The middleware dilemma of middle powers: AI-enabled services as sites of cyber conflict in Brazil, India, and Singapore

Sukumar, A.M.; Broeders, D.; Cristiano, F.; Delerue, F.; Douzet, F.; Géry, A.

5 The middleware dilemma of middle powers

AI-enabled services as sites of cyber conflict in Brazil, India, and Singapore

Arun Mohan Sukumar

Introduction

Although no accepted definition of the term exists, "middle powers" includes those countries that exercise a high degree of economic sovereignty,[1] and strongly influence regional developments through their political, economic, cultural, or military capabilities. Middle powers may also influence rule-making in specific domains of global governance. Notably, these countries tend to favor the *status quo* of the liberal international order, preferring to engage multilateral regimes and seek accommodations from them as needed, rather than challenging those regimes or the broader, hegemonic interests that underpin them.[2] "Middle powers" encompasses both developed and developing countries. Indeed, the term is as much a reflection of states' material capabilities as it is of "normative and behavioral criteria."[3] Middle powers aspire to maintain and elevate their international status. Technological leapfrogging – the adoption by developing countries of frontier technologies for governance, skipping in the process older-generation technologies that are either resource-intensive or unscalable – figures prominently in this pursuit of status.[4] Leapfrogging, whether through the adoption of GSM telephony, IPv6, or 5G, has not just been viewed as a sustainable path to economic prosperity. It is also a totem of empowerment for middle powers, allowing them to participate on equal footing with Great Powers on Research & Development, standard-setting, and application of new technologies for their own requirements.

Artificial Intelligence and Machine Learning (AI/ML) represent one such frontier technology. Since the publication of the world's first national AI strategy in 2017 by Canada – a self-described "middle power"[5] – no less than 54 countries have either announced or are in various stages of declaring their own national strategies.[6] Several of these strategies, especially those drawn by middle powers, emphasize the importance of AI in leapfrogging hurdles to the delivery of services in sectors such as healthcare, education, transportation, and e-commerce. In particular, they underline the need to take advantage of vast troves of data generated by their population to train

DOI: 10.4324/9781003284093-7

predictive algorithms and develop ML models for the efficient delivery of said services. Given the costs and limited availability of high-skilled workers to train healthcare professionals, lawyers, and educators, among others, emerging markets may seek to replace them with AI-enabled 'bots.'

A review of national AI strategies suggests states may pursue one of two paths to promote innovation and adoption of AI-enabled services. Some countries may choose to "make public datasets available" for market players to develop proprietary AI-enabled services, and concurrently, set up regulatory sandboxes to pilot those products.[7] Other states may opt to leverage their Digital Public Infrastructure (DPI), i.e., public technical standards and protocols that allow third parties to access personal data of citizens or anonymized data, with clearly defined guidelines on the nature of data that can be shared, the duration of data sharing, as well as permissible use-cases.[8] Such infrastructure, which can be considered "middleware," then becomes the conduit for access of data to train AI/ML models. The "middleware" model is likely to be preferred by many states as it allows for more granular, revocable, and regulated data-sharing, rather than one-time access to public databases. Middle powers in particular may condition the use by market players of such middleware on their affordable provision of AI-enabled services in sectors such as health and education.

Examples of such middleware infrastructure developed by middle powers include protocols that standardize data-sharing (for example, Personal Health Records in Japan),[9] common and interoperable railroads for digital transactions (PayNow in Singapore,[10] Unified Payments Interface in India,[11] etc.), or unique digital identifiers, often validated by biometric markers (Aadhaar in India,[12] MOSIP in Philippines,[13] e-ID system in Estonia,[14] etc.). The leveraging of middleware DPIs towards AI-enabled services is in the early stages of conceptualization and implementation at the time of writing. Nevertheless, it is highly likely that middle powers that have made considerable advancements in building such infrastructure – Australia, India, Brazil, Norway, Japan, South Africa, and Singapore, to name a few – will rely on them to promote innovation and at-scale adoption of AI-driven services. Indeed, the high degree of standardization in data collection, labelling, and sharing through middleware DPIs makes it easier to develop and train ML models. DPIs also allow regulators to calibrate the nature of data collected, allowing in some cases for the sharing of scarce personal and population-level information, and minimizing the collection of potentially harmful information in others. These reasons make it probable that public, middleware infrastructure will be used to develop AI-based applications and services across the world. For instance, it is worth highlighting how the COVID-19 pandemic has accelerated the adoption of AI-enabled diagnostics that rely on data from contact-tracing applications or chest imaging databases built by states.[15] This trend will likely continue in the future, especially in middle powers that have created centralized national databases faster than advanced economies.

The development of AI-enabled products and services that rely on such middleware infrastructure also creates a dilemma for states. DPIs are heavily reliant on Application Programming Interfaces (APIs) that lay down technical specifications for data collection and sharing. In some cases, the middleware in question is nothing but an API, i.e., a few lines of code that allow public and private players to connect with each other and share data. Payment railroads are a common example of such APIs. In other instances, APIs are necessary to allow external applications to connect to the public infrastructure and retrieve data from its servers. With respect to AI-enabled services or products, APIs will be key to ensuring that ML models developed by third parties have access to the right data parameters in order to train their algorithms. Essential as they are to the adoption and scaling of digital infrastructure, APIs are also vulnerable to sophisticated cyber attacks. By their very nature, APIs are designed to facilitate the seamless integration of third-party applications with databases, cloud services, virtual networking functions, etc. The emphasis on ease of access has often come at the cost of secure API design.[16] In the case of AI-enabled services that run on public datasets or middleware infrastructure, this vulnerability is compounded by the fact that there is minimal human supervision of the interaction between the service and the user. As a result, attacks on AI-enabled services through APIs could seriously impair both the availability of the service as well as its predictive accuracy and effectiveness. Attacks against the availability or integrity of AI-enabled services may thus have the effect of undermining public confidence and trust in them, especially in developing countries and middle powers.

To be sure, APIs are potent vectors for cyber attacks wherever they are deployed. With API 'calls' comprising over 80% of the Internet's platform-led traffic, such vectors are omnipresent.[17] The role of APIs in linking DPI to AI-enabled services, however, makes them an even more lucrative target for state and non-state actors who seek not only entry into critical national databases, but also disrupt autonomous and minimally supervised platforms that provide essential services.

This chapter highlights how AI-enabled services running on public, digital infrastructure could emerge as vectors of cyber conflict. States face a difficult choice between opening up national databases or other public infrastructure to third parties in order to promote AI innovation atop its data and risking not only the security of those databases but also that of critical, even lifesaving, services. The "middleware dilemma" is most acute for middle powers, especially large emerging markets that are undergoing rapid industrialization but find themselves constrained by resources or capital to provide essential services at scale. As a result, they are compelled to turn towards digital or digital-enabled services, including AI services.

The chapter is organized as follows: section two explores the 'middleware dilemma' in detail, highlighting security risks associated with API deployment, and their increasing role in the training of AI/ML modes. Section three outlines efforts by three middle powers – Brazil, Singapore, and

India – to make available public data and digital infrastructure through APIs to promote AI innovation in their healthcare sector. Drawing on these national models and strategies, Section four presents an overview of threats and vulnerabilities faced by states in securing such services and their underlying infrastructure.

APIs and the "middleware dilemma"

The internet is witnessing unprecedented 'API-fication.' APIs are lines of code that allow software to communicate with each other, and thus facilitate greater connectivity and interoperability among the network, data, and application layers that make up cyberspace. With digital environments becoming increasingly heterogenous – most businesses and enterprises today delegate routing, data processing, and even cybersecurity functions to virtual networks and cloud services located halfway across the world – APIs have become crucial to the smooth functioning of critical internet services. Through their enabling role in the retrieval and processing of data at the application/device level, APIs have also been instrumental in realizing the "platform economy," as it is known today.[18] For the same reason, APIs have been key to the rapid expansion and proliferation of federated and centralized databases across the world. The DPI developed by middle powers such as Australia, Brazil, and India, to name a few countries, too depend on APIs for their implementation and use. Indeed, regulatory tools such as the 2018 Revised Payments Directive (PSD2) in the European Union and the 2020 Consumer Data Right Act in Australia require even private actors to provide standardized APIs so that user data is interoperable and seamlessly accessible by all authorized parties.

