Pushing boundaries

An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions

Jansen, Bernardus; Kadenko, Natalia; Broeders, Dennis; van Eeten, Michel; Borgolte, Kevin; Fiebig, Tobias

DOI
10.1016/j.giq.2023.101862

Publication date
2023

Document Version
Final published version

Published in
Government Information Quarterly

Citation (APA)
Jansen, B., Kadenko, N., Broeders, D., van Eeten, M., Borgolte, K., & Fiebig, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, *40*(4), Article 101862. https://doi.org/10.1016/j.giq.2023.101862

Government Information Quarterly 40 (2023) 101862

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions

Bernardus Jansen [a], Natalia Kadenko [a], Dennis Broeders [b], Michel van Eeten [a,*], Kevin Borgolte [c], Tobias Fiebig [d]

[a] Delft University of Technology, Postbus 5 2600 AA Delft, The Netherlands
[b] Leiden University, Postbus 9500 2300 RA Leiden, The Netherlands
[c] Ruhr University Bochum, Postfach 10 21, 4844721 Bochum, Germany
[d] Max-Planck-Institut für Informatik, Saarland Informatics Campus Building E1, 466123 Saarbrücken, Germany

ARTICLE INFO

Keywords:
Digital autonomy
Digital sovereignty
e-Government
Security
Cybersecurity
Information technology

ABSTRACT

In just a few years, the issue of "digital sovereignty" has emerged as an important security issue for governments across the globe, reflecting a growing unease about the security risks associated with government services that depend on foreign service providers for digital infrastructure and traffic routing. This work investigates to which extent government services and communication with citizens relies on infrastructure outside their own jurisdiction for six countries facing sensitive or sometimes even antagonistic relations with neighbors: India, the Netherlands, Pakistan, Taiwan, Ukraine, and the United Kingdom. By combining various methods (traceroute measurements, passive DNS data and geolocation), we determine where and how domains are hosted, as well as the network paths taken by citizens' traffic to them. We uncover different strategies and degrees of autonomy, as well as difficult tradeoffs between different risks to autonomy, some of which might be larger than the risks associated with the dependency on foreign providers. This includes transnational providers being used by all countries, with geopolitical rivals even being tenants on the same network and traffic between citizens and governments regularly traversing international borders. Furthermore, we compared our empirical findings to stated governmental policies and find that they are not always consistent.

1. Introduction

In recent years the discussion about digital sovereignty has crossed over from authoritarian states to western, liberal states. States like Russia and China have been championing the cause of 'cyber sovereignty' for about two decades, focusing on the concept of information security, meaning government control of international and domestic information flows and regime continuity (Broeders, Adamson, & Creemers, 2019; Creemers, 2020; Kurowska, 2020). The notorious Great Firewall of China and the recent Russian plans for a RuNet are technological translations of these notions of sovereignty, blocking access to unapproved content and mandating domestic routing of information in times of crisis respectively (Stadnik, 2021).

Western countries have traditionally resisted this narrative of cyber sovereignty, favoring the idea of an open and free Internet in terms of the digital economy and the protection of fundamental rights, and denouncing information security as a Trojan horse to introduce content control (Maurer, 2019). However, in recent years western countries have started to adopt the narrative of digital sovereignty and strategic autonomy to address problems of digital foreign interference by state actors and dependence on foreign governments and foreign big tech platforms and infrastructures, thus 'democratising' the language of sovereignty in the global digital domain beyond authoritarian states. These discussions first took off in the wake of the Snowden revelations which highlighted the world's vulnerability to American digital espionage, not in the least through the global dependency on American platforms, services, clouds and infrastructure (Maurer, Skierka, & Morgus, 2015; Pohle, 2020). Many of the proposed counter measures were technological in nature and focused on data localization, restrictions on routing and adding infrastructure such as new sea cables to bypass the United States. More recently, digital sovereignty and strategic autonomy have become a prominent feature of the European and E.U. policy landscape (Christakis, 2020; Moerel & Timmers, 2021; Pohle, 2020). This has to be seen in the context of rising geopolitical and geo-

* Corresponding author.
E-mail address: m.j.g.vaneeten@tudelft.nl (M. van Eeten).

https://doi.org/10.1016/j.giq.2023.101862
Received 4 July 2022; Received in revised form 20 May 2023; Accepted 2 August 2023
Available online 21 August 2023

economic tensions, such as the U.S.-Sino competition and the political tensions with Russia. The concerns are various and include digital espionage (American, Russian and Chinese), the fall out of the competition between China and the U.S., the increase in information operations and digital interference, and dependencies on foreign technology, infrastructures and raw materials. E.U. Commission President Von der Leyen (2019) presented her team as the "the geopolitical Commission (…) that Europe urgently needs" and has underlined sovereignty and strategic autonomy as key elements of E.U. policy making for cyber security and the digital ever since.

