet Technol. Secur. Trans., vol. 7, no. 2, 2017.

16 D. Hunter, J. Parry, K. Radke, and C. Fidge, "Authenticated encryption for time-sensitive critical infrastructure," in ACM International Conference Proceeding Series, 2017.

17 M. Evans, Y. He, L. Maglaras, and H. Janicke, "HEART-IS: A novel technique for evaluating human error-related information security incidents," Comput. Secur., vol. 80, 2019.

18 E. Bertino, S. Nepal, and R. Ranjan, "Building Sensor-Based Big Data Cyberinfrastructures," IEEE Cloud Comput., 2015.

19 R. Luh, G. Schramm, M. Wagner, H. Janicke, and S. Schrittwieser, "SEQUIN: a grammar inference framework for analyzing malicious system behavior," J. Comput. Virol. Hacking Tech., vol. 14, no. 4, 2018.

20 D. L. Marino, C. S. Wickramasinghe, and M. Manic, "An adversarial approach for explainable AI in intrusion detection systems," in Proceedings: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, 2018.

REFLECTION

Selected conversations from a study tour of Berlin and Brussels

Prof Lyria Bennett Moses, Director of the Allans Hub for Technology, Law and Innovation, University of New South Wales, Sydney

August 2019

About the Author

Lyria is Director of the Allens Hub for Technology, Law and Innovation and a Professor in the Faculty of Law at UNSW Sydney. Lyria's research explores issues around the relationship between technology and law, including the types of legal issues that arise as technology changes, how these issues are addressed in Australia and other jurisdictions, and the problems of treating "technology" as an object of regulation. Recently, she has been working on legal issues associated with the use of "artificial intelligence" technologies, the appropriate legal framework for enhancing cyber security and oversight for law enforcement intelligence. Lyria is a member of the editorial boards for Technology and Regulation, Law, Technology and Humans and Law in Context.

The KAS–sponsored visit of a delegation of Australians to Berlin and Brussels in 2019 provided an opportunity to consider different responses to mutual challenges posed by cyber threats. These ranged from the role of data protection law, to the inclusion of high–risk vendors in new 5G networks, to the form of law and the European regulatory focus on cyber security. While the full richness of the conversations cannot be captured here, some highlights are summarised below.

There is some difference between how the relationship between cyber security and data protection laws is perceived in Germany and Australia. In Germany, these are treated as distinct legal and policy domains – the former concerns critical infrastructure and technical protections and the latter protection of personal data. In Australia, the two issues are often intertwined in policy debates. In particular, moving to a stronger data protection regime is more often linked with enhanced protection from cyber fraud and reduced cyber risk.

In Germany, the primary form of data protection is the GDPR, which is becoming more popular over time, in particular due to its ability to enhance trust online. There was some discussion around what Australia can learn from this, given there is no real mechanism in Australia for holding even large listed companies to account for data breaches, given the impact on share price is minor. While the GDPR is often viewed fondly in Australia, there remain issues in Germany. There are still some residual concerns about impact on innovation. Further, there are federal issues with different agencies are responsible for regulating the use of data – meaning one can have 16 decisions for the same violation (from each German state).

Germany is currently looking to harmonise but it is challenging as the state agencies do not report to the federal government. Federalism also poses challenges for data privacy law in Australia, with different privacy laws in each state and territory in addition to the federal Privacy Act.

In regards to 5G and so-called high risk vendors, the Australian stance is that this was a risk-based decision rather than a trade-based decision or a decision about a particular vendor. The balance of risk is perceived differently in Germany as the focus of its relationship with China has been primarily economic. As a result, the German regulations will operate at a general level, requiring enterprises to demonstrate that they have not been influenced. This may lead to a similar result, namely the exclusion of some Chinese companies, but this will depend on how the general regulations operate in practice. The current question is whether there can be a more open framework at the network periphery than what may be required in the core – a question on which there are different views. The Australian view is that such a distinction is not possible in the context of 5G.

The Australian and US approach to the question of Huawei and 5G has forced the EU to think more deeply, but there remains difference of opinion concerning the relative balance of commercial and national security considerations.

It is possible that Huawei would be able to litigate in Germany, or retaliate against German exporters, were it excluded from the 5G network. There is also significant work being done in Germany across ministries to better understand the current position in terms of foreign policy vis a vis China and the Pacific (internationally and within Europe), China's likelihood of interference, and technical questions about 5G and potential impact at different ends of the network. Generally, Germany is seeking to work with China and encourage it to engage constructively and in light of important values in the international sphere. It is also focussed on remaining a liberal open economy. Australia's perception of risk is different due to high Chinese ownership and geographical proximity. Both countries are concerned about theft of intellectual property and trade secrets in areas such as quantum computing.