Despite their popularity, however, API security still leaves much to be desired. APIs have earned notoriety in recent years as attack surfaces for data breaches, identity theft and account takeovers, ransomware injections, IoT exploitation and DDoS attacks, among others.[19] One estimate suggests API attacks will emerge as the leading vector of cyber attacks by 2022. The security considerations involving APIs are three-fold: first, the widespread use of APIs results in a crowding of digital networks and infrastructure by third parties, making it difficult to manage or monitor the proliferating endpoints. Indeed, network administrators have no 'over-the-horizon' visibility with respect to third-party applications or devices that are constantly pinging their databases or infrastructure with API calls. Second, APIs may be developed by actors across the network, but there are no clear frameworks for accountability and remedial action in case of API-enabled attacks.[20] The poor maintenance and updating of APIs has even contributed to the phenomenon of 'zombie' APIs that continue to be functional (and potentially leak data) although their developers have long abandoned their active use.[21] Finally, a culture of data maximalism – "when in doubt, collect" – pervades API

design, with the result that API attacks often result in "excessive data exposure"[22] of users. A design culture favoring ease of access has also resulted in the neglect of security evaluations in the development cycle, although there is more awareness among API programmers today than even the recent past.

On account of these factors, threats to API security have risen in severity and sophistication. The Open Web Application Security Project Foundation's (OWASP) annual 'Top 10' rankings of API security threats – considered a benchmark among market players and cybersecurity researchers alike – has consistently identified the following as high-priority concerns:[23]

a Code injection, i.e., pinging the API with malicious code that allow unauthorized actors to retrieve, manipulate, or destroy user data;
b Broken authentication, i.e., the use of APIs for credential stuffing or brute force attacks that permit malicious actors from taking control of user accounts associated with a service or application;
c Man-in-the-Middle attacks that take advantage of poor encryption protocols (at rest or in transit) to retrieve highly sensitive user details;
d Insecure design of APIs that lean on legacy methods to recover user credentials, retrieve data, generate error messages, etc., without adequate threat modeling.

Given the nature and gravity of such threats, the use in particular of APIs that allow third parties to connect and retrieve information from middleware infrastructure presents a major cybersecurity concern for states. In the case of many middle powers, especially large developing countries, the government plays an important role in shaping the digital economy. The state in question may want to share data with market players in a bid to boost private innovation. While APIs present a relatively easy and seamless way for many states to create middleware that collects data or retrieves it from existing databases, they must balance such convenience against the risk of losing highly sensitive information. In some instances, only states have the legal imprimatur to collect certain types or categories of data from citizens, and the possibility of leakage or unauthorized exposure of such data (for example, biometric or health data) to third parties through APIs is high.

The concern that APIs may be vectors for cyber attacks and indeed, cyber conflict, is compounded in the case of AI-enabled services. States may allow the use of APIs specifically to promote AI/ML innovation on public databases or infrastructure in a number of ways. Governments could lay down specifications and protocols for retrieving data either from databases or directly from citizens. Once data is collected through such traditional, "dumb" APIs, it is left to the third party to anonymize the data and use it to train their proprietary ML models. Alternatively, states could provide "clean rooms" or closed environments where personal and population-level data is anonymized and training models built without actual transfer of data. Such a model relies

on advancements in secure multi-party computation that allows for training of algorithms without having to share private data.[24] And finally, states could open up their infrastructure to third party Machine Learning APIs (ML APIs) that are used by start-ups, enterprises, and public agencies alike. Indeed, this third option may emerge as a popular one for many market players who do not themselves have the capacity or resources to train ML models, but have innovative AI-enabled services to offer. The widespread adoption of cloud computing has boosted the popularity of ML-as-a-Service: AI-enabled products and services have increasingly begun to offload data processing and training of algorithms to cloud-based ML services such as Google, AWS, and Azure. Their APIs perform a number of critical functions, providing both 'off-the-shelf' and customizable neural networks to third-party applications. For start-ups that want to train their own algorithms on cloud-based services, ML APIs are invaluable for data labeling, maintaining registries of training models, and for periodic audit of those models.[25]

These methods of using APIs to facilitate third party access and innovation in AI-enabled services are not without risks. The security considerations and threats involving APIs in general have already been documented in this section, and need not be repeated here. Such threats are, however, more pronounced with respect to the use of APIs to train ML models. With greater volumes of data being called by APIs for training purposes, they become lucrative targets for state and non-state adversaries. A major concern with the use of traditional and ML APIs is their handling of data, and the measures taken by states as well as private actors to not only anonymize training data but also minimize risks of subsequent de-anonymization.[26] In many developing countries, judicial and regulatory capacity to address de-anonymization risks breaches may be limited, as a result of which its resolution could be entirely dependent on voluntary, technical steps taken by market players. Without effective safeguards to prevent de-anonymization, APIs could be exploited by adversaries to capture highly sensitive details from training data about the population.

ML APIs have surged in popularity, especially in the aftermath of the COVID-19 pandemic. With businesses and NGOs moving their operations online, the demand for AI-enabled audio/video, text-based, and Natural Language Processing (NLP) services has increased significantly. The health sector has seen perhaps the biggest transformation during this period, as witnessed by the move towards predictive diagnostics and 'health bots' that perform remote consultation. The rapid rise and adoption of ML APIs raise the concern that their software design may sidestep security considerations in favor of scale and ease of access. It is not simply the secure design of ML APIs that matter, but also their use by developers or services who are new to using 'off-the-shelf' tools for training ML models. As Wan et al. note, ML API misuses have already become commonplace, because start-ups or businesses are not fully aware of attributes of ML tools offered by cloud services like

Amazon or Google.[27] Their study of 360 applications that relied on ML APIs found that developers routinely called the wrong API – for e.g., many apps confused "image classification" APIs with "object detection" APIs, the latter being used to identify objects within an image – which affected the accuracy and effectiveness of the service.[28] Additionally, many developers also interpreted the predictive results delivered by ML APIs incorrectly, mistaking probabilistic assessments for binary ('yes' or 'no') results.[29] A poorly understood and utilized ML API ecosystem is ripe for exploitation and disruptive cyber attacks.

As more applications and services rely on ML APIs to retrieve and train data through DPI, states will thus be confronted by the challenge of securing that data against API design flaws, improper use, and exploitation. Training models not only require large datasets, but are also in need of constant updates both to the ML APIs as well as the data itself. As Chen et al. note, the predictive performance of ML APIs can grow "significantly worse over time" even when they rely on the same datasets.[30] Routine updates both to the API (by the cloud-based provider) and the training data are crucial to the model's effective performance. Unfortunately, such a highly dynamic environment also increases the chances for MITM attacks that may be carefully disguised as API updates or requests for new data. Cloud service providers have been criticized in the past for considering security as an "externality," and shifting the loss from cyber attacks on to the users.[31] If they adopt the same approach with respect to ML APIs, especially those that 'call' public infrastructure, states may be constrained to address cyber attacks on their infrastructure and AI-enabled services quickly and effectively. A 2017 review of iOS and Android developer guidelines found many aspects of application-layer security on these platforms to be insufficient or only partly aligned to OWASP standards.[32] With no human supervision of interactions between AI-enabled services and their users, similar vulnerabilities in ML APIs could be exploited to disastrous consequences.

In summary, vulnerabilities associated with traditional and ML APIs could result in the misuse, manipulation, and even denial of AI-enabled essential services that rely on them. Given deficiencies in secure API design, and in many instances, their poorly understood application with respect to core functions, API-driven middleware could be prime targets of strategic adversaries in the event of conflict. Given these concerns, it is worth examining the different approaches of middle powers with respect to the adoption of APIs for AI-enabled services in critical sectors, and the possible security repercussions of those API-led models.

Case studies: Brazil, India, and Singapore

The critical sector of healthcare has been identified by several states, including middle powers, as ripe for technology leapfrogging. Emerging markets

and developing countries with large populations have historically struggled to train medical professionals whether in the field of diagnostics or healthcare services. With a view to address the lack of skilled professionals, governments have turned to digital healthcare services. Furthermore, the COVID-19 pandemic has catalyzed rapid advancements in digital health, including in the development of AI-enabled diagnostics and services. However, digitizing sensitive health data of populations and rendering them accessible to third parties – via API-based middleware – raises the possibility of such information being compromised or corrupted by adversaries.

The following section outlines recent and ongoing efforts by three middle powers – Brazil, Singapore, and India – to make available public health data via APIs for external developers, including of AI-enabled applications in the sector. In particular, it emphasizes those historical and institutional reasons why these states have chosen to pursue three different approaches to using APIs for facilitating third-party access to healthcare databases.