The yearning for tech independence is hardly restricted to Europe, however. Any country that faces geopolitical tensions with neighbors, antagonists, or even allies, may worry about its dependencies on services being operated in those countries. These dependencies expose governments to risks in terms of state adversaries gaining access to hosts running government services or intercepting traffic between those services, citizens and business. Technical solutions to decrease dependence on foreign actors and infrastructures – or even to just demarcate national boundaries on the global infrastructure of the Internet – have been debated for a long time. Ranging from proposals to superimpose 'Westphalian borders' onto the Internet (Demchak & Dombrowski, 2013) to arguments against imposing (any) state sovereignty on the Internet, warning against splintering the Internet and the disruption of Internet governance as it currently functions (Mueller, 2017, 2020). One of the often-heard technical arguments against sovereignty on the Internet is that the distributed architecture of the Internet and the logic of BGP routing is not equipped to deal with imposing sovereign concerns. However, recent research has shown that dedicated governments are able to bend routing and data flows into national preferences if they are willing to put political dedication and resources into it. For example, Russia has basically detached the Crimea from Ukrainian routing and has embedded it into Russian networks and routing, making Crimea 'Russian' in terms of digital data flows (Douzet et al., 2020). Whether these kinds of technological interventions make parts of the Internet more sovereign and – more importantly – whether they contribute to a greater independence and decreased vulnerability to outside interventions, is an open question.

Countries are viewing the integration of their digital economy and government systems into the global Internet as a potential risk that is increasingly framed in the language of digital sovereignty and strategic autonomy. The debate about digital sovereignty is wide ranging – we will go into more detail in the next section – and has political, administrative, and technological layers. While the concept of digital sovereignty is a new buzzword in many countries, it relates to geopolitical tensions, which are of all times. Some countries have been developing their infrastructure under geopolitical pressures well before the concept of digital sovereignty and strategic autonomy became prominent, whereas other countries have only recently returned to a geopolitical view of on their infrastructure. If we want to learn how considerations of digital sovereignty and strategic autonomy might be translated into policies and practices for digital government infrastructure, hosting and communications flows, we can study the choices and practices of government digitization in countries that have been living with long standing geopolitical tensions. In this study we focus on the technical choices made at the national level to secure the hosting of government domains and routing that underlies the digital interaction between governments and citizens. Other relevant, comparable studies have focused on the use of HTTPS as a way of securing government domains (Singanamalla et al. (2020); Hsiao et al., 2019) and, more closely related to this study, some that investigated 'Schengen Routing'. These latter studies, many in the wake of the 2013 Snowden leaks, analyzed the concept of routing not crossing the borders of the Schengen area with the goal of regaining and retaining digital sovereignty in the Schengen area (Dönni, Machado, Tsiaras, & Stiller, 2015; Pohlmann, Sparenberg, Siromaschenko, & Kilden, 2014). However, these studies are different from ours in that they investigate whether Schengen routing could be possible, while we conduct measurements of the actual routing of packets.

In this paper we will focus empirically on the technological layer of hosting and routing. This is one element of what might be called digital sovereignty. As it focuses on core service provision of the state to its citizens and the communication between the state and its citizens, it is arguably a vital element. Our first question is to what extent government websites rely on hosting and cloud infrastructure outside their own jurisdiction. The second is to what extent traffic between citizens and governments crosses jurisdictions. The third question is how these technological choices relate to government policy and strategy. The fourth question is what kind of risks these technological choices entail and how these relate to the idea of digital sovereignty. We will first define the risks of government dependency on foreign infrastructure and then conduct an empirical analysis of the location of government websites and the traffic flows between websites and citizens for six countries: India, the Netherlands, Pakistan, Taiwan, Ukraine, and the United Kingdom. Each of these countries has complicated relations with neighboring countries— some complications are of recent origin, such as the U.K.'s departure from the European Union, while others reflect long-standing geopolitical antagonisms. Our study is agnostic to whether the goal of digital sovereignty is indeed worth striving for and whether governments are better off in reducing their dependencies in light of all consequences of such a strategy. Rather, our aim is to bring evidence to this debate and empirically analyze how different countries have chosen different strategies in this space. This aims to provide governments with a better understanding of the options that they have, so that they can make more informed risk trade-offs around the provisioning of their computational infrastructures.

2. Mapping digital sovereignty

Sovereignty is both the cornerstone of the international (legal) order as well as a rather elusive concept. Stephen Krasner (1999) referred to sovereignty as 'organized hypocrisy' to signify that it is often a malleable concept that strong states shape according to their needs. Sovereignty has legal and institutional connotations at both the domestic and the international level. Domestically, Weber (2004) famously defined the (sovereign) state as having the monopoly on the legitimate use of violence. Internationally, the international system of states is built on legal sovereignty and norms on non-intervention in the affairs of another state, sometimes called Westphalian sovereignty. These conceptions revolve around rights and obligations, or the authority that a state has by virtue of being an internationally recognized sovereign state. Krasner (1999, pp. 12–14) also introduces the notion of 'interdependence sovereignty', meaning a 'government's capacity to control cross-border movements of any kind (ideas, goods, people)'. This crucial notion of *control* is juxtaposed with *authority* when it comes to sovereignty: "authority involves a mutually recognized right for an actor to engage in specific kinds of activities (…) control can be achieved simply through the use of brute force with no mutual recognition of authority at all" (Krasner, 1999, p. 10). The debates about digital sovereignty and strategic autonomy seem to resolve mostly around the notion of interdependence sovereignty and control, even though there are some overtones of legal sovereignty as well.

