

TOWARDS A DATA-CENTRIC GREAT GAME

**NEW CHALLENGES FOR SMALL STATES IN CONTEMPORARY
POWER POLITICS**

Valtteri Vuorisalo & Mika Aaltola



TOWARDS A DATA-CENTRIC GREAT GAME

NEW CHALLENGES FOR SMALL STATES IN CONTEMPORARY POWER POLITICS

- Technology is taking centre stage in power politics. In particular, the ability to refine and utilize data increasingly correlates with the transforming global distribution of power.
- The world is gravitating towards US and Chinese hubs of refined data. The convergence of data towards these two hubs accelerates the divergence of states into the haves and have-nots of data, and is likely to result in a realignment of partnership systems.
- Standards which enable data convergence also create forms of governance and regulatory spaces that challenge the shape and dynamic of traditional global governance.
- While recent Finnish security reports recognize the importance of new technologies and the cyber domain, data-centricity is not fully embraced either in policy or in practice.
- As the technology sector grows in significance, new forms of relationships between states as well as public and private organizations need to be envisioned and established.



VALTTERI VUORISALO

Professor of Practice

Faculty of Management and Business

Tampere University



MIKA AALTOLA

Director

Finnish Institute of International Affairs

ISBN 978-951-769-706-4

ISSN 1795-8059

Language editing: Lynn Nikkanen

Cover photo: Piqsels

TOWARDS A DATA-CENTRIC GREAT GAME

NEW CHALLENGES FOR SMALL STATES IN CONTEMPORARY POWER POLITICS

INTRODUCTION

The goal of every nation's security and defence policy is to maximize its ability to act in all security scenarios. This is underscored in the Finnish Government's Defence Report 2021.¹ Yet, as leading states develop and deploy a growing number of off-set data-driven technologies to maintain asymmetric advantages over their competitors, the task is arguably increasingly challenging and less understood in practice – especially by smaller states.

The US Department of Defense's 2020 Data Strategy² rightly recognizes that in today's world, data is the “primary and permanent asset” with which global influence, security and prosperity are ensured. It is clear that a data-centric approach is the core element in the ongoing geopolitical competition as “an essential and integral part of the [national security] mission itself”.

The key to a data-centric approach is the alchemy of turning data from a passive element into a more dynamic, smarter, and more refined entity. The move to a data-centric approach, where data is the key resource and enabler of desired outcomes, is not a simple technical upgrade. Rather, it is a profound transformation of organizational culture whereby trusted, dynamic collaboration between siloed entities is a fundamental necessity in order to understand and plan for the types of data and data formats that exist and that are needed in an organization.

Naturally, the move to data-centricity involves technological activities as well. Yet instead of involving infrastructure-wide and massively expensive big bang upgrades, a more subtle and accessible mixture of existing legacy systems, new technologies, and cross-platform data flows can be utilized to create defensive and offensive capabilities for interstate competition, for example. Instead of being out of reach for smaller actors, this type of multi-modal approach enables a new way of looking at data and understanding it not only in terms of something to be secured, but in terms of catalyzing it for proactive capabilities and deterrence.

Data-driven technology is evolving exponentially and, accordingly, we are witnessing accelerating competition on the world stage, where the stage itself and the norms bound to it are simultaneously transforming. For example, the stage is increasingly inhabited by actors who are not constrained by wishful public statements to forego abusing (digital, financial, informational, and other) interdependencies. Moreover, to add insult to injury, these interdependencies are too often governed by rules which are animated by drivers that do not fit existing understandings of defence, security or resilience.

As a result of these structural transformations, the nature of distributional capabilities is changing as the US and China engage in intensifying strategic competition in all domains, and as other traditional and emerging actors try to stay in the game or mitigate the implications of the overall radical shift. Yet the rapid evolution of data-driven technologies is propelled by US market-based and Chinese state-centric companies, whose influence and power grow as they develop new markets, technologies, and standards, which govern these technologies and – through them – the new human activities that these technologies enable. This is a de facto form of power and disaggregated governance. It erodes and challenges the traditional rules-based international order in which standard-setting has typically, with delay, been conducted via international organizations, where major states have held sway.

