Metábasis.it
PHYLOSOPHY AND COMMUNICATION

ONLINE INTERNATIONAL JOURNAL OF PHILOSOPHY
WITH *PEER REVIEW*
WWW.METABASIS.IT
November 2023 year XVIII n. 36

THE IMPACT OF ARTIFICIAL INTELLIGENCE AND DATA ON POLITICAL POWER AND GEOPOLITICAL EQUILIBRIA

DOI: 10.7413/18281567256

by Paolo Bellini - Università degli Studi dell'Insubria, Varese-Como
Edoardo Campanella - Harvard Kennedy School
Alessandro Piccioni - Università degli Studi dell'Insubria, Varese-Como and Nexi Group

Abstract

Navigating the governance of macroscopic changes presents an inherently multifaceted challenge. Analogous to the resistance encountered during organizational transformations by employees, every societal shift – be it a technological revolution or alterations in technical and cultural landscapes – elicits significant skepticism and distrust among the populace. Recent global upheavals, such as the COVID-19 pandemic and the conflict between the Russian Federation and Ukraine, have polarized societies, particularly affecting nations with a lesser degree of cultural preparedness and minimal levels of mutual trust. The advent of the digital revolution, transforming modes of work and consumption, alongside historically significant events like wars and pandemics, invariably triggers a resurgence of nostalgic nationalism.

Keywords: Information, Power, Geopolitics, Intelligence, Ethics.

Introduction

In 1983, in the midst of the Cold War, Stanislaw Petrov, then a Russian general, was asked to replace the duty officer at the bunker located near Moscow *Serpuchov 15*. General Petrov's task was to monitor the OKO satellite system placed to guard U.S. missile sites, interpreting and verifying its data, in order to inform his superiors of a possible nuclear attack against the Soviet Union [1]. In the event of detecting an assault by Western forces, the USSR's doctrine mandated an immediate, comprehensive nuclear retaliation against the United States, encapsulating the Cold War's doctrine

of *mutual assured destruction* [2]. Just after midnight, Petrov detected the launch of five missiles from the United States, headed toward Russian territory. Considering the U.S. attack to be too small compared to their weapons endowments, Petrov decided to declassify - correctly - the signal received as an error of the monitoring system. This assessment, in very good probability, averted a catastrophic military escalation.

This episode highlights the critical importance of data and information management in shaping strategic decision-making and altering the power dynamics among nations throughout history. For illustration, consider the use of Caesar's cipher, an encryption technique employed by the Roman general Julius Caesar. Caesar, cognizant of the strategic value of secure communication, utilized this cipher to safeguard messages sent to his military commanders. [3].

When juxtaposing the information management challenges of yesteryears with today's context—marked by an exponentially greater volume of data, enhanced accessibility, rapid dissemination capabilities, and sophisticated predictive analytics—it becomes evident that relying solely on human intuition for data governance is inadequate. This paradigm shift necessitates a re-evaluation of current methodologies and the implementation of precise governance policies and standards to ensure the prudent management of information in an era dominated by digital proliferation.

Data and power

Following Italy's decision to send arms to Ukraine, the Russian Federation's government issued a retaliation threat against Italy. This threat was historically unique as it did not foresee a traditional attack on strategic infrastructure, nor did it initially involve rationing the natural resources Italy imports from Russia. Instead, the threat entailed the potential release of confidential data and information about public figures and political leaders.

Gauging the actual power behind such aggressive and threatening rhetoric is challenging, not only due to the difficulties in verifying the extent of the threats posed but also because of the inherent complexities associated with defining power and its underlying dynamics.

In *The Changing Nature of World Power* [4], the author, Prof. Nye, says verbatim:

> Power in international politics is like the weather. Everyone talks about it, but few understand it. Just as farmers and meteorologists try to forecast storms, so do leaders

> and analysts try to understand the dynamics of major changes in the distribution of power among nations. [...] Power, like love, is easier to experience than to define or measure.

Nevertheless, it is clear from what the government institutions of the Russian Federation have expressed: information governance is a key lever for managing political power and protecting its position in the global geo-political balance.
Academic research in this regard had largely predicted a transformation of power in a virtual, reticular and cyber-communicational sense.