Brazil

Background

Among developing countries and middle powers, Brazil stands out as a pioneer in the 'informatization' of national healthcare services. Brazil's Unified Health System (SUS), a universal healthcare program established in 1988, is among the largest of its kind in the world.[33] Since 1993, Brazil has created several specialized national databases pertaining to vaccinations, cancer screening and treatments, infectious disease surveillance, movement of restricted drugs, patient visits, and social security benefits. However, it has struggled to digitize these databases and make them interoperable across sectors and healthcare providers.[34] Consequently, private players have stepped in to build their own algorithms for data retrieval and linkage from these databases. Given some of these databases have no anonymization features,[35] the involvement of private actors has raised concerns around privacy and cybersecurity. Although an 'e-SUS' platform has been in existence since 2014 to collect primary healthcare data and population-level indicators, the development of this platform has been hampered by a lack of training in data-entry among healthcare workers as well as "bureaucratization of their work process."[36] Another major challenge in digitizing and consolidating such data has been the lack of a unique identity program in Brazil.[37] And finally, the absence until 2020 of an overarching data protection legislation meant there were no general legal or policy measures governing the handling of sensitive health data. As a result of all these factors, Brazil's expansive policy infrastructure on healthcare and social security has historically been challenged by a skeletal digital infrastructure with no "semantic and technological standardization" for data.[38] However, this scenario has changed dramatically in the aftermath of the COVID-19

pandemic, whose precipitation of the demand for digital healthcare services appears to have been seized by both government and private actors.

The role of APIs in the digitization of healthcare

With the onset of the COVID-19 pandemic, Brazil re-oriented the implementation of three key policy instruments – the National Digital Health Strategy, 2020–2028 (NDHS), National Health Data Network (RNDS) (2020), and the National Artificial Intelligence Strategy, 2021 (NAIS) – to mitigate the spread of the coronavirus and manage the treatment of those infected. These policies were in advanced stages of consultations well before the pandemic, but Brazilian regulators were compelled by the coronavirus' rapid spread to digitally unify various elements of the health system in a bid to address COVID-19 surveillance, immunization, adequate availability of hospital facilities, testing records, etc. For example, the RNDS was initially supposed to be rolled out as a pilot project in a single Brazilian province in March 2020, but was repurposed to "receive and share information [across the country] that could help [the government] control" the pandemic.[39] Similarly, the national health strategy emphasized the interoperability of data across healthcare providers to help tackle together the spread of COVID-19.[40] Finally, the national AI strategy declared that health would be one of the first sectors to see the roll out of AI-driven pilot and implementation projects.[41]

The RNDS in particular is slated to play a critical role in the standardization and interoperability of health data in Brazil. The NDHS declares the eventual objective of the RNDS to be the creation of an ecosystem where the "SUS, public and private healthcare organizations, technology companies, research centers, universities and other stakeholders share data […] well as exercise, test and evaluate new models, patterns, technologies and design."[42] In July 2020, Brazil made the submission of SARS-CoV-2 diagnostic tests to the RNDS – whether conducted by public or private laboratories – mandatory.[43] Following this legal measure, the SUS created "accrediting systems and technical documentation" in its 'DATASUS' platform to facilitate such submission and data sharing.[44] The technical documentation in question referred to a set of API standards. At the time of writing, the Brazilian Ministry of Health has expanded the suite of APIs available in DATASUS, and includes those that not only allow for the sharing of test data, but also the sharing of clinical studies results, immunization data, pharmacy inventories, and primary healthcare data into RNDS.[45] The ministry's Coronavirus-SUS app, used for contact tracing, relied on the Google/Apple Exposure Notification (GAEN) API developed jointly by the two companies.[46] Although it remains possible to export data from government websites or health applications directly, the Brazilian government has strongly encouraged the use of these APIs[47] over other channels, creating the basis for a digital health architecture that is heavily reliant on middleware.

AI-enabled services and future plans

The Brazilian ordinance of August 2020 that established the RNDS offers an insight into the role of APIs in promoting AI-driven innovation in the country's health sector. The ordinance attempts to promote "interoperability" in:[48]

a Information models, i.e., "conceptual and contextual human representation" of data;
b Computational models, i.e., data structures as programmed in a computing language; and
c "Semantic" and "syntactic" data models, i.e., human and computational representations respectively of "classifications, taxonomies, and ontologies" and other information models relevant to the sector.

From Brazil's detailed and carefully crafted attempts to introduce standardization and interoperability in electronic health records, it is amply clear the country's regulators do not see APIs simply as a quick fix towards digitizing the sector. Instead, Brazil's recent national strategies on digital health and AI, as well as a slate of pandemic-era policies, appear to signal the creation of an API-centric middleware ecosystem that facilitates the sharing of personal and non-personal data, and in turn, promotes innovation in AI-enabled services. Brazil's National Health Information and Informatics Policy (PNIIS), introduced in July 2021, specifically call for the use of AI to meet the needs of healthcare professionals and researchers.[49] The 'Conecte-SUS' app, which provides users with a longitudinal record of their clinical history that can be shared with healthcare providers and researchers via DATASUS APIs, has already been earmarked by local governments as a DPI to promote AI-enabled innovation.[50] Several multistakeholder pilot projects on predictive COVID-19 diagnostics have already been implemented in Brazil, although it is unclear at the time of writing whether they have relied on APIs or single-site data. In any event, the 'API-fication' of Brazil's digital health sector appears to be a deliberate and ambitious strategy to ensure public and private agencies can rely on large volumes of data to train and develop ML models in primary healthcare and diagnostics.

Singapore

Background

As a middle power with outsize ambitions to shape normative and material outcomes in cyberspace, Singapore has long sought the comprehensive digitization of key sectors of domestic governance. GovTech, a specialized agency established in 2016 to catalyze the digital transformation of Singapore's public sector and user-facing services, makes a credible claim to be "the first of its

kind" in the world.[51] Among its other responsibilities, GovTech is responsible for the country's "Strategic National Projects" which includes user- and business-facing platforms to access government services, the national digital identity program (Singpass), the country's unified payment gateway (PayNow), and CODEX, a technology stack to standardize the development of applications and handling of data across the country's private and public sectors.[52] While Singapore thus pioneered the development of several DPIs, it has moved cautiously with respect to the digitization of its healthcare sector. The fact that Singapore's "worst cyber attack" implicated its national SingHealth system, may have been a contributing factor.[53] The country's digital health policies initially monitored standalone products and services for quality assurance, risk attributes, and adverse event reporting, and it was only in 2020 that the government sought to address questions regarding the integrity and security of health data.[54] As in the case of Brazil, the COVID-19 pandemic catalyzed the creation of legal and technical frameworks on health data in Singapore. The Regulatory Guidelines on Software Medical Devices, issued in April 2020, underline application-layer security concerns similar to those identified by OWASP. The Guidelines call on software developers to ensure, among others:[55]

a Use of proper authentication protocols, both at the device and API levels;
b Development of "layered authorization models" to differentiate privilege levels for users and devices;
c Encryption for data at rest and transit; and
d Deployment of network monitoring and intrusion detection systems.

Notably, the Guidelines also specify regulatory requirements for AI-enabled medical devices and services. AI/ML services that rely on 'static' datasets as well as continuous learning are required to submit descriptions of data attributes, labels, training models, built-in audit processes, and security features, prior to their registration with Singapore's Health Sciences Authority.

The role of APIs in the digitization of healthcare

Singapore has conceptualized its DPI as platforms, and not specific products, believing the latter to be an impediment to at-scale delivery of services.[56] Consequently, APIs have played a prominent role in connecting these middleware platforms to market actors and end-users. Singapore's "platform-as-a-service" model is made possible by the presence of an "engagement layer" of APIs that connect various agencies and institutions within government.[57] Indeed, Singapore's (now) Chief Digital Officer has characterized some of these APIs as "whole-government APIs."[58] They allow, for instance, businesses to obtain licensing or regulatory approvals from multiple bureaucracies through a single application. Similarly, through the integration of the Singpass system across various government platforms, the Singaporean citizen can avail of any public service through her digital ID.

Through the creation in 2017 of a centralized API Exchange (APEX), Singapore brought its 'whole-government' APIs under an umbrella framework. APEX allows government agencies to share data with each other as well as the broader public, allowing, for instance, private services to retrieve user data previously authenticated by the state, or citizens to submit governance proposals that are then channeled to the appropriate entity.[59] Given its extensive interface with government portals and sensitive data, agencies and third parties are required to undergo a training session and test application-layer security protocols before APEX onboarding is complete.[60]

More pertinent to the context at hand, Singapore has also created a portal called 'data.gov.sg' that offers third parties access to public datasets through APIs.[61] Set up in 2011, the portal was criticized in its initial years for being a "data dump" of files in PDF and CSV format that had to be manually downloaded.[62] In recent years, it has undergone a comprehensive transformation, and while data files may still be downloaded, it is through APIs that the outside world engages with 'data.gov.sg.' Most importantly, the portal also makes available APIs that allow for the retrieval of real-time data in such domains as meteorology and transport.