The complexities and potential trajectories for offset options defy even the most informed strategic planners, and create friction, delay, surprise, dependency and vulnerability for all states. For example, the dynamics of convergence and divergence coexist. Contemporary data flows contribute to the convergence of traditionally clear boundaries of the domestic and foreign, virtual and real, and peace and war. This multiplies the aspects of operational opportunity, enabling full-spectrum and multi-domain operations. Further, the technological evolution enables (expensive) platforms that merge multiple capabilities with interdomain implications such as the 5th generation fighter aircraft platforms. At the same time, it enables the creation of (cheap) single-purpose platforms such as micro-drones. Both developments are enabled by the convergence of data.

1 Valtioneuvosto, 'Valtioneuvoston Puolustuselonteko', 2021, <https://valtioneuvosto.fi/delegate/file/94720>.

2 Department of Defense, 'DoD Data Strategy', 2020, <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>.



U.S. Army Cyber Command Soldiers participating in a cybersecurity exercise in May 2021.
Source: José Cole/U.S. Army Cyber Command

This Briefing Paper is intended as a timely input into the emerging discussion on how the rapid evolution of technology creates previously unhighlighted consequences, which limit a nation's ability to act in all security scenarios. To illustrate our arguments, we highlight select strategic-level global phenomena and examples pertaining to more local national security contexts. Special attention is paid to the rise of data-centricity and the way that Finland, as a small actor, has taken initial steps towards it. First, we will briefly examine how different states are reacting to the increasing role of technology. Second, we will elaborate on the notion of data-centricity and key trends related to data, which impact a state's ability to act. Third, we will analyze how two recently published Finnish security policy reports take data-centricity into account. Finally, we will conclude with thoughts and considerations for the future.

STATES, POWER POLITICS, AND TECHNOLOGY

Information technology, as an enabler of data flows, is becoming the prime instrument for statecraft and strategic competition among states and non-state actors more broadly. It has become a tool with which states project sovereign power and gain economic, political and

security advantages, and a tool with which international norms and the world order itself can be reshaped.³

The United States, through its public and private sectors and academia, continues its determined focus on producing offset technological innovations, which give it an operational advantage. Gathering, refining, and analyzing data is seen as the prime ingredient for the desired effects, and the US continues its efforts to secure access to data through diplomatic, legislative, and clandestine means, even as more and more data is also gathered through public-private partnerships. Moreover, the US is working in collaboration with the EU to ensure that technology continues to serve interests on both sides of the Atlantic. Security and privacy concerns as well as the misuse of technology are given special attention in ongoing democratic debates on regulating the private and public gathering of data.

Meanwhile, China is growing in systemic significance. Western countries often accuse China of engaging in espionage and illicitly collecting data through various technologically enabled means. But China has a broader set of assets in systemic competition, which include an expanding economy, investments made in technology, and its determined security posture. Yet one of its advantages is often overlooked: the amount of data it

3 HM Government, 'The Integrated Review 2021', <https://www.gov.uk/government/collections/the-integrated-review-2021>.

can collect from its population and utilize, for example for AI training purposes, without the limitations of Western norms and values. This gives China a unique advantage in innovating new data-centric solutions which bring human behaviour patterns to the fore.

The US and China are not alone in the game. While Russian technological capabilities are often underestimated or criticized, Moscow has sought to establish a Russia-centric digital ecosystem and, perhaps more importantly, has been successful in producing innovative inter-domain operational manoeuvres in political, strategic, and military spheres abroad. Most notoriously perhaps, Russia has managed in recent years to take advantage of democratic (digital) vulnerabilities and to project power in and through the cyber domain – for example in the form of gathering intelligence, distributing disinformation and, accordingly, intensifying political and cultural clashes in societies it views as adversarial. Further, a range of regional powers, such as Israel and Turkey, are arguably keen to gain access to data, often through spying logics in the cyber domain in particular. This was witnessed recently when the Pegasus spyware was used to target heads of state, activists and opposition members in various countries. Market-based solutions are internationally available, with Pegasus highlighting Israel's advanced cyber know-how in particular.⁴

DATA-CENTRICITY, CONVERGENCE, AND DIVERGENCE

Technology is arguably changing the rules and means of systemic competition. Yet technology cannot fulfil its promise without data. Provokingly, one could argue that technology exists only to enable data flows. Herein lies the challenge: even if technologies could enable smooth data flows in theory, different datasets, poor data quality, scalability issues, and organizational processes and regulation hinder this. In consequence, refined interoperability is not fully achieved or even allowed, and the goals of fluidity and agility are not met.