From an Australian perspective, what stands out is the relevance of trust in a corporation (through finances and corporate structure) when it can be directed by its government. Ultimately, Germany's relationship with China is different to Australia's relationship, giving each a different perspective on the risks presented by Huawei. Germany is particularly conscious of freedom of trade and refuses to arbitrarily exclude vendors. Australia is more conscious of China's global ambitions. The major challenge is not espionage (that can be solved through end to end encryption, although the security agencies have other concerns about this approach) but rather sabotage of the network.

Germany is co-operating within the EU on a broader framework, which will involve certification and risk assessment. It is likely that the EU will differentiate requirements according to layers of the network; rural/urban divides do not work for Germany because there are state capitals of varying size. The European Network and Information Security Agency (ENISA) will also be involved and will propose a tool box of measures. This will hopefully lead to a level of harmonisation in the EU, but, because public security is not part of the EU agreements, countries can still make diverse decisions on national security grounds.

The world is currently dependent on very few suppliers with the goal of building local capacity in core technologies impracticable given the fast pace of development. This forces a choice.

The Australian and US approach to the question of Huawei and 5G has forced the EU to think more deeply, but there remains difference of opinion concerning the relative balance of commercial and national security considerations. In Europe, the telecommunications framework has a competition focus, which means operators compete to reduce costs. This makes using Huawei attractive.

Europe in general, and Germany in particular, have legislation focusing specifically

on cyber security. In the EU, this has gone into effect and there is ongoing work on the framework for the development of national cyber security schemes, with different countries at different stages of developing these. The European law applies to all member states as of 28 June, also making ENISA permanent. ENISA aims to build cyber security capacity in member states and enhance awareness through initiatives like Cyber Security Month. It participates in a broader policy network and supports member states in event of wide scale cyber attack. EU legislation also creates an EU framework for certification of cyber security devices and products. Market players can get certificate from any EU state; that certificate is then valid for the whole EU. The legislation ultimately is about certification – depending on context, this is only sometimes mandatory and industry will be involved in the mandatory elements. At the moment many of the concepts are at a high level, eg "internet connected products" which covers hackable toys, data protection principles, fraud, etc. Member states have different views on these laws eg France is looking at a more interventionalist stance than Germany. The discussion in the UK remains more industry-friendly.

Germany also has cyber security legislation. This deals with critical infrastructure, including power, water, nutrition/food, IT and telecommunications. For these sectors, it is mandatory to file reports to the security agencies and government should there be any cyber threat events. The agencies can then collect information and support companies that have been attacked. The Act also established a Federal Office for IT Security, supported by a research institute that reports to the Federal Ministry of the Interior. That facilitates the collection of information and development of expertise.

There are maps being developed, by BDI working with Deloitte, of cyber security laws around the world. Interestingly, Australia was shown as not having any laws specifically dealing with cyber security. Partly, this is a definitional question. For example, Germany's laws deal with liaison between government and industry around the protection of critical infrastructure against cyber security threats, whereas Australia's laws on a similar subject matter are wider in scope (covering all security threats). There seems to be little benefit in mapping only countries that have laws that deal separately rather than holistically with cyber security threats. In particular, by suggesting Australia has no cyber security laws, users of the map may be misled in their understanding on which countries were using law to help manage cyber security threats.

Editor

Katja Theodorakis

Publisher

Konrad Adenauer Stiftung (Australia) Limited
Regional Programme Australia and the Pacific

11/3 Sydney Avenue
Barton, ACT 2600
Australia

Tel: +61 2 6154 9322

www.kas.de/australia

Design, Layout and Typeset

Swell Design Group

Paper

ecoStar+ is an environmentally responsible paper. The fibre source is FSC Recycled certified. ecoStar+ is manufactured from 100% post consumer recycled paper in a process chlorine free environment under the ISO 14001 environmental management system.

This edition, a collection of contributions from Australia and Germany, is concerned with emerging trends, challenges and patterns in cybersecurity that are relevant for both countries. The publication is framed by a conceptualization of cyberspace as a realm of converging and diverging forces and interests: technological, social, political, economic, institutional, cultural, ideational/ideological and strategic. These co-exist, compete and act upon each other – forming a complex ecosystem of dynamic, interlinked threat and opportunity vectors. This is based on the recognition that viewing cybersecurity as a mainly technological matter would be reductionist and fail to capture the complexity of a space created and shaped by humans.

KONRAD ADENAUER STIFTUNG

Konrad-Adenauer-Stiftung (Australia) Limited
Regional Programme Australia and the Pacific

11/3 Sydney Avenue
Barton ACT 2600
Australia

Connect

Telephone +61 2 6154 9322
Website kas.de/australia
Social facebook.com/KAS.canberra
linkedin.com/company/konradadenauerstiftungaustralia