> One can consider the many political units that populate the planet, nation-states, kingdoms, federal and confederal unions, etc., as hubs of a global network, aimed at managing the world's population. According to this paradigm, therefore, the power of any political-administrative aggregate would depend on the economic, military and communicational connections that bind it to others. Therefore, the political strength of such hubs would inevitably be linked to their connective capacity (internal and external) both on the industrial and financial level and on the terrain of consensus production, the construction of widely shared values, technological expansion and military intervention. These connections are in turn interpretable, quantitatively and in a purely material sense, considering roads, bridges, railways, energy supply networks, air and sea routes, the Internet, etc., and in an immaterial sense, observing the Web, the airwaves, etc. They are also qualitatively distinguishable according to the capacity of activation and control that each political aggregate possesses over them. [5bis]

Also in *The Changing Nature of World Power* [4], The author, Professor Nye, acknowledges that the sources of power for nations have evolved over the centuries and anticipates significant changes in the future. Writing in the 1990s, he predicted that the twentieth century would witness a rise in the importance of informational and institutional power, while military force would continue to play a critical role. Upon closer examination, this prediction appears to be accurate, as evidenced by Table 1, which outlines the major sources of power by century.

Revealing sensitive information constitutes one of the three primary methods of engaging an adversary. It's important to note that cyberattacks often target not individuals but the information systems of key infrastructures and businesses. These intrusions aim to manipulate or delete data, controlling access to disrupt business operations and the delivery of services.

Cyberwarfare has reached a scale in terms of involvement and the extent of direct and indirect damage comparable to traditional warfare. However, traditional warfare, such as naval battles, demands considerable preparation and expertise, leading to a significant asymmetry in offensive capabilities (for example, a U.S. Navy admiral possesses vastly more experience and strategic skills than a counterpart from an Eastern European country). In contrast, cyberwarfare is inherently simpler, with a higher success rate, requires less expertise, and leverages constantly evolving technologies, methodologies, and vulnerabilities. This levels the playing field among the actors involved, often allowing the use of resources outside official military programs. This aspect fuels the ethical-legal debate over its legitimacy, partly due to the involvement of loosely defined organizations and independent groups capable of executing effective cyberattacks.[6] .

The Italian economic system has faced significant challenges due to cybersecurity flaws, particularly among SMEs, which form the backbone of the country's economy and have been underprepared for large-scale ransomware attacks. Italy has experienced a high rate of ransomware attacks, leading the country to establish a dedicated government cybersecurity authority and specialized cyber defence teams[1]. For this reason, the government set a course whose first step was the establishment of a government authority dedicated to *cybersecurity* and the creation of specialized cyber defense teams. Significant investments have also been made concerning communications infrastructure[2] in relation to the computer networks[3] that businesses use *as-a-service*. This should ensure a system of protections in line with European regulations and provide greater cybersecurity in general.

Another prevalent form of cyberwarfare involves exploiting digital tools, sensitive data, and knowledge of specific historical-political contexts to influence public opinion via the media. In this

[1] https://www.ansa.it/sito/notizie/tecnologia/software_app/2022/07/13/cybercrime-a-maggio-italia-prima-in-europa-per-ransomware_f64dd5dd-433b-4293-91f2-2ed42364cc74.html

[2] https://www.huffingtonpost.it/economia/2022/08/01/news/fastweb_contro_tim_sul_cloud_di_stato_parte_lo_scontro_legale_tra_le_cordate-9974868/

[3] https://www.ansa.it/sito/notizie/ansa_eventi/2022/06/14/google-cloud-presenta-2-nuove-basi-a-milano-e-torino_79883a6d-7867-4781-b8b4-e27b3a3a3da1.html

case, the *mediasphere* is widely used, by the major planetary political powers, as an indirect weapon to try to constitute a *soft power* [5] exercised through targeted propaganda actions, dissemination of *fake news* and systematic censorship of information sources managed by those who from time to time assume the traits of the enemy. These types of attacks are not necessarily configured within a context of war, but are perpetrated on an ongoing basis involving - truly or allegedly - all the most important socio-economic and political acts on the planet (e.g., the election of the president of the United States of America) [4].