Understanding the dynamics of data is of critical importance to security authorities in particular, since their success depends on getting the right, secured data to the right place at the right time, while they are simultaneously challenged by organizational obstacles,

debates over jurisdiction, and lack of interoperability.⁵ Yet there is more to data.

Even data is useless if a “vision for data” is missing. As the ability to integrate and refine data becomes the most important ingredient for success, it is imperative that we understand what kind of data is important, what trade-offs are required to gain access to it, and what the impact of new data on old data is. Too often there is no appointed authority that could govern and curate the utilization and optimization of data. If data is the key strategic resource, a vision for how to utilize and refine it should accompany it, instead of the predominant focus on data-protection practices that usually lag behind existing infiltration practices.⁶

Central to the vision for data is the notion of “data-centricity” as an evolutionary step from “network-centricity”. The key premise in the network-centric doctrine is that the role of data is to support platforms. In a data-centric doctrine, this notion is reversed: it is the role of the platform to gather data and ensure its smooth flow (to and from other platforms). This requires that data is placed at the heart of all strategic thinking. This seemingly small change of perception has huge consequences: it impacts how activities are planned, trained for, executed, and evaluated. It impacts the procedures of collaboration and the roles people have in organizations.

Data and divergence

One consequence of the convergence-divergence discrepancy is “relocalization”, where the promotion of the interests of one's own state or political bloc is given primacy over that of others. This is based on various factors and concerns. Power through regulation is one of them. For example, market areas – most notably, perhaps, the EU – can regulate access to their markets based on policy-related reasons.⁷ This decoupling at the policy level affects the geographical separation of markets and production areas. The finance sector is particularly dependent upon regulation, which ensures awareness over data flows. However, ungoverned and “black” data flows are increasing (e.g. via organized crime and crypto-currencies), and they propel vulnerabilities for regulatory actors as

4 BBC, ‘Pegasus: Spyware sold to governments “targets activists”’, 19 July 2021, <https://www.bbc.com/news/technology-57881364>.

5 Valtteri Vuorisalo, ‘Ketterät kehitysohjelmat vauhdittavat digitalisaatiota’, Viestimies, publication by The Signals Officers' Association, 72, issue 1 (Raisio: Newprint Oy, 2017).

6 NATO, ‘The Secretary General's 2020 Annual Report’, 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/sgar20-en.pdf.

7 Thomas Raines, ‘Raise the Bar by Leveraging the EU's Regulatory Power’, 12 June, 2019, <https://www.chathamhouse.org/2019/06/raise-bar-leveraging-eus-regulatory-power>.

their ability to “see” is intentionally blurred and made passive through inevitable regulatory delays.

Data and convergence

A further dynamic of decoupling is related to the ownership of data. If refined data is the new strategic resource, we need to understand where we can find it.⁸ Broadly speaking, there are two main hubs of data in the world, made up of US and Chinese companies with different public-private relationships. Both governments seek to ensure their access to the data gathered by actors in the respective hubs. The convergence of data to these two hubs accelerates the division of states into the haves and have-nots of data. It is also a driver in the geopolitical re-alignment of states.

From a European perspective, this is worrying. For example, there is no major cloud service provider owned by EU-based entities. Consequently, in this new data-centric reality, the EU’s relative power is in decline as it cannot lay claim to local “data fields” (as analogous to oil fields).

The EU is typically seen as a regulatory power, insofar as the source of its power is the ability to control access to a market of 400 million people. If data is the new source of wealth and influence, one can also ask what the feasibility of the EU’s digital regulation would be in the future. There are at least two reasons for this. First, the EU’s current regulatory process cannot keep up with the pace with which new technologies and data flows are created. Second, as data is the new source of strategic wealth, investors are likely to evaluate what is the most cost-effective and normatively sustainable way to acquire it. Bluntly put, is it “drilling for data” in a market of 400 million people, which is intensely regulated and bureaucratic, or should the focus be on the potential of the billions outside the Union, whose activities and data are not as regulated?