Digital sovereignty – or its many permutations such as cyber sovereignty, technological sovereignty, data sovereignty and digital strategic autonomy – is wide field that is often lacking in precise definitions. We will sketch the wider field and, given the fact that our empirical focus is on national government system and government–citizen interaction, culminate in specific aspects of digital and data sovereignty. Cyber sovereignty is mostly used by Russia and China and is focused on control over the national digital info-sphere (Creemers, 2020; Kurowska, 2020). These countries, preferring the language of information security over cyber security, want (absolute) control over what information enters and circulates in the domestic digital debate. A related debate is that on

'cyber westphalia' and the question whether the international state system can be superimposed on the global Internet. This debate is partially technical in nature, i.e., can this be done, but mostly political in nature, i.e., should it be done, with some in favor (Demchak & Dombrowski, 2013) and some vehemently against (Mueller, 2020). These debates are linked with the territorial dimension of sovereignty and ultimately ask the question if cyberspace can be 'bordered' along the borders of sovereign states. Because most technological translations of that idea would require changes in routing and data traffic, many fear that (attempted) re-bordering would result in Internet fragmentation (Drake, Cerf, & Kleinwaechter, 2016; Mueller, 2017). Most of these notions of sovereignty center around the notion of control of the transfer and storage of data, and some even control of information itself) .

The debate about digital sovereignty in Europe and the E.U. started in the wake of the Snowden revelations, that exposed European vulnerability to cyber espionage, and intensified in recent years (Monsees & Lambach, 2022; Barrinha & Christou, 2022; Broeders, Cristiano, & Kaminska, 2023) . The main ingredients of the current debates are: the need for an autonomous European/E.U. position in relation to the geo-economic and geopolitical competition between the U.S. and China, the need to decrease dependency on big tech corporations and platforms, and the need to decrease European/E.U. dependencies on raw materials and vital elements of the digital supply chain, like semiconductors. These debates take place against a background of rising geopolitical tensions and increasing state cyber operations in cyberspace, ranging from disinformation and (election) interference, via sabotage to sophisticated cyber espionage, such as the SolarWinds hack. In these debates technological sovereignty and digital sovereignty are often on the same level, with technological sovereignty tilted a little more towards the hardware. Strategic autonomy, a term borrowed from the geostrategic/military domain, is often portrayed as a condition for sovereignty.

Data sovereignty is usually seen as a subset of digital sovereignty and has elements of state sovereignty and personal sovereignty. At the state level it is about keeping control over data for both economic reasons – as raw material for the data economy – and for the political reason of keeping control over sensitive and confidential data, such as government data and communications. The political also extends to the personal as data sovereignty sometimes includes notions of privacy and data protection that are protected in the E.U. as fundamental rights through the GDPR. The fact that the E.U. Court of Justice rendered the data exchange arrangement between the E.U. and the U.S. – first the 'E.U.-U.S. Safe Harbour agreement' and second the 'Privacy Shield' – invalid, among others for reasons of inadequate protection of E.U. citizen data against American law enforcement and intelligence agencies, is testimony of the intersection between the political and the personal when it comes to data. These European debates connect to longer standing debates about data nationalism and data localization that are held (far) beyond the European subcontinent (see for example Chander and Lê, 2015; Taylor, 2020).

While the concept of digital sovereignty is hard to pin down and remains rather abstract, one concrete aspect that is widely understood to be a key part of sovereignty is data localization. The geographic and organizational location of IT services and traffic is relevant in terms the threats posed by states or state-sponsored actors. These typically possess more resources than conventional cybercrime operators, as well as legal and extra-legal means to exert pressure on third parties to covertly cooperate. The threat model of interference with government services and communications spans two main classes of risk: (i) risks related to the hosts operating these services and (ii) risks related to the traffic between these hosts and users, most notably citizens. Hosts located in other countries provide those countries with opportunities for access and interference. Most governments have physical and legal means to acquire access to hosts in their own jurisdiction. Many countries have adopted legislation that grants them extra-territorial access to hosts in other countries, if these hosts are operated by a legal entity with ties to a corporation that falls with its jurisdiction. A well-known example is the U.S. Cloud Act (Rojszczak, 2020), but many countries have laws with extra-territorial effects on Internet services (Hildebrandt, 2013; Internet Society, 2018). In addition to geography, the organizational location also matters. When government domains are located with commercial providers that also serves domains for other clients, this introduces additional risk. Adversaries could become tenants on the same infrastructure and leverage side-channel attacks to break client isolation and glean sensitive data (Cojocar et al., 2020; Ristenpart, Tromer, Shacham, & Savage, 2009).

The second class of risk concerns interference with traffic between citizens and the hosts running the government services. The risk of interception of that traffic are being reduced by the widespread adoption by government domains of Transport Layer Security (TLS) (Hsiao et al., 2019). Yet, important risks remain for encrypted web traffic flowing through other jurisdictions. The NSA has warned about ways in which TLS traffic might be decrypted (Schneier, 2019). Additionally, some security protocols and appliances are alleged to have been backdoored allowing access to knowledgeable attackers (Robertson, 2021). More generally, two key risks remain even with encyption: first, encryption does not stop adversaries from collecting potentially revealing metadata; and, second, adversaries can store encrypted traffic to be decrypted later, with quantum computing being a widely acknowledged threat for current encryption methods (Faulconbridge, 2021; Simonite, 2016). Even when traffic does not normally traverse the borders of a state adversary, BGP hijacks can potentially make any traffic path vulnerable to be intercepted. Though BGP hijacks are often attributed to misconfigurations, governments have been implicated in their occurrence (Doffman, 2020; Wolf, 2010). The more countries and organizations are involved in the hosting and routing of government websites, the more government services are subjected to external jurisdictions and adversaries. These threats to sovereignty are why some countries have pursued strong localization strategies (Taylor, 2020) and why intelligence agencies might adopt dedicated networks, like the U.S. Intelink network.