'Data.gov.sg' hosts over 100 datasets pertaining to health.[63] These include data on infectious disease prevalence, incidence of cancer among the population, preventive health screening results, prevalence of so-called 'lifestyle' diseases such as hypertension, diabetes, cholesterol and obesity, hospital facilities and physicians by secondary and tertiary sectors, immunization statistics, and of course, COVID-19-related information. It is worth noting here that many health-related datasets have been made available through APIs following the onset of the coronavirus pandemic, although they have been in existence for years. The rapid onboarding of health data for third party access, combined with Singapore's overall vision and concerted push to promote "open data" governance through APIs suggests the government is heavily leaning on middleware-driven innovation in healthcare services.

AI-enabled services and future plans

In October 2021, Singapore published AI in Healthcare Guidelines (AIHGle) that offer non-binding recommendations to developers and adopters for the "safe implementation" of AI-enabled medical devices.[64] While the Guidelines devote their attention mainly to questions of fairness and explainability of algorithmic decision-making, as well as end-user communication about the working of such AI-enabled devices, security considerations also figure prominently in the document.

The AIHGle identifies both "data risks" and "algorithmic risks" with respect to the security of the AI-enabled service.[65] To mitigate data risks, the Guidelines recommend safeguards against unauthorized access (through APIs or otherwise) to testing, training, and clinical data. The AIHGle also suggests de-identifying personal data where possible, and where "individual

characteristics need to be retained," using techniques such as "data masking, pseudonymization, or data perturbation."[66] To prevent re-identification, developers are encouraged to keep access logs and apply, where possible, techniques such as secure, multi-party computation. The document acknowledges algorithmic risks, i.e., security concerns pertaining to learning and implementation lifecycles, are more accentuated in AI/ML services that rely on "continuous learning" through dynamic and real-time data flows. In such cases, implementers are encouraged to monitor abnormal algorithmic behavior caused by "maliciously introduced data" or manipulations at the end-user level.[67] The AIHGle places much emphasis on human intervention in the implementation process. Implementers of AI-enabled services should have "self-validation" or fail-safe mechanisms that trigger human intervention when baseline performance of the algorithm is affected and even "contingency plans" that "include shutting down the AI device and switching to analogue protocols."[68]

Although the Guidelines are notable for their level of detail and specifications with respect to cybersecurity as well as algorithmic decision-making, it is unclear how its non-binding recommendations will be enforced by the Singaporean government. The AIHGle recommends developers and implementers enter into Service Level Agreements (SLAs) that demarcate their respective responsibilities for the training and implementation lifecycle.[69] Given the Guidelines are only a few months old at the time of writing, it is not clear how they apply to health data retrieved through 'data.gov.sg,' especially in the case of dynamic datasets. Notably, the Singapore government uploaded 40 health datasets onto the portal two weeks after the AIHGle was published, perhaps reflecting its interest in leveraging public data to promote AI/ML innovation.

India

Background

India has the distinction of running the largest biometrics-driven digital identity program in the world, which has been operational since 2009.[70] The digital ID, called Aadhaar, is fashioned as a DPI used to authenticate the identity of Indian citizens seeking to avail of public and private services. Aadhaar may be considered as the first in a suite of DPIs that have since been implemented by the Indian government in sectors such as finance, logistics, and health. While some of these DPIs, such as DigiLocker – a cloud-based repository where an individual may choose to store electronic records pertaining to identity, educational and employment history, etc. – are designed as products, most middleware infrastructure built by the Indian state has taken the form of APIs and protocols. Examples include the Unified Payments Interface (a common railroad for instantaneous money transfers domestically), the Bharat Bill Payment System (an API-driven gateway for utilities payment),

the Goods and Services Tax Network (for collecting GST accrued to both the federal and local governments), etc.[71]

Since 2017, following its publication of a National Health Policy, the Indian government has sought also to incubate a "federated national health information architecture to roll out and link systems across public and private healthcare providers."[72] In 2018, India published a strategy paper on a National Health Stack (NHS), described as a "collection of cloud-based services" that run on open and interoperable APIs.[73] The strategy paper also mooted the creation of a digital health ID, a unique identifier that would allow Indian citizens to not only obtain longitudinal health records from a federated database, but also share it with healthcare providers anywhere in the country. Despite its ambitious goals, however, the NHS has struggled to materialize on account of two reasons. The domain of health is constitutionally the preserve of state governments in India, who have been reluctant to support a national initiative partly on account on lack of clarity on the implications of the technical infrastructure for their services.[74] Additionally, Indian regulators have also found it difficult to persuade large healthcare conglomerates to standardize and thereby render patient health records interoperable. As with Brazil and Singapore, however, the Indian government has attempted to use pandemic-era health surveillance powers to shift the momentum in its favor.

The role of APIs in the digitization of healthcare

To mitigate the spread of the coronavirus, India's National Health Authority (NHA) developed and mandated the use of two platforms for contact-tracing and COVID-19 vaccine management. Called Aarogya Setu ('Health Bridge') and CoWIN[75] respectively, the development and implementation of these applications provided the government with the institutional fillip needed to create a pan-Indian technical architecture for the NHS.[76] The NHA has sought to utilize not only the personnel resources it marshalled to develop these applications, but also the ties built with healthcare providers to coordinate CoWIN registrations and vaccine deliveries, towards the cause of the health stack. The NHS is envisioned as a "building block" comprising the following layers:[77]

a Data layer, which includes health IDs, longitudinal Personal Health Records (PHRs), registries of healthcare professionals and services, as well as other healthcare-related data such as hospital visit summaries, prescriptions, immunization records, etc.;
b A protocol layer, also known as the Unified Health Interface (UHI)[78] that comprises APIs enabling the seamless retrieval and sharing of data among various actors involved in the provision of healthcare services. Specifically, the UHI will comprise three categories of APIS: registry APIs, gateway APIs, and consent/information exchange APIs. Registry APIs facilitate the standardized collection and maintenance of data,

gateway APIs lay down specifications for access to particular healthcare networks, and consent APIs specify rules for "data fiduciaries," which are specialized entities that manage the consent of the user to share data with third parties;

c An application layer, featuring user-facing apps developed by public and private actors.

As the outline above indicates, the UHI is critical to smooth functioning of the NHS. The API-driven layer will not only determine who can access sensitive health data of Indian citizens, but also the granularity of the data so shared with different types of entities.

AI-enabled services and future plans

At the time of writing, the various policies and technical specifications that make up the NHS are in early stages of stakeholder consultations, but the proposed architecture of the NHS makes it clear APIs will invariably play an important role in ensuring access to training data for AI/ML services. Key to the use of health data for training ML algorithms will be the classification and labeling of data, which are part of the standardized PHRs. Additionally, a draft policy on data retention released alongside technical specifications refers to the conditions under which personal data may be anonymized or pseudonymized, as well as circumstances under which anonymized data should be deleted.[79] Nonetheless, the question remains as to the technical architecture that will facilitate the anonymization of data and concurrently, the use of training data in India's health sector. The NHA's blueprint for the health stack leaves this question open and suggests AI-enabled "clinical decision support systems" will be rolled out in Year 4 of its implementation.[80]

APIs, AI insecurities, and middle power diplomacy

The middleware architecture proposed or implemented by Brazil, Singapore, and India to digitize health data and render it available for training AI/ML models reveals the extent to which developing countries are reliant on APIs. Indeed, the three 'models' presented in this chapter are likely to be adopted by others states to jumpstart the development of AI-enabled services not only in health but also other sectors. States that have already made significant strides towards digitizing public datasets may opt, like Singapore, to make such data available via APIs but leave the selection of data and training of ML models to third parties. Those countries that have lagged behind in digitization may develop APIs to facilitate the standardized input of electronic records and the integration, subsequently, of national databases, as Brazil has done. In such cases, the respective entities responsible for digitizing health records may offer secondary APIs to facilitate third-party access. In yet other cases, states may not only standardize the creation of electronic records but

lay down strict policies and technical specifications – as India proposes – to determine how such data is shared with public and private actors alike.

All three approaches present security concerns for AI/ML services that may be exploited by strategic adversaries. Developing countries that make datasets available for third-party use may not have the regulatory capacity of a small, and relatively wealthy country like Singapore to monitor or enforce guidelines like the AIHGle. The use of APIs available on 'data.gov.sg' is governed by Terms of Service under Singapore's Open Data License, which not only restrict the use of such APIs to specific purposes but also prohibit downstream sub-licensing by third parties.[81] The Singapore model places a lot of trust in self-regulation by the market. For most emerging markets, however, a strong cybersecurity or data protection regulator is essential to monitor malicious ICT activity, because an infant private sector may have even lesser resources than the state to mitigate them. Cyber attacks by state or state-sponsored actors could specifically target API vulnerabilities to manipulate or destroy information in public databases, with a view to compromising AI-enabled services that rely on them. Additionally, poor API security on the part of private actors could have serious and adverse consequences for the integrity of the same training model data that is subsequently used by other developers for their respective services. Finally, the challenges of securing AI-enabled services grow in complexity when they rely on real-time APIs that provide 'live' data. At the time of writing, most datasets uploaded onto 'data.gov.sg' are static in nature. But as Singapore (and other countries) develop real-time APIs, regulators will need to find mechanisms that instantaneously identify and remedy serious cyber attacks on dynamic datasets, failing which they may cause lasting and widespread damage on AI-enabled services that rely on the same data. The risks associated with ML APIs and Man-in-the-Middle attacks have already been documented in this chapter, and they apply in particular to the Singapore model.