The use of data for targeting adversaries represents just one facet of offensive strategies. Since 2020, the notion of normalcy has undergone a profound transformation. The COVID-19 pandemic has emerged as a significant global event, altering the daily routines, societal balances, and priorities of populations worldwide. Beyond the realm of public health management, the pandemic has necessitated widespread home confinement, disrupting the traditional modes of knowledge transmission and affecting an entire generation of school-aged children for over a year. In response, the field of biomedical sciences has been at the forefront, developing therapeutic strategies, prevention tools, and containment policies to combat the virus.

In this context, the exchange and management of information have assumed a pivotal role in ensuring the security of nations eager to conceal their unpreparedness and avoid the economic downturn resulting from decreased consumer spending. Furthermore, countries have recognized the value of sharing data and research findings in the hope of accelerating the recovery process from the pandemic and health crisis. In addition to the construction of shared algorithms to give a clear picture of the epidemiological evolution of the disease [9, 10], building solid data policies, both of collection and analysis and of data sharing, allowed the appropriate *sizing of social* and health services and the definition of behavioural rules that would allow the tightness of care systems and the correct *risk assessment* for the different segments of the population [11].

[4] https://www.nytimes.com/2021/03/16/us/politics/election-interference-russia-2020-assessment.html

Legal and regulatory framework

Data governance, information extraction and processing are key strategic processes whose impact ranges from *business models of* enterprises, to geopolitical balances between different countries. Setting a regulatory framework, which allows for citizen and consumer protection on the one hand, and appropriate *data sharing* practices on the other, which enhance data and information also through extra-territorial enlargement of data governance, is a complex and most urgent issue.

In recent years, in fact, jurisprudence has had to update itself radically. As an example, it raises an interesting reflection that in Roman law one of the most relevant punishments was considered *damnatio memoriae,* that is, the sentence of forgetting. This sentence stipulated that every trace, every piece of data, every piece of information referring to a convicted person should be erased. Today, however, oblivion is no longer a condemnation, it is a right enshrined by the European Union in the set of rules related to the protection of the dignity and privacy of the citizen [12].

On the other hand, the European Union's regulatory effort is a journey that consists of more than twenty years of regulatory production. Started with the publication of the *ePrivacy Directive* (2002) [22] and *GDPR - General data protection regulation* (2016) [18], it is still ongoing and sees, among others, two recent important measures regarding the publication of the proposal to regulate the use of artificial intelligence algorithms. The first known as the *AI Act* (2021) [15] is a synthesis of a set of Union and OECD acts [26] related to artificial intelligence [16, 17]. The second is a proposal for data management and sharing called the *Data Governance Act* (2020) [23]. The latter in particular lays the groundwork for ushering in a broader common regulation of oversight and sharing. It expresses the idea that digital sovereignty, is not based on isolationism, but on collaboration and openness to other countries that balances the free flow of data itself. This culminates in the proposed creation of a common digital territory for the European Union, the United States of America and any high state that wishes to join.

Another important step in the direction of a transatlantic digital pact is the recent *Declaration for the Future of the Internet* (2022) [24], proposed by the White House and signed by sixty states. The document commits the signatories to the creation of a single, open global Internet capable of promoting competition, privacy, respect for human rights and fundamental freedoms, as well as the free flow of information and inclusive and sustainable connectivity, with the aim of distributing the benefits of the digital economy as widely as possible.

However, new technologies, and in particular everything related directly or indirectly to digital systems, present *policy makers* with more than one *trade-off* and difficulty [13, 14].

In the first instance, regulations that have validity over territories so wide in scope and with such a heterogeneous cultural background are very difficult to imagine. Indeed, in *The Moral Machine Experiment* [25] scientists at the MIT Media Lab showed how ethics is *geography-specific,* that is, there are *cultural-clusters* with respect to the identification of what is good and what is bad, what is right and what is wrong. A cross-cultural one-fits-all regulation that is shared by all is therefore very difficult to conceive- and for now-the jurisprudential approach of different states is still very diverse.