The threat model is not meant imply that the secure solution for government services is to host and route all communications in-country on governmental infrastructure. That conclusion would be wrong. Localization only addresses certain risks and might actually increase others. For example, when having to choose between brittle domestic infrastructure and resilient U.S. cloud providers, the former might be more vulnerable by attacks by geopolitical antagonists from countries outside of the U.S. If those antagonists are deemed to pose a greater threat to sovereignty than U.S. intelligence operations, then locating the government services in U.S. cloud providers might be the preferred option.

The overarching idea of our threat model is that these threats compel governments to carefully assess the risk trade-offs they face when provisioning their infrastructure. These trade-offs can be informed by better understanding the various practices governments have followed for their IT services, when facing threats to their sovereignty, as evidenced in the different strategies of pursued by different countries. This is the topic of our empirical investigation.

We selected six countries where the hosting and communications of public-facing government IT has evolved under different threats to their sovereignty: Taiwan, Ukraine, Pakistan, India, the Netherlands, and the U.K. The first four countries have had to cope with complicated relationships with neighbors for a long time, whereas in the Netherlands and the U.K. the debate about sovereignty is much more recent. The Snowden revelations brought into focus the dependency on the U.S. and the increased offensive cyber operations from countries like China, Iran and Russia have further pushed digital sovereignty further up the agenda. We are interested to measure the geographical and organizational localization of the hosting and communications of public-facing online government services under these varying threats to sovereignty.

3. Data collection

In this section, we present our methodology to identify how and where government domains are hosted and how citizens can reach them. We do this for six countries with historical entanglements with their neighbors, specifically Taiwan and Ukraine as two countries in the shadow of a significantly larger neighbor, the Netherlands, and the United Kingdom as two geographically close countries that saw a change in relations following Brexit, and finally, India and Pakistan as two countries that share a long history of conflict and war.

3.1. Identifying government domains

For India, Pakistan, Ukraine, the United Kingdom and Taiwan, we leverage the hierarchical nature of their respective top-level domains (TLDs). Four countries exclusively allocate government sites under gov.<cc>., where "cc" stands for the top-level country code of the country – e.g., TW for Taiwan. Taiwan additionally uses the privately operated domain gov.taipei for government services in the capital. Pakistan leverages an additional second-level domain for each region. Hence, for each country, we include domains matching this pattern in passive DNS data from DNSDB (Farsight Security, 2023), a dataset commonly used for this purpose in the network measurement research community. To identify government domains in the Netherlands, we can conveniently use an exhaustive list regularly published by the Dutch government, the Websiteregister (Ministerie van Algemene Zaken, 2020).

3.2. Hosting location (country/hoster)

Determining where a domain is hosted has two parameters: Which hoster/network entity hosts the domain, and where the system hosting the website is physically located.

3.2.1. Hoster identification

To determine the hoster for a given domain, we resolved all collected government domains to their IP address(es) through active forward DNS. For each resulting IP address, we determined the Autonomous System (AS) name and number, smallest encompassing subnet and network description through public WHOIS services provided by the organizations responsible for IP address registration (ICANN, 2023). This information identifies the organization responsible for operating the IP addresses, i.e., hosting the domain.

3.2.2. Geolocation

WHOIS information tells us the registered corporate location of an organization, and not the physical location of a specific server. Instead, we use RIPE's IPMap (Du, Candela, Huffaker, Snoeren, & Claffy, 2020) and the Maxmind GeoLite2 Country database—two commonly used resources for this purpose—as our main sources for geolocation information.

To further improve reliability beyond known limitations in these data sources (Poese, Uhlig, Kaafar, Donnet, & Gueye, 2011; Shavitt & Zilberman, 2011), we performed additional spot-checks using manual measurements. As we are most interested in traffic traversing international borders, we focused on eliminating false positives (IP addresses that are deemed to be located outside the country of origin while they are not) instead of eliminating all false negatives (IP addresses deemed to be located within the country of origin while they are not). Where we were unable to confidently establish a location for an IP address, we labeled its location as'Unknown' and did not count it as being located outside the country of origin.

3.2.3. Shared infrastructures

We also identify with what other domains, if any, government domains share their hosting using passive DNS data. Having obtained government domains and their IP addresses as described in Section 3.1, we search for all domains pointing to the same IP addresses as the government domains. We consider all domains obtained through this search that we did not previously identify as government domains to be non-government domains. This allows us to determine the number of government and non-government domains on any IP address.

3.2.4. Path detection

We use traceroute measurements to identify the traffic paths from resident users to their respective government's domains. A traceroute works by sending packets with a limited TTL (Time To Live) to a target, starting with a TTL 1. At each router, the TTL is decreased by one, and if it reaches zero, the router sends a message back to the sender, notifying them of the TTL having been exceeded. Hence, by sending packets with an increasing TTL from 1, we will receive these TTL exceeded from all routers along a path, revealing routers on the path along with their distance.

To be able to conduct traceroutes representative of citizens in the selected countries, we utilize the RIPE Atlas platform (RIPE Network Coordination Centre, 2023c) to perform our measurements from within our target countries. The Atlas platform employs probes hosted by volunteers to perform Internet measurements. These probes are distributed around the world and at the time of writing, over 11,000 probes are connected to the Atlas platform (RIPE Network Coordination Centre, 2023b) though they are not distributed equally: 540 Atlas probes were located in the Netherlands, while only a single probe was connected in Pakistan. We were able to deploy two additional probes for two more end-user ISPs in Pakistan through personal contacts.