Brazil's API strategy is aimed at integrating electronic health records across the country, and making them available for governments at the federal, state, and local levels. As a result, AI/ML innovation in Brazil and other countries that follow its path may be more decentralized. Municipalities and local healthcare providers may tie up with research institutions and market actors to pilot AI-enabled services in provinces by granting them access to public data through their own APIs. The challenge inherent in this approach lies in testing and auditing the security of locally developed APIs that grant third-party access to national databases. Local governments may not spend as much time and resources reviewing their APIs for security flaws as a national regulator or agency. The cybersecurity of national infrastructure is only as strong as its weakest link. If security considerations are not adequately baked into the design lifecycle of such local APIs, states will be confronted with the same challenges identified above with respect to AI/ML services.

India's approach to standardizing electronic records and specifying rules for their sharing via APIs may seem tightly controlled, but presents its own set

of problems. Government control of API design and implementation, even in a democracy, can result in the API development process being opaque and unaccountable to outside stakeholders. Admittedly, this is a problem with the API-fication of public databases everywhere. However, India's wielding of executive power to force the adoption of DPI like Aadhaar[82] and Aarogya Setu, and the non-responsiveness of its bureaucracy to serious security incidents[83] raises the concern that a powerful government apparatus may be less receptive and agile to innovation. Additionally, with the state being the ultimate arbiter of key API decisions such as data labeling and the granularity of data sharing, its unaccountability vis-à-vis the research community and market actors can hamper investigations into security breaches of AI-enabled services.

The three countries whose plans for digital healthcare have been reviewed here not only stand out for contrasting API-led approaches to data sharing with third parties. They are also influential middle powers and democracies, whose successes in digitalizing their economies will be closely observed by regional and global actors alike. As they emulate attempts by these countries to open up public databases to third parties, states may, in the process, also replicate poor cybersecurity practices with respect to APIs.

Whatever the model, APIs are likely to emerge as vectors of cyber attacks on AI-enabled middleware services in middle powers. The COVID-19 pandemic has accelerated the digital transformation of their economies and societies, but attendant cyber risks have also risen. If the SingHealth system suffered a cyber attack in 2018, API-driven infrastructure in other middle powers, such as India's biometric ID system[84] and Brazil's Conecte-SUS platform[85] already suffered serious breaches during the pandemic. As governments rush to share data with the market through APIs for AI/ML innovation, they can also open a gateway for malicious actors. Handling as they do large volumes of information, APIs could be used to corrupt strategic information in databases about the demographic make-up of a country. Then there is the possibility of attack on the AI-enabled service itself. The damage caused by cyber attacks on training data and ML models will not only be economic, but political and psychological. Such attacks can erode trust in AI-enabled services among states and societies alike. In sensitive sectors such as health or transportation where real-time data is involved, cyber attacks can have catastrophic consequences, leading to human casualties.

How are middle powers likely to respond in geopolitical terms to this middleware dilemma?

The first possibility is that middle powers, including those states that have been traditionally reluctant to join alliances or plurilateral security arrangements, may seriously evaluate the possibility of collective measures to defend and even respond to cyber attacks on middleware infrastructure. Many middle powers are constrained by resources to build serious offensive and cyber capabilities. As a result, they have "over-invested" in publicly observable

efforts to build institutional cyber capacity (policies, regulatory agencies, etc.) with little deterrent effect to show for the same.[86] Were these states to open their databases and middleware infrastructure to AI-enabled services, whose security policies as well as algorithmic models are not always fully transparent, they would have even less control or oversight over their digital networks. To detect, prevent, and mitigate cyber attacks on critical resources, therefore, states may seek assistance from countries with more advanced capabilities. In particular, middle powers may enter into agreements with other states, including Great Powers, to protect their infrastructure from malicious cyber operations. A good example of collective cyber diplomacy in this regard is the Quad, a group consisting of the United States and three middle powers – Australia, India, and Japan. Motivated primarily by security compulsions in the wake of China's military "assertiveness" in Asia,[87] the Quad has committed to a number of cybersecurity initiatives, including a Quad Cybersecurity Partnership to share threat information about, develop software standards for, and build capacity to address cyber attacks on critical infrastructure.[88] Proposals for middle powers to develop collective diplomatic and military measures to mitigate major cyber threats are not new, and the 'middleware dilemma' identified in this chapter offers another compelling reason for such cooperation.[89] A second possibility is that middle powers could engage in cyber diplomacy to articulate and implement norms on the security of AI-enabled services. These norms, which may be articulated in intergovernmental or multistakeholder venues, may be comparable to guidelines on data and algorithmic risks identified by Singapore's AIHGLe or address AI vulnerabilities highlighted by other prominent regulators such as the European Union's ENISA.[90] States may also incubate or encourage market players to develop industry guidelines on API security, which has been lagging despite their growing importance to digital services, including AI-enabled services.

In summary, the 'middleware dilemma' will nudge middle powers to play a more active role in cybersecurity diplomacy, with a view to ensure the stability of cyberspace and to enhance their own capacities to address sophisticated cyber threats. Needing to sustain the digital transformation of key sectors, middle powers cannot afford to let discussions on AI security be shaped solely by Great Power politics: their proactive diplomacy could well lead to new norms or collective arrangements on the protection both of critical infrastructure as well as AI-enabled services that run on them.

Relevant disclosure and conflict of interest

The author is a volunteer with iSPIRT, a not-for-profit entity based in Bengaluru responsible for developing some API-driven digital public infrastructure for the Indian government. He is not involved in any technical or policy effort related to digital health data in the country, and as such, does not report any conflicts of interest.

Notes

1 Allan Patience, "Imagining middle powers," *Australian Journal of International Affairs* 68, no. 2 (15 March 2014): 214.
2 Eduard Jordaan, "The concept of a middle power in international relations: distinguishing between emerging and traditional middle powers," *Politikon* 30, no. 1 (May 2003): 167.
3 Charalampos Efstathopoulos, "Reinterpreting India's rise through the middle power prism," *Asian Journal of Political Science* 19, no. 1 (April 2011).
4 See generally, Jose Goldemberg, "Technological leapfrogging in the developing world science & technology," *Georgetown Journal of International Affairs* 12, no. 1 (2011).
5 Adam Chapnick, "The middle power," *Canadian Foreign Policy Journal* 7, no. 2 (January 1999): 73.
6 "Artificial intelligence index report 2021" (Stanford University Human-Centered Artificial Intelligence, November 2021), 155.
7 Johnny Kung, "Building an AI world: Report on national and regional AI strategies, second edition" (CIFAR, May 2020), 14.
8 Liv Marte Nordhaug and Kevin O'Neil, "Co-developing digital public infrastructure for an equitable recovery," *The Rockefeller Foundation* (blog), 22 July 2021.
9 Lalla Soundous Elkhaili El Alami, Asuka Nemoto, and Yoshinori Nakata, "Investigation of users' experiences for online access to their electronic health records in Japan," *Global Health & Medicine* 3, no. 1 (28 February 2021).
10 "PayNow Singapore," accessed 8 February 2022. https://abs.org.sg/consumer-banking/pay-now/.
11 "UPI: Unified payments interface – Instant mobile payments, *NPCI*," accessed 8 February 2022. https://www.npci.org.in/what-we-do/upi/product-overview.
12 "About your Aadhaar," *Unique Identification Authority of India, Government of India*, accessed 8 February 2022. https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html.
13 Omidyar Network, "The open-source, identity platform MOSIP hits a new milestone," *Omidyar Network* (blog), 6 July 2020.
14 "ID-card," *e-Estonia*, accessed 8 February 2022. https://e-estonia.com/solutions/e-identity/id-card/.
15 See, "AI at the forefront of efforts to treat coronavirus patients," *GOV.UK*; "Big push for AI proves fruitful and useful," *TechNews Singapore Government*, 1 July 2020; Sarah O'Meara, "China's data-driven dream to overhaul health care," *Nature* 598, no. 7879 (6 October 2021): S1–3.
16 Mark Boyd, "Understanding what it takes to secure your API," *ProgrammableWeb*, 27 September 2017; "State of develops 2021" (Google Cloud, 2021), 24–25.
17 "Akamai: API attacks are exposing security vulnerabilities," *VentureBeat* (blog), 27 October 2021.
18 Tiffany Xingyu Wang and Matt McLarty, "APIs aren't just for tech companies," *Harvard Business Review*, 13 April 2021.
19 See generally, "API data breaches in 2020," *CloudVector* (blog), 23 December 2020.
20 Jason Macy, "API security: Whose job is it anyway?" *Network Security* 2018, no. 9 (1 September 2018): 6–9.
21 Deokyoon Ko, Kyeongwook Ma, Sooyong Park, Suntae Kim, Dongsun Kim, and Yves Le Traon, "API document quality for resolving deprecated APIs," in *2014 21st Asia-Pacific Software Engineering Conference* (2014), 27–30; "How zombie APIs pose a forgotten vulnerability," *Traceable App & API Security*, 28 May 2021.
22 Vickie Li, "API security 101: Excessive data exposure," *ShiftLeft*, 13 July 2021.