Divergence of actors

The new, data-centric world opens doors for new non-state actors, and to new coalitions of state and criminal non-state entities. Further, global technology companies are growing in social, economic, political, and even geopolitical influence.

The staggering amounts of data they have access to is their main source of influence. In addition, the fact that they are in a prime position to shape the new standards of communication and collaboration creates new and sometimes unforeseen means of societal influence that tend to travel across state borders. For example, companies impact how we interact with the world, and they are effectively becoming new sources and interpreters of the “real” for us.⁹

Moreover, technology is not only an enabler but also a source of threats, which need to be responded to. This poses a further challenge to governance systems, which need to find ways in which their capabilities match the latest technologies. This demands governance systems to be able to compete with the best talent, which is currently drawn to large corporations, start-ups, and even criminal enterprises with competitive compensation. As the private sector – both licit and illicit – grows in capability, it becomes an attractive partner but also a potential systemic challenger.

Convergence of actors

To sustain a strategic advantage through technology, new partnerships, standard-setting mechanisms, and co-creation and resource-pooling methods across public and private sectors and friendly nations are needed. Through such actions, the integration of key data flows can be achieved, which, in turn, translates into enhanced means to use power. Yet this is no easy task, but one that requires planning, time, skills, and money.

It should be noted that organizational and procedural issues emerge when new technological capabilities are introduced into old ecosystems. Existing mission-critical technologies cannot simply be removed. This adds to the complexity and demands an understanding of the inter-relationships between old and new technologies, and of the outcomes which both are intended to produce. In the absence of a tailored data-centric vision, this understanding is rarely achieved, which results in capability overlaps and gaps, and in a delay in a nation’s ability to act.

8 The Economist, ‘The world’s most valuable resource is no longer oil, but data’, 6 May, 2017, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

9 Valtteri Vuorisalo, ‘Algorithmic Life & Power Flows in the Digital World’, in M. Lehto, P. Neittaanmäki (eds.), *Cyber Security: Cyber power and technology* (Berlin: Springer, 2018).

Top scoring countries in the 2020 Global Cybersecurity Index (GCI)

Rank	Country	Score
1	United States of America*	100
2	United Kingdom	99,54
2	Saudi Arabia	99,54
3	Estonia	99,48
4	Republic of Korea	98,52
4	Singapore	98,52
4	Spain	98,52
5	Russian Federation	98,06
5	United Arab Emirates	98,06
5	Malaysia	98,06
6	Lithuania	97,93
7	Japan	97,82
8	Canada*	97,67
9	France	97,60
10	India	97,50

*No response to the 2020 GCI questionnaire. For countries that did not submit responses to the questionnaire, desk research was conducted through publicly available information on official websites and other resources.

Figure 1. Countries ranked in the top of the Global Cybersecurity Index (GCI) in 2020.
Source: The United Nations International Telecommunication Union (ITU).

DATA-CENTRICITY AND NATIONAL SECURITY IN FINLAND

Horizontal “inter-agency” collaboration has always been at the core of Finland’s security policy. Finland has also increasingly paid attention to the cyber domain: the Cyber Security Strategy was launched in 2013 and updated in 2019. With the introduction of the new intelligence laws in 2019, Finland’s capability to monitor and govern data flows has arguably increased.

Two influential reports on Finland’s national security and its future have been published recently, namely the Finnish Government’s Defence Report 2021 and the Finnish Security and Intelligence Service’s

National Security Overview 2021¹⁰. They recognize the importance of new technology and the cyber domain, but do not take a data-centric view, the like of which was discussed above. In fact, the Defence Report leaves the role of data undiscussed altogether. This contrasts with the UK Ministry of Defence’s Digital Strategy, for example, which sees data and its exploitation as critical elements that will “revolutionize warfare and transform defence”.¹¹ Finland’s National Security Overview fares slightly better and recognizes the role of data, but

¹⁰ Finnish Security Intelligence Service, “The National Security Overview 2021”, <https://supo.fi/en/national-security-overview>.