To reduce the number of required measurements and to make our measurements most representative for end-user traffic, we selected only probes connected to residential ISPs for India, the Netherlands, the United Kingdom and Ukraine using a dataset developed by Lone, Korczyński, Gañán, and van Eeten (2020) that allows us to identify probes located at end-user ISPs. For Taiwan and Pakistan, we selected all connected probes due to the limited number of available endpoints. The number of probes and targets selected per country can be found in Appendix 1.

4. Hosting locations of government domains

In this section, we present our results on *where* government infrastructure is hosted. See Fig. 1 for an overview of the Top hosting-locations and organizations for each country. We find that for the Netherlands, Ukraine, India and Taiwan, over 90% of all government domains are hosted inside the country. The U.K. government hosts just over 75% of its domains domestically, while Pakistan has a larger number of government domains hosted outside of its borders than within, with the single largest share after Pakistan itself residing in the U.S.

Another pattern that stands out is how government domains are spread over hosting providers. For India and Taiwan this is centralized, with the Taiwanese government hosting over 82% of their domains with a single provider, the government's own GSNET (Government Service Network). The leading Indian provider, National Informatics Center, is also a government-affiliated entity and hosts 65% of Indian government domains. Contrary, the single largest providers for Ukraine and the Netherlands host less than a third or a quarter, respectively, of all domains. Still, these providers host more than three times the number of domains compared to the number two providers. For Pakistan, the difference is a factor of two. Finally, the United Kingdom, shows a distributed pattern: domains are spread out over a large number of providers, with no single provider hosting more than 10% of all government domains. While the UK is the most extreme case in this regard, we find a similar heavy tail of small providers hosting government domains for the Netherlands, Pakistan, Ukraine and the United Kingdom.

In all countries, we find government services hosted with U.S. providers. Notably, for the United Kingdom, 6 the top 10 providers are

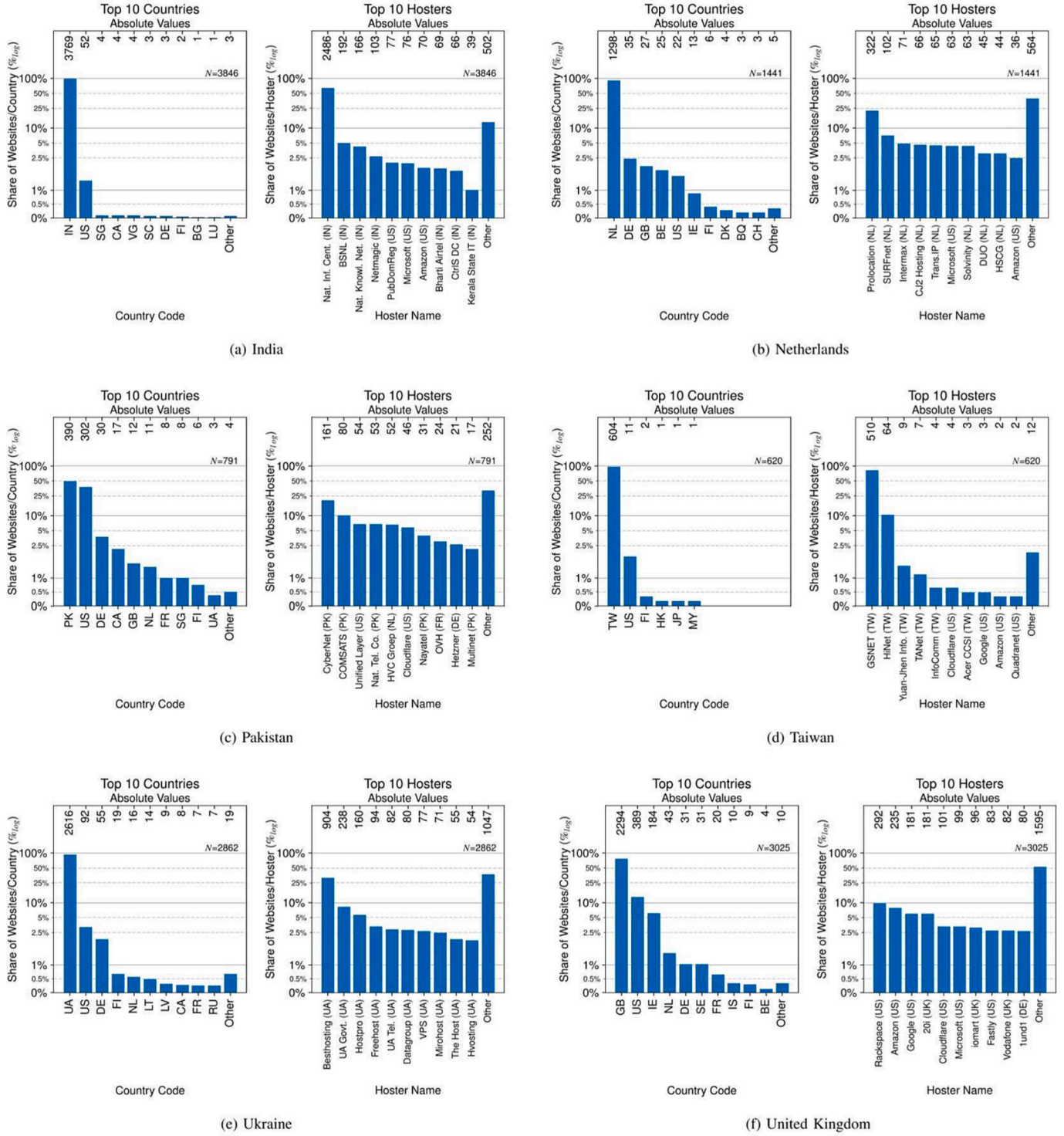

Fig. 1. a-f. Overview of the hosting locations (country/provider) for government systems in India, the Netherlands, Pakistan, Taiwan, Ukraine, and the United Kingdom. The country codes in parentheses denote the location of the provider as registered in WHOIS.