23 "OWASP Top 10:2021," accessed 8 February 2022. https://owasp.org/Top10/.
24 See generally, Chuan Zhao, Shengnan Zhao, Minghao Zhao, Zhenxiang Chen, Chong-Zhi Gao, Hongwei Li, and Yu-an Tan, "Secure multi-party computation: Theory, practice and applications," *Information Sciences* 476 (1 February 2019).
25 See generally, "MLOps with azure machine learning" (Microsoft); "Creating a machine learning-powered REST API with Amazon API gateway mapping templates and amazon sagemaker," *Amazon Web Services*, 13 March 2020.
26 Karl Manheim and Lyric Kaplan, "Artificial intelligence: Risks to privacy and democracy," *Yale Journal of Law and Technology* 21 (2019): 127–129.
27 Chengcheng Wan, Shicheng Liu, Henry Hoffmann, Michael Maire, and Shan Lu, "Are machine learning cloud APIs used correctly?" in *2021 IEEE/ACM 43rd International Conference on Software Engineering* (ICSE, 2021), 127.
28 Ibid., 128.
29 Ibid., 129.
30 Lingjiao Chen et al., "Did the model change? Efficiently assessing machine learning API shifts" (29 July 2021): 2.
31 Bruce Schneier and Trey Herr, "Russia's hacking success shows how vulnerable the cloud is," *Foreign Policy* (blog), 24 May 2021.
32 Andrey Krupskiy, Remmelt Blessinga, Jelmer Scholte, and Slinger Jansen, "Mobile software security threats in the software ecosystem, a call to arms," in *Software Business: 8th International Conference, ICSOB 2017* (Springer, 2017).
33 Katherine E. Bliss, "Brazil's Sistema Único Da Saúde (SUS): Caught in the cross fire," *Center for Strategic and International Studies*, 21 June 2017.
34 See generally, M. Sanni Ali, Maria Yury Ichihara, Luciana Cruz Lopes, George C.G. Barbosa, Robespierre Pita, Roberto Perez Carreiro, Djanilson Barbosa dos Santes, et al., "Administrative data linkage in Brazil: Potentials for health technology assessment," *Frontiers in Pharmacology* 10 (23 September 2019).
35 Ibid., 14.
36 Fernando Rocha Lucena Lopes, Karolinne Souza Monteiro, and Silvana Santos, "How data provided by the Brazilian information system of primary care have been used by researchers," *Health Informatics Journal* 26, no. 3 (1 September 2020).
37 Sanni Ali et al., "Administrative data linkage," 2.
38 Giliate Cardoso Coelho Neto, Rosemarie Andreazza, and Arthur Chioro, "Integração Entre Os Sistemas Nacionais de Informação Em Saúde: O Caso Do e-SUS Atenção Básica," *Revista de Saúde Pública* 55 (1 December 2021): 95.
39 "Conecte SUS pilot project: Final report in Alagos" (Brasilia: Ministry of Health, 2021), 3.
40 *Brazilian National Digital Health Strategy (2020–2028)* (Brasilia: Ministry of Health, 2020), 76–93.
41 "The new Brazilian strategy for artificial intelligence," *Offices of Science and Innovation*, accessed 8 February 2022. https://sweden-science-innovation.blog/brasilia/the-new-brazilian-strategy-for-artificial-intelligence/.
42 *Brazilian National Digital Health Strategy (2020–2028)*, 106.
431 *st Brazilian National Digital Health Strategy 2020–2028 Monitoring and Evaluation Report* (Brasilia: Ministry of Health, 2021), 18.
44 Ibid., 26.
45 "Portal de Serviços," accessed 8 February 2022. https://servicos-datasus.saude.gov.br/.
46 "Apple and Google's COVID-19 exposure notification API updated with improvements, Brazil launches app with alerts –9 to 5 Mac," *9to5mac.com*, 31 July 2020.
47 Olhar Digital, "Covid-19: Falha Na Plataforma e-SUS Gera Subnotificação de Casos No País," *Olhar Digital* (blog), 19 June 2020: 19. [translation by Safari].

48 Imprensa Nacional, "PORTARIA No 1.434, DE 28 DE MAIO DE 2020 – DOU – Imprensa Nacional," accessed 8 February 2022. https://www.in.gov.br/web/dou. [translation by Safari].
49 Imprensa Nacional, "PORTARIA GM/MS No 1.768, DE 30 DE JULHO DE 2021 – DOU – Imprensa Nacional," accessed 8 February 2022. https://www.in.gov.br/web/dou. [translation by Safari].
50 "The digitization of public services as a way to add value to the population," *Ideiagov*, accessed 8 February 2022. https://ideiagov.sp.gov.br/a-digitalizacao-dos-servicos-publicos-como-forma-de-agregar-valor-para-a-populacao/.
51 "Government tech for the people," *TechNews Singapore Government*, 23 May 2016.
52 "Our strategic national projects," accessed 8 February 2022. https://www.smartnation.gov.sg//initiatives/strategic-national-projects.
53 Irene Tham, "Personal info of 1.5 m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack," *The Straits Times*, 20 July 2018.
54 "Digital Health," Health sciences authority (Singapore), accessed 8 February 2022. https://www.hsa.gov.sg/medical-devices/digital-health.
55 "*Regulatory Guidelines for Software Medical Devices – A Lifecycle Approach*" (Singapore: Health Sciences Authority, April 2020).
56 "How can Singapore's govtech stay number one?" *GovInsider* (blog), 16 January 16, 2020.
57 Wendell Santos, "How Singapore will run the country using APIs," *ProgrammableWeb*, 24 June 2018.
58 Ibid.
59 "Case study (APEX – Singapore)," in *Embracing Innovation in Government: Global Trends 2018* (OECD, 2018); "Inside Singapore's plans to share data across agencies," *GovInsider* (blog), 19 May 2017.
60 "API exchange (APEX) – A centralised data sharing platform for the public sector," *Singapore Government Developer Portal*.
61 "Data.Gov.Sg," *Data.gov.sg*, accessed 8 February 2022. https://data.gov.sg/.
62 Santos, "How Singapore will run."
63 "Health," *Data.gov.sg*, accessed 8 February 2022. https://data.gov.sg/group/health.
64 *Artificial Intelligence in Healthcare Guidelines (AIHGle)* (Singapore: Ministry of Health, October 2021).
65 Ibid., 5.
66 Ibid., 19.
67 Ibid., 38.
68 Ibid., 35.
69 Ibid., 12.
70 "What to know about aadhaar, India's biometric identity system," *Time*, 28 September 2018.
71 See generally, Vivek Raghavan, Sanjay Jain, and Pramod Varma, "India stack – digital infrastructure as public good," *Communications of the ACM* 62, no. 11 (November 2019).
72 *National Health Policy, 2017* (Government of India, 2017), 25.
73 *National Health Stack: Strategy and Approach* (Government of India, July 2018).
74 Smriti Mudgal Sharma, "National health stack: A job half well-done," *Ideas for India*, 10 September 2018.
75 CoWIN is an online portal, but Indian citizens can also register for vaccines on the portal through Aarogya Setu, the contact-tracing app. Mandatory registration through CoWIN was subsequently rolled back by the Indian government. "For 18+, On-site registration allowed at government vaccine centres," *NDTV.com*, 24 May 2021.