In the second instance, while in one respect the risk of under-regulation relates to the failure to protect citizens, over-regulation risks exacerbating the already high levels of resistance of companies and populations in embracing new technologies by slowing down scientific research.

A possible solution

Safeguarding citizens' rights and ensuring equilibrium among nations are increasingly contingent upon adept governance of data and information. It is clear that no singular measure can fully address this multifaceted issue. Hence, a tripartite approach is proposed to lay down a technological and legal-cultural foundation for bolstering digital sovereignty, in its most comprehensive interpretation.

Firstly, an ongoing effort is required to enhance technological and institutional frameworks. This foundational step is critical for establishing a robust infrastructure capable of supporting digital sovereignty initiatives.

Secondly, regulatory measures need to be introduced or expanded upon, complementing those proposed by the European Union [19], with a particular focus on the domain of intangible assets, data being the foremost among these. Traditional perspectives on strategic state assets have been predominantly confined to physical assets such as airports, power plants, and logistical infrastructures. However, the increasing strategic significance of digital assets has not been adequately recognized or protected by existing legal frameworks.

Third, a decisive cultural shift is necessary to empower citizens to comprehend the significance and value of data protection. The Digital Economy and Society Index (DESI) report, annually published by the European Commission, highlights a concerning deficit in digital skills within populations, exemplified by Italy's poor performance. This deficiency leaves citizens vulnerable to various cyber

threats and diminishes their capacity to perform basic critical actions, such as verifying the authenticity of information. Moreover, the general populace's struggle to grasp complex concepts related to automated information processing exacerbates resistance to utilizing and managing advanced digital tools. This resistance is not unprecedented; historical analogs, such as the Luddite movement of the 19th century, illustrate similar pushbacks against radical technological changes, now reemerging in a contemporary digital context. [20, 21].

Conclusions

Navigating the governance of macroscopic changes presents an inherently multifaceted challenge. Analogous to the resistance encountered during organizational transformations by employees, every societal shift—be it a technological revolution or alterations in technical and cultural landscapes—elicits significant skepticism and distrust among the populace. Recent global upheavals, such as the COVID-19 pandemic and the conflict between the Russian Federation and Ukraine, have polarized societies, particularly affecting nations with a lesser degree of cultural preparedness and minimal levels of mutual trust. The advent of the digital revolution, transforming modes of work and consumption, alongside historically significant events like wars and pandemics, invariably triggers a resurgence of nostalgic nationalism. This sentiment serves as a refuge for globalized communities, longing for a bygone era marked by the absence of digital intrusion, impermeable national frontiers, and a perceived greater capacity of governments to safeguard their constituents.

Therefore, the mere establishment of infrastructure and standards proves inadequate in guaranteeing compliance with policies aimed at safeguarding a state's intangible assets. Such policies must be complemented by comprehensive digital literacy initiatives that engage the entire citizenry, fostering a more informed and resilient society in the face of technological and societal transformations.

Bibliography

[1] Chan, S. (2017). Stanislav Petrov, Soviet Officer who helped avert nuclear war, is dead at 77. *New York Times*, *18*.

[2] Sokolski, H. D. (Ed.). (2004). Getting MAD: nuclear mutual assured destruction, its origins and practice. *Strategic Studies Institute, US Army War College.*

[3] Luciano, D., & Prichett, G. (1987). Cryptology: From Caesar ciphers to public-key cryptosystems. *The College Mathematics Journal*, *18*(1), 2-17.

[4] Nye, J. S. (1990). The changing nature of world power. *Political Science Quarterly*, 105(2), 177-192.

[5] Nye, J. S. (1990). Soft power. *Foreign policy*, (80), 153-171.

[5bis] Bellini P. (2011) *Mitopie tecnopolitiche. Stato.nazione, impero e globalizzazione*, Mimesis, Milano - Udine 2011, 73.

[6] Dipert, R. R. (2010). The ethics of cyberwarfare. *Journal of Military Ethics*, 9(4), 384-410.