American companies, including the top 3. We find American hosting providers in the top 10 of all countries, except for Ukraine. Even in Ukraine, however, the U.S. still harbors the single largest share of Ukrainian government domains after Ukraine itself.

In light of the conflict with Russia, it is remarkable that we find seven websites of Ukrainian government entities hosted on Russian infrastructure, mostly pertaining to small and regional government bodies. Besides using Russian hosting providers, several of these sites also use yandex.ru. as their email provider. Despite the protracted conflict between Ukraine and Russia, ongoing since 2013, these sites remain operational on Russian infrastructure.

One site that has apparently been taken down in the recent past, however, is simferopol-rada.gov.ua. This site would normally have hosted the website of the Crimean parliament but is currently dysfunctional. While the site has disappeared, the domain's DNS records still point to IP addresses that are announced by CrelCom, a Crimean ISP. Our classification of those addresses as "Russian" is based on the data reflected in the RIPE NCC address database as of now, and we note that

this data has been changed to "Russian" from "Ukrainian" between 2013 and 2014 (Network Coordination, 2023). For the Netherlands, an E.U. member state, national and E.U. guidelines makes it generally undesirable to host government websites outside of the E.U. Not all domains are of an equally sensitive nature, however. For example, nlintheusa.com, the website of the Dutch embassy in the U.S., is hosted in the U.S. A more delicate example is the website bzksocialmedia.nl. This serves as a directory of all social media accounts belonging to the Dutch Ministry of the Interior and Kingdom Relations. It is also hosted in the United States. In an era of fake news, the ability to verify sources is crucial. Authoritative directories like this could be considered part of a nation's digital sovereignty, making external dependencies undesirable.

As a final note, we point out that the total number of government domains differs greatly between the countries (see top right corner of each plot in Fig. 1). These differences, however, do not explain the patterns we discussed above. Taiwan has the lowest number (620), while India has the highest (3846). Yet they are both highly centralized on in-country government providers. Pakistan has the second lowest number (791) and yet shows a highly distributed pattern with around a third of the domains hosted in-country, while the rest is with commercial providers across the globe.

5. Governments on commercial platforms

Next, we visualize the concentration of government domains and co-location with non-government domains. In Fig. 2, we plot the number of non-government domains (x-axis) vs. the number of government domains (y-axis) per IP address (marker), where the size of the marker indicates the total number of domains pointing that IP.

We find several interesting patterns. First, on the right side of the figures, we see one or more large red markers indicating a high concentration of domains (all above 100 K, many above 1 M) on a single IP. Among these domains there are only a handful—up to a dozen only for the U.K.—government domains. On closer investigation, we find these to be examples of government sites being hosted on very large (i.e., in terms of tenants per address) commercial infrastructures. For the Netherlands, the major platform is GitHub, where one government entity uses GitHub's user- pages feature to share information on a