76 See Saurav Basu, "Effective contact tracing for COVID-19 using mobile phones: An ethical analysis of the mandatory use of the Aarogya Setu application in India," *Cambridge Quarterly of Healthcare Ethics* 30, no. 2 (2020).
77 See *Consultation Paper on Proposed Health Data Retention Policy* (National Health Authority, April 2021).
78 See *Consultation Paper on Unified Health Interface* (National Health Authority, March 2021).
79 *Consultation Paper on Proposed Health Data Retention Policy*, 30.
80 *National Digital Health Blueprint* (Government of India, 2017), 51.
81 See, "Singapore open data licence," *Data.gov.sg*, accessed 9 February 2022. https://data.gov.sg/open-data-licence.
82 Vindu Goel, "'Big brother' in India requires fingerprint scans for food, phones and finances," *The New York Times*, 7 April 2018, sec. Technology.
83 Aria Thaker, "In a year of data breaches, India's massive biometric programme finally found legitimacy," *Quartz*, 26 December 2018.
84 "Chinese hackers targeted aadhaar database, times group: Report," *NDTV.com*, 22 September 2021.
85 "Brazil health ministry website hit by hackers, vaccination data targeted," *Reuters*, 11 December 2021, sec. Technology.
86 See, Nadiya Kostyuk, "Deterrence in the cyber realm: Public versus private cyber capacity," *International Studies Quarterly* 65, no. 4 (17 December 2021).
87 "Quad: The China factor at the heart of the summit," *BBC News*, 24 May 2022, sec. India.
88 "*Quad Cybersecurity Partnership: Joint Principles*" (Government of Japan).
89 Lisa Davidson, "Analysing the characteristics of middle power cyber capability," in *European Conference on Cyber Warfare and Security* (Academic Conferences International Limited, 2017); Roland Paris, "*Can Middle Powers Save the Liberal World Order*?" (Chatham House, 2019); Louk Faesen, Tim Sweijs, Alexander Klimburg, and Giulia Tesauro, "The promises and perils of a minimum cyber deterrence posture: Considerations for small and middle powers" (The Hague Centre for Strategic Studies, April 2022); Sangbae Kim, "The inter-network politics of cyber security and middle power diplomacy: A Korean perspective" (East Asia Institute, 2014).
90 "Artificial intelligence cybersecurity challenges" (ENISA, 15 December 2020).

Bibliography

1st Brazilian National Digital Health Strategy 2020–2028 Monitoring and Evaluation Report. Brasilia: Ministry of Health, 2021. https://bvsms.saude.gov.br/bvs/publicacoes/1st_brazilian_national_digital_health_strategy.pdf.

"AI at the forefront of efforts to treat coronavirus patients," *GOV.UK,* 8 February 2022. https://www.gov.uk/government/news/ai-at-the-forefront-of-efforts-to-treat-coronavirus-patients.

"Akamai: API attacks are exposing security vulnerabilities." *VentureBeat* (blog), 27 October 2021. https://venturebeat.com/2021/10/27/akamai-apis-attacks-are-exposing-security-vulnerabilities/.

"API data breaches in 2020." *CloudVector* (blog), 23 December 2020. https://www.cloudvector.com/api-data-breaches-in-2020/.

"API exchange (APEX) – A centralised data sharing platform for the public sector." *Singapore Government Developer Portal,* 8 February 2022. https://www.developer.tech.gov.sg/technologies/data-and-apis/apex.

"Apple and Google's COVID-19 exposure notification API updated with improvements, Brazil launches app with alerts –9 to 5 Mac." *9to5mac.com*, 31 July 2020. https://9to5mac.com/2020/07/31/apple-and-googles-covid-19-exposure-notification-api-updated-with-improvements-brazil-launches-app-with-alerts/.

"Artificial intelligence cybersecurity challenges." *Report/Study ENISA*, 15 December 2020. Accessed 6 June 2022. https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

Artificial Intelligence in Healthcare Guidelines (AIHGle). Singapore: Ministry of Health, October 2021. https://www.moh.gov.sg/docs/librariesprovider5/eguides/1-0-artificial-in-healthcare-guidelines-(aihgle)_publishedoct21.pdf.

"Artificial intelligence index report 2021." *Stanford University Human-Centered Artificial Intelligence*, November 2021. Accessed 8 February 2022. https://aiindex.stanford.edu/wp-content/uploads/2021/11/2021-AI-Index-Report_Master.pdf.

Basu, Saurav. "Effective contact tracing for COVID-19 using mobile phones: An ethical analysis of the mandatory use of the Aarogya Setu application in India." *Cambridge Quarterly of Healthcare Ethics* 30, no. 2 (2020): 1–10. https://doi.org/10.1017/S0963180120000821.

"Big push for AI proves fruitful and useful." *TechNews Singapore Government*, 1 July 2020. https://www.tech.gov.sg/media/technews/big-push-for-ai-proves-fruitful-and-useful.

Bliss, Katherine E. "Brazil's Sistema Único Da Saúde (SUS): Caught in the cross fire." *Center for Strategic and International Studies*, 21 June 2017. Accessed 8 February 2022. https://www.csis.org/blogs/smart-global-health/brazils-sistema-unico-da-saude-sus-caught-cross-fire.

Boyd, Mark. "Understanding what it takes to secure your API." *ProgrammableWeb*, 27 September 2017. https://www.programmableweb.com/news/understanding-what-it-takes-to-secure-your-api/analysis/2017/09/27.

"Brazil health ministry website hit by hackers, vaccination data targeted." *Reuters*, 11 December 2021. https://www.reuters.com/technology/brazils-health-ministry-website-hit-by-hacker-attack-systems-down-2021-12-10/.

Brazilian National Digital Health Strategy (2020–2028). Brasilia: Ministry of Health, 2020.

"Case study (APEX – Singapore)." *Embracing Innovation in Government: Global Trends 2018*, OECD, 2018. https://www.oecd.org/gov/innovative-government/Singapore-case-study-UAE-report-2018.pdf.

Chapnick, Adam. "The middle power." *Canadian Foreign Policy Journal* 7, no. 2 (January 1999).

Chen, Lingjiao et al. "Did the model change? Efficiently assessing machine learning API shifts," arXiv:2107.14203 [stat.ML] (29 July 2021).

"Chinese hackers targeted Aadhaar database, times group: Report." *NDTV.com*, 22 September 2021. Accessed 6 June 2022. https://www.ndtv.com/india-news/chinese-hackers-targeted-aadhaar-database-times-group-report-2549166.

Consultation Paper on Proposed Health Data Retention Policy. New Delhi: National Health Authority, April 2021. https://abdm.gov.in/assets/uploads/consultation_papersDocs/Consultation_Paper_on_Health_Data_Retention_Policy_21.pdf.

Consultation Paper on Unified Health Interface. New Delhi: National Health Authority, March 2021. https://abdm.gov.in/assets/uploads/consultation_papersDocs/UHI_Consultation_Paper.pdf.

Conecte SUS Pilot Project: Final Report in Alagos. Brasilia: Ministry of Health, 2021. https://bvsms.saude.gov.br/bvs/publicacoes/conectesus_pilot_project_final_report.pdf.

"Creating a machine learning-powered REST API with amazon API gateway mapping templates and amazon sagemaker." *Amazon Web Services*, 13 March 2020. https://aws.amazon.com/blogs/machine-learning/creating-a-machine-learning-powered-rest-api-with-amazon-api-gateway-mapping-templates-and-amazon-sagemaker/.

Davidson, Lisa. "Analysing the characteristics of middle power cyber capability." In *European Conference on Cyber Warfare and Security*, 566–572, Reading: Academic Conferences International Limited, 2017. https://www.proquest.com/docview/1966799273/abstract/F35A1A01AE474C6FPQ/1.

Efstathopoulos, Charalampos. "Reinterpreting India's rise through the middle power prism." *Asian Journal of Political Science* 19, no. 1 (April 2011): 74–95. https://doi.org/10.1080/02185377.2011.568246.

El Alami, Lalla Soundous Elkhaili, Asuka Nemoto, and Yoshinori Nakata. "Investigation of users' experiences for online access to their electronic health records in Japan." *Global Health & Medicine* 3, no. 1 (28 February 2021): 37–43.

Faesen, Louk, Tim Sweijs, Alexander Klimburg, and Giulia Tesauro. "The promises and perils of a minimum cyber deterrence posture: Considerations for small and middle powers." *The Hague Centre for Strategic Studies*, April 2022. https://hcss.nl/report/promises-and-perils-of-minimum-cyber-deterrence-posture/.

"For 18+, on-site registration allowed at government vaccine centres." *NDTV.com*, 24 May 2021. Accessed 9 February 2022. https://www.ndtv.com/india-news/coronavirus-those-in-18-44-age-group-allowed-on-site-registration-appointment-on-cowin-for-vaccination-at-government-centres-2448313.

Goel, Vindu. "'Big brother' in India requires fingerprint scans for food, phones and finances." *The New York Times*, 7 April 2018. https://www.nytimes.com/2018/04/07/technology/india-id-aadhaar.html.