¹¹ UK MOD, ‘Digital Strategy for Defence: Delivering the Digital Backbone and unleashing the power of Defence’s data’, 2021, <https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data>.

mostly in relation to the data security of organizations which are responsible for critical functions in society. This illustrates a passive form of resilience rather than a more proactive vision of future challenges by active outside actors.

Using the conceptualization laid out above, we can dive deeper into how mature these reports are in relation to data-centricity:

1. Data-centricity, divergence, and convergence.

The Defence Report does not place emphasis on data. The word “data” is only mentioned when defining the cyber domain. Securing network and infrastructure services which enable data flows are mentioned, as is the need to secure storage (for data). Many other tasks, which need to be resolved to derive value from data, are not mentioned. These include resolving the question of data interoperability (with methods other than standards), the capabilities required for data curation and management mechanisms, and tools of data exploitation, to name just a few examples.

Moreover, in the Defence Report, the question of how new technologies impact people within the organization is only discussed from the perspective of conscript and reservist training needs. What is missing is a reflection on how existing staff will need to be constantly trained to meet the emerging challenges.

The National Security Overview, however, does take data into account when it is examined instrumentally, as a resource to be protected and secured by organizations responsible for critical functions in society. Further, data and information are elevated to the category of critical infrastructure. Information infrastructure is seen as a gateway to Finnish data.

2. Divergence of actors.

The National Security Overview recognizes the growing number of actors in the security system by focusing on cybercrime and terrorist actors in particular. The Defence Report examines the actors from a wider perspective, especially from the perspective of securing access to critical skills, which are needed to produce and integrate new technologies in all security scenarios. As the private sector is the source of technology and skills, its importance and systemic influence is expected to increase. This also holds true when it comes to new

technological standards. Interestingly, the Defence Report does not discuss the impact of evolving standards or new forms of governance, but simply states that interoperability is ensured through the implementation of international standards.

3. Convergence of Actors

The Defence Report sees that collaboration with all actors in society is the backbone of defence. Countering attack vectors on a grand scale necessitates the establishment of strategic foresight and readiness in collaboration with other governmental actors, the private sector, and national and international organizations and partners. Moreover, the Defence Report recognizes that the private sector is the main driver for many new technologies. Collaboration is needed to ensure access to and skills for these technologies. The role of new legislation is highlighted in this activity. Yet the Report does not pay attention to the fact that technologies evolve faster than the legislation attempting to govern them.

CONCLUSION

As technology and data-centric implications emerge and evolve quickly, and as states struggle to keep up, we are caught between convergence and divergence, and between fast technological and slow regulatory and policy change. The collision points of these dynamics are likely to be sources of nasty surprises, friction and disruption going forward. Many questions duly arise as a result.

First, slowness in government has traditionally ensured checks and balances. Today, the rapid evolution of technology has a huge impact on a nation's ability to act in all security scenarios. Is slowness in government an advantage or would quicker legislative or regulative action be of benefit – especially if the latter is seen as a source of power and influence?

Second, novel software solutions, which challenge our existing platforms and applications, can evolve in months, even if the hardware encapsulating them can last for decades. How do we ensure security of supply of the skills that are needed to develop and operate critical systems that bring together the hardware and application aspects and related temporal dynamics?

Third, the exponentially increasing volume of data is the backbone of our way of life, and staggering amounts of it are created daily. In the past, critical resources have been stable and identifiable. How do we treat data as a critical resource when it is constantly growing and evolving?

Finally, as technology and data evolve, new forms and frontiers of human activity are simultaneously created and established. How do we create new democratic models of governance and jurisdiction for these new domains and activities, where the logics of

action do not follow the old precedents?

To answer these questions, new forms of collaboration are needed. The future is so complex and serendipitous that small states cannot imagine approaching it without taking advantage of all of the capabilities that are available in society. Vertical, siloed operating models need to be replaced with new, more horizontal activities which utilize capabilities in the public sector, private sector, and academia. As the world stage continues to evolve, only one thing is certain: if we keep doing old things, we will not get new results. /