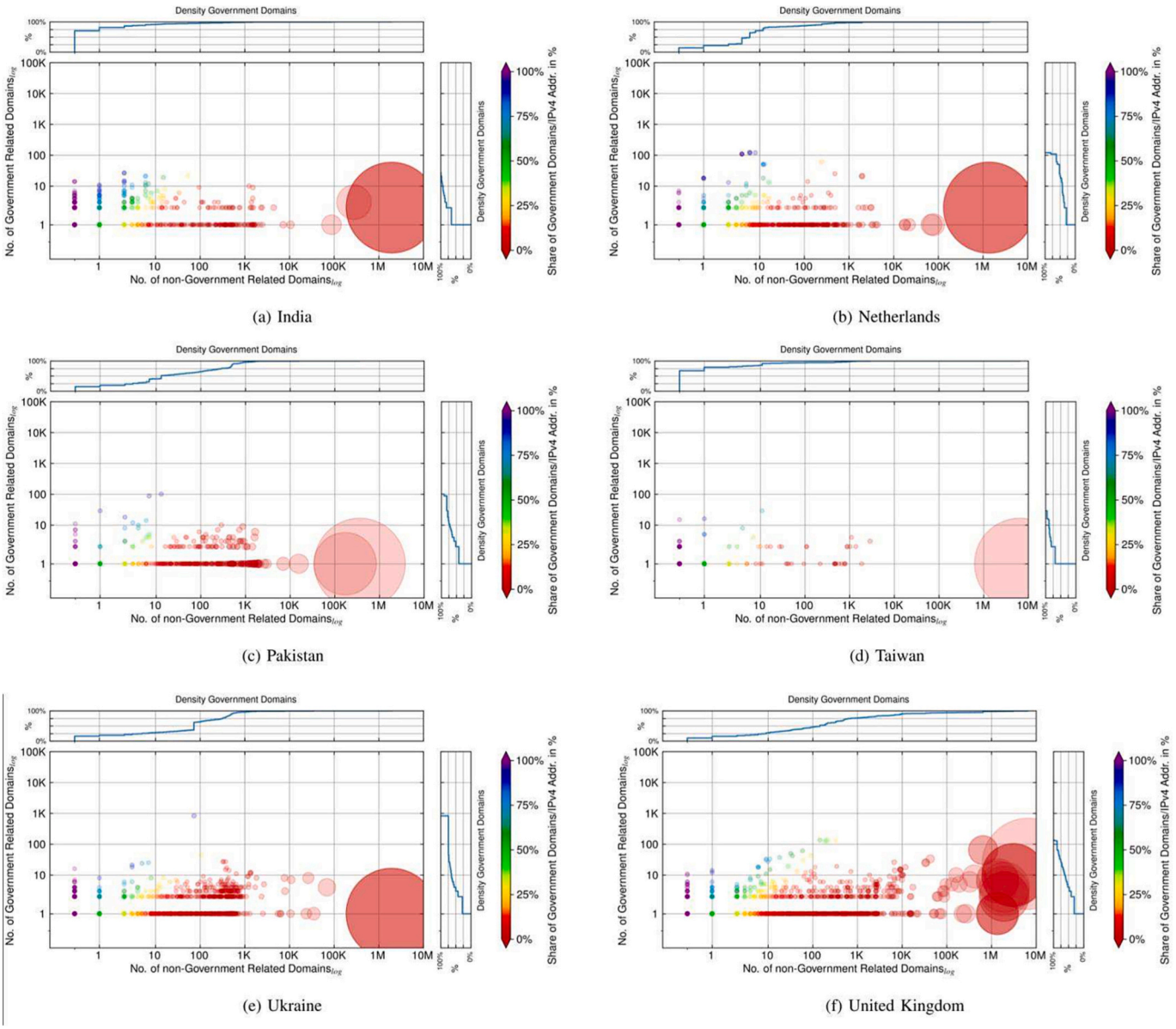

Fig. 2. a-f. Overview of the number of non-government domains on IPv4 addresses with at least one government domain on it. Each dot is an IPv4 address. The size of the markers corresponds to the total number of domains seen on the IP address (log transformed for legibility).

government communication tool developed during the COVID-19 pandemic. In the case of Ukraine, the "outlier" is a single—now defunct—government website for the regional court in Lviv, hosted on Google infrastructure. For Pakistan, we find two government domains, one from a regional government body, one from an economic development project, pointing to a major U.S.-based shared hosting provider: Confluence Networks. In Taiwan, we find a single website from a regional government, which has been hosted with Google. For India, we find an online-learning site of the government hosted on Google infrastructure, and several smaller sites that are hosted on Confluence Networks. However, at the moment, the sites hosted at Confluence Networks appear to be defunct.

Only for the U.K., we find a range of active government websites on large shared infrastructure. This includes several town councils on Google, Amazon, Weebly, and Squarespace, and an open data website hosted on GitHub. The most prominent site being hosted on a major shared hosting platform is the public website of MI5, the U.K.'s security service. It shares an IP address with, among others, the U.K. Institute for Forest and Tree Research, the U.K.'s Gambling Commission, and an Austrian web shop selling sneakers.

The more colorful set of markers on the left side of the graph indicate IPs hosting where the portion of government domains starts to increase from 25% to, all the way on the left, 100%. Where government domains form the majority, these IPs are likely to be government-contracted servers.

The density graph above and to the right of each plot shows the number of domains present on the IP addresses along the x-axis and y-axis. For India and Taiwan the density plot confirms that the bulk of government domains (67.3% for Taiwan, and 70.5% for India) is located on IP addresses with no non-government domains. Similarly, a steep pattern on the density graph along the y-axis for Taiwan and India indicates that for both countries around 2/3rd of government domains (68.0% for Taiwan and 64.3% for India) are not co-located with any other government domains.

In contrast, the more gradual rise of the density graphs for Pakistan, Ukraine, and the U.K.—as well as for a limited extent also for the Netherlands—shows the more diverse set of hosting infrastructures used in these countries. This comprises the whole spectrum of government-operated infrastructure, to government-dominated infrastructure at commercial providers, all the way to fully open commercial shared-hosting platforms. An interesting exception to this pattern can be found in Fig. 2e for Ukraine. We find a single IP address hosting 829 (25.56%) of all gov.ua. domains, which causes a small jump in the density graph. A closer investigation of the service revealed that it is a private entrepreneur (rada.org.ua) offering accessible hosting of websites for "Rada", that is, regional and village councils. Based on information on the website, the service seems to not have been organized or explicitly endorsed by the central government. Furthermore, correlating our measurement data with the Ukrainian public tender repository (Clarity Project. #2753217418, 2021) indicates that the number of councils hosted there is indeed accurate, with some websites not currently active but part of an ongoing or lost tender process.

6. Paths to government systems

To identify *how* end-users reach government websites, see Fig. 3, we divide the results into two main categories: where the target domain is hosted in the country itself and where the target domain is outside the country. The target in-country category is additionally divided into three subcategories: (i) stays in country, for traceroutes that remain fully within the respective country; (ii) leaves country, for traceroutes that cross over an international border at least at one point; and (iii) leaves continent, for traceroutes that at least at one point cross over into another continent.