Goldemberg, Jose. "Technological leapfrogging in the developing world science & technology." *Georgetown Journal of International Affairs* 12, no. 1 (2011): 135–141.

"Government tech for the people." *TechNews Singapore Government*, 23 May 2016. https://www.tech.gov.sg/media/technews/government-tech-for-the-people.

"How can Singapore's Govtech stay number one?" *GovInsider* (blog), 16 January 2020. https://govinsider.asia/security/how-can-singapores-govtech-stay-number-one-chan-cheow-hoe-government-chief-digital-technology-officer/.

"How zombie APIs pose a forgotten vulnerability." *Traceable App & API Security*, 28 May 2021. https://www.traceable.ai/blog-post/how-zombie-apis-pose-a-forgotten-vulnerability.

"Inside Singapore's plans to share data across agencies." *GovInsider* (blog), 19 May 2017. https://govinsider.asia/innovation/api-exchange-apex-govtech-chan-cheow-hoe/.

Jordaan, Eduard. "The concept of a middle power in international relations: Distinguishing between emerging and traditional middle powers." *Politikon* 30, no. 1 (May 2003).

Kim, Sangbae. "*The Inter-Network Politics of Cyber Security and Middle Power Diplomacy: A Korean Perspective*." Seoul: East Asia Institute, 2014.

Ko, Deokyoon, Kyeongwook Ma, Sooyong Park, Suntae Kim, Dongsun Kim, and Yves Le Traon. "API document quality for resolving deprecated APIs." *21st Asia-Pacific Software Engineering Conference* 2 (2014): 27–30.

Kostyuk, Nadiya. "Deterrence in the cyber realm: Public versus private cyber capacity." *International Studies Quarterly* 65, no. 4 (17 December 2021): 1151–1162.

Krupskiy, Andrey, Remmelt Blessinga, Jelmer Scholte, and Slinger Jansen. "Mobile software security threats in the software ecosystem, a call to arms." in *Software Business: 8th International Conference, ICSOB 2017, Essen, Germany, June 12–13, 2017, Proceedings*, edited by Helena Holmström Olsson, Arto Ojala, and Karl Werder, pp. 161–175, Springer, 2017.

Kung, Johnny. "Building an AI world: Report on national and regional AI strategies." *CIFAR*, May 2020. https://cifar.ca/wp-content/uploads/2020/10/building-an-ai-world-second-edition.pdf.

Li, Vickie. "API security 101: Excessive data exposure." *ShiftLeft*, 13 July 2021. https://blog.shiftleft.io/api-security-101-excessive-data-exposure-a730d351fbae.

Lopes, Fernando Rocha Lucena, Karolinne Souza Monteiro, and Silvana Santos. "How data provided by the Brazilian information system of primary care have been used by researchers." *Health Informatics Journal* 26, no. 3 (1 September 2020): 1617–1630.

Macy, Jason. "API security: Whose job is it anyway?" *Network Security* 2018, no. 9 (1 September 2018): 6–9.

Manheim, Karl, and Lyric Kaplan. "Artificial intelligence: Risks to privacy and democracy." *Yale Journal of Law and Technology* 21 (2019): 127–129.

"MLOps with azure machine learning." *Microsoft,* 23 January 2022. https://azure.microsoft.com/en-us/resources/mlops-with-azureml/.

National Digital Health Blueprint. New Delhi: Ministry of Health and Family Welfare, Government of India, 2017. https://abdm.gov.in/home/ndhb.

National Health Policy, 2017. New Delhi: Ministry of Health and Family Welfare, Government of India, 2017. https://www.nhp.gov.in/nhpfiles/national_health_policy_2017.pdf.

National Health Stack: Strategy and Approach. New Delhi: National Institute for Transforming India (NITI Aayog), Government of India, July 2018. https://abdm.gov.in/publications/NHS_Strategy_and_Approach.

Neto, Giliate Cardoso Coelho, Rosemarie Andreazza, and Arthur Chioro. "Integração Entre Os Sistemas Nacionais de Informação Em Saúde: O Caso Do e-SUS Atenção Básica." *Revista de Saúde Pública* 55 (1 December 2021).

Nordhaug, Liv Marte, and Kevin O'Neil. "Co-developing digital public infrastructure for an equitable recovery." *The Rockefeller Foundation* (blog), 22 July 2021. https://www.rockefellerfoundation.org/blog/co-developing-digital-public-infrastructure-for-an-equitable-recovery/.

Olhar Digital. "Covid-19: Falha Na Plataforma e-SUS Gera Subnotificação de Casos No País." *Olhar Digital* (blog), 19 June 2020. https://olhardigital.com.br/2020/06/19/noticias/covid-19-falha-na-plataforma-e-sus-gera-subnotificacao-de-casos-no-pais/.

O'Meara, Sarah. "China's data-driven dream to overhaul health care." *Nature* 598, no. 7879 (6 October 2021): S1–S3. https://doi.org/10.1038/d41586-021-02694-1.

Omidyar Network. "The open-source, identity platform MOSIP hits a new milestone." *Omidyar Network* (blog), 6 July 2020. https://medium.com/omidyar-network/the-open-source-identity-platform-mosip-hits-a-new-milestone-ff9137610bed.

Paris, Roland. "*Can Middle Powers Save the Liberal World Order*?" Paris: Chatham House, 2019.

Patience, Allan. "Imagining middle powers." *Australian Journal of International Affairs* 68, no. 2 (25 March 2014): 210–224.

"Quad cybersecurity partnership: Joint principles." *Government of Japan,* 6 June 2022. https://www.mofa.go.jp/files/100348060.pdf.

"Quad: The China factor at the heart of the summit." *BBC News*, 24 May 2022. https://www.bbc.com/news/world-asia-india-61547082.

Raghavan, Vivek, Sanjay Jain, and Pramod Varma. "India stack – digital infrastructure as public good." *Communications of the ACM* 62, no. 11 (November 2019): 76–81.

"*Regulatory Guidelines for Software Medical Devices – A Lifecycle Approach*." Singapore: Health Sciences Authority, April 2020. https://www.hsa.gov.sg/docs/default-source/hprg-mdb/gudiance-documents-for-medical-devices/regulatory-guidelines-for-software-medical-devices---a-life-cycle-approach.pdf.

Sanni Ali, M., Maria Yury Ichihara, Luciana Cruz Lopes, George C.G. Barbosa, Robespierre Pita, Roberto Perez Carreiro, Djanilson Barbosa dos Santes et al. "Administrative data linkage in Brazil: Potentials for health technology assessment." *Frontiers in Pharmacology* 10 (23 September 2019): 1–20.

Santos, Wendell. "How Singapore will run the country using APIs." *ProgrammableWeb*, 24 June 2018. https://www.programmableweb.com/news/how-singapore-will-run-country-using-apis/else-where-web-case-study/2018/06/24.

Schneier, Bruce, and Trey Herr. "Russia's hacking success shows how vulnerable the cloud is." *Foreign Policy* (blog), 24 May 2021. https://foreignpolicy.com/2021/05/24/cybersecurity-cyberattack-russia-hackers-cloud-sunburst-microsoft-office-365-data-leak/.

Sharma, Smriti Mudgal. "National health stack: A job half well-done." *Ideas for India*, 10 September 2018. Accessed 9 February 2022. http://www.ideasforindia.in/topics/human-development/national-health-stack-a-job-half-well-done.html.

"State of develops 2021." *Google Cloud*, 2021. https://services.google.com/fh/files/misc/state-of-devops-2021.pdf.

Thaker, Aria. "In a year of data breaches, India's massive biometric programme finally found legitimacy." *Quartz*, 26 December 2018. Accessed 9 February 2022. https://qz.com/india/1501568/in-2018-supreme-court-backed-indias-aadhaar-despite-data-leaks/.

Tham, Irene. "Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack." *The Straits Times*, 20 July 2018. https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most.

Wan, Chengcheng, Shicheng Liu, Henry Hoffmann, Michael Maire, and Shan Lu. "Are machine learning cloud APIs used correctly?" *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*, 2021. https://doi.org/10.1109/ICSE43902.2021.00024.

Wang, Tiffany Xingyu, and Matt McLarty. "APIs aren't just for tech companies." *Harvard Business Review*, 13 April 2021. https://hbr.org/2021/04/apis-arent-just-for-tech-companies.

"What to know about Aadhaar, India's biometric identity system." *Time*, 28 September 2018. Accessed 8 February 2022. https://time.com/5409604/india-aadhaar-supreme-court/.

Zhao, Chuan, Shengnan Zhao, Minghao Zhao, Zhenxiang Chen, Chong-Zhi Gao, Hongwei Li, and Yu-an Tan. "Secure multi-party computation: Theory, practice and applications." *Information Sciences* 476 (1 February 2019): 357–372.