[7] Campanella, E., & Dassù, M. (2019). Anglo nostalgia: The politics of emotion in a fractured West. Oxford University Press.

[8] Campanella, E., & Dassù, M. (2019). Brexit and nostalgia. *Survival*, 61(3), 103-111.

[9] Pastor-Satorras, R., Castellano, C., Van Mieghem, P., & Vespignani, A. (2015). Epidemic processes in complex networks. *Reviews of modern physics*, 87(3), 925.

[10] Pastor-Satorras, R., & Vespignani, A. (2002). Epidemic dynamics in finite size scale-free networks. *Physical Review* E, 65(3), 035108.

[11] Khalatbari-Soltani, S., Cumming, R. C., Delpierre, C., & Kelly-Irving, M. (2020). Importance of collecting data on socioeconomic determinants from the early stage of the COVID-19 outbreak onwards. J *Epidemiol Community Health*, 74(8), 620-623.

[12] Rodotà, S. (2012). The right to have rights. *Gius. Laterza & Sons Spa*.

[13] Marseglia, G. R. (2021). AI Act: impacts and proposals. *Semiannual online journal: www.i-lex.it.*

[14] Marseglia, G. R., Dal Mas, F., Massaro, M et al (2021).; "The Artificial Intelligence Act: practical implications of the ethics of Artificial Intelligence"; in Vjollca Kopsaj (ed.), "Issues in Practical Philosophy 2021". Pavia, Printservice publisher; ISBN: 9788898765980.

[15] European Commission, "Proposal for a regulation of the Europe-an Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts." 29.4.2021. European Union (2021).

[16] European Commission, Directorate-General for Communications Networks, Content and Technology, "Ethics guidelines for trustworthy AI," Publications Office, 2019, https://data.europa.eu/doi/10.2759/177365

[17] European Commission, "White paper on Artificial Intelligence - A European approach to excellence and trust," 19.2.2020, COM (2020).

[18] European Parliament, "Regulation 2016/679 of the European Parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." 27.4.2016. Official Journal of the European Union (2016).

[19] European Commission, "The Digital Economy and Society Index," European Union (2021).

[20] Jones, Steven E. "Against technology: From the Luddites to neo-Luddism." Routledge, 2013.

[21] Kaczynski, Theodore John. "Industrial society and its future." (1995).

[22] European Parliament, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic

communications sector (Directive on privacy and electronic communications). 31.7.2002. Official Journal of the European Union.

[23] European Parliament (2020), Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act).

[24] White House (2022), A declaration for the future of the internet. Available at: https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf

[25] Awad, E., Dsouza, S., Kim, R., Schulz, J., Henrich, J., Shariff, A., Rahwan, I. (2018). The moral machine experiment. *Nature*, 563(7729), 59-64.

[26] Yeung, K. (2020). Recommendation of the council on artificial intelligence (OECD). *International Legal Materials, 59*(1), 27-34.

[27] Campanella, E. (2021). Social Capitalism.

Period	**Leading State**	**Major Resources**
Sixteenth century	Spain	Gold bullion, colonial trade, mercenary armies, dynastic ties
Seventeehth century	Netherlands	Trade, capital markets, navy
Eighteenth century	France	Population, rural industry, public administration, army
Nineteenth century	Britain	Industry, political cohesion, finance and credit, navy, liberal norms, island location
Twentieth century	United States	Economic scale, scientific and technical leadership, universalistic culture, military forces and alliances, liberal international regimes, hub of transnational communication

Metábasis.it
PHYLOSOPHY AND COMMUNICATION

ONLINE INTERNATIONAL JOURNAL OF PHILOSOPHY
WITH *PEER REVIEW*
WWW.METABASIS.IT
November 2023 year XVIII n. 36

MIMESIS
Sesto San Giovanni (MI)
via Monfalcone, 17/19

AlboVersorio Edizioni
& AlboVersorio Edizioni
di Ass. NonsoloSophia
nonsolosophia@gmail.com

Autorizzazione del Tribunale di Varese n. 893 del 23/02/2006.
ISSN 1828-1567