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

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

RECYCLED
Paper made from recycled material
FSC® C102086
www.fsc.org

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.