For the Netherlands and the United Kingdom, this latter category considers the European Union instead of the European continent, since that actually represents a more relevant legal jurisdiction than individual neighboring countries. As the crossing of international borders is implicit for domains hosted outside the country, this category has not been subdivided any further.

Overall, the portion of traffic to government sites that never leaves the country is highly variable—from 21.11% for Pakistan to 80.79% for Taiwan—and heavily influenced by the hosting location of government domains, see Section 4. Even for government domains hosted inside the country, all countries see traffic crossing over international borders. The degree to which this happens differs significantly between countries: from 1.32% for Pakistan to 18.81% for the U.K. We even find that all countries except Ukraine and Taiwan see traceroutes with a domestic

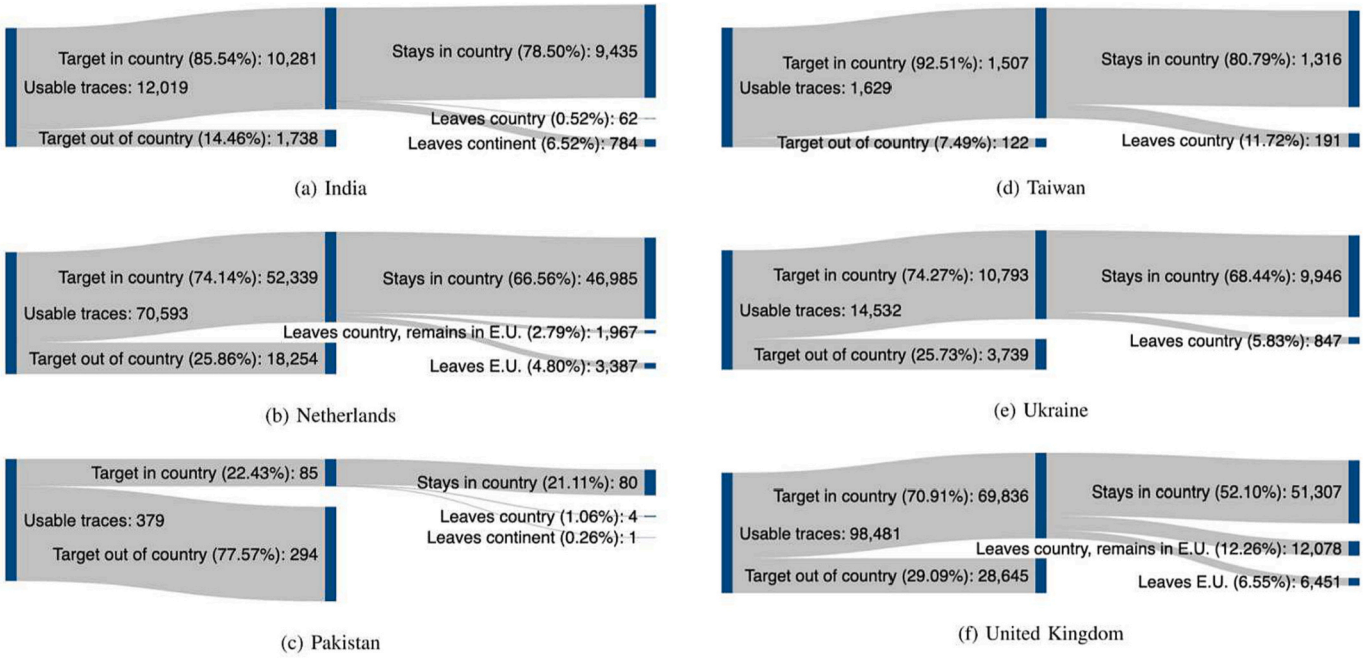

Fig. 3. a-f. Overview of the paths taken to government domains per country.

destination cross continental borders. For the Netherlands and India, traceroutes that cross the border are more likely to also leave the continent/E.U. For the United Kingdom and India, the largest single share of intercontinental traceroutes passes through the United States, though the degree to which this happens differs. Almost 90% of British traceroutes leaving the E.U. pass through the United States, while this is just over 49% for India. For the Netherlands, the United Kingdom is the most significant non-E.U. country with traceroutes passing through its borders at just under 66% of non-E.U. traceroutes. In contrast to the United Kingdom and India, only 21% of its intercontinental traceroutes pass through the U.S. The single Pakistani traceroute passing outside the Asian continent passes only through France before returning to Pakistan.

While we see traceroutes for India and Pakistan passing through the United States and/or Europe, the reverse pattern is not present. Traceroutes for the Netherlands, the United Kingdom and Ukraine at no point cross into Asia.

For the Netherlands and the United Kingdom, we find that the largest share of border- crossing traceroutes that remain within the E.U. pass through geographically close neighbors. The Netherlands sees 38% of traceroutes pass through Germany, while the United Kingdom sees 51% passing through the Netherlands and 38% through Germany. Ukraine, on the other hand, sees its largest share of non-domestic traceroutes pass through the Netherlands (31%), only then followed by neighboring Russia (26%). Again, we see traffic transecting boundaries that delineate antagonistic relationships.

Notably, Taiwan's intra-Asian traceroutes exclusively pass through either neighboring parts of China (98%, all through Hong Kong) and Japan (2%), which—in the former case—may have sensitive geopolitical implications. Given the accelerated breakdown of the 'one country, two systems' model that used to characterize Chinese governance of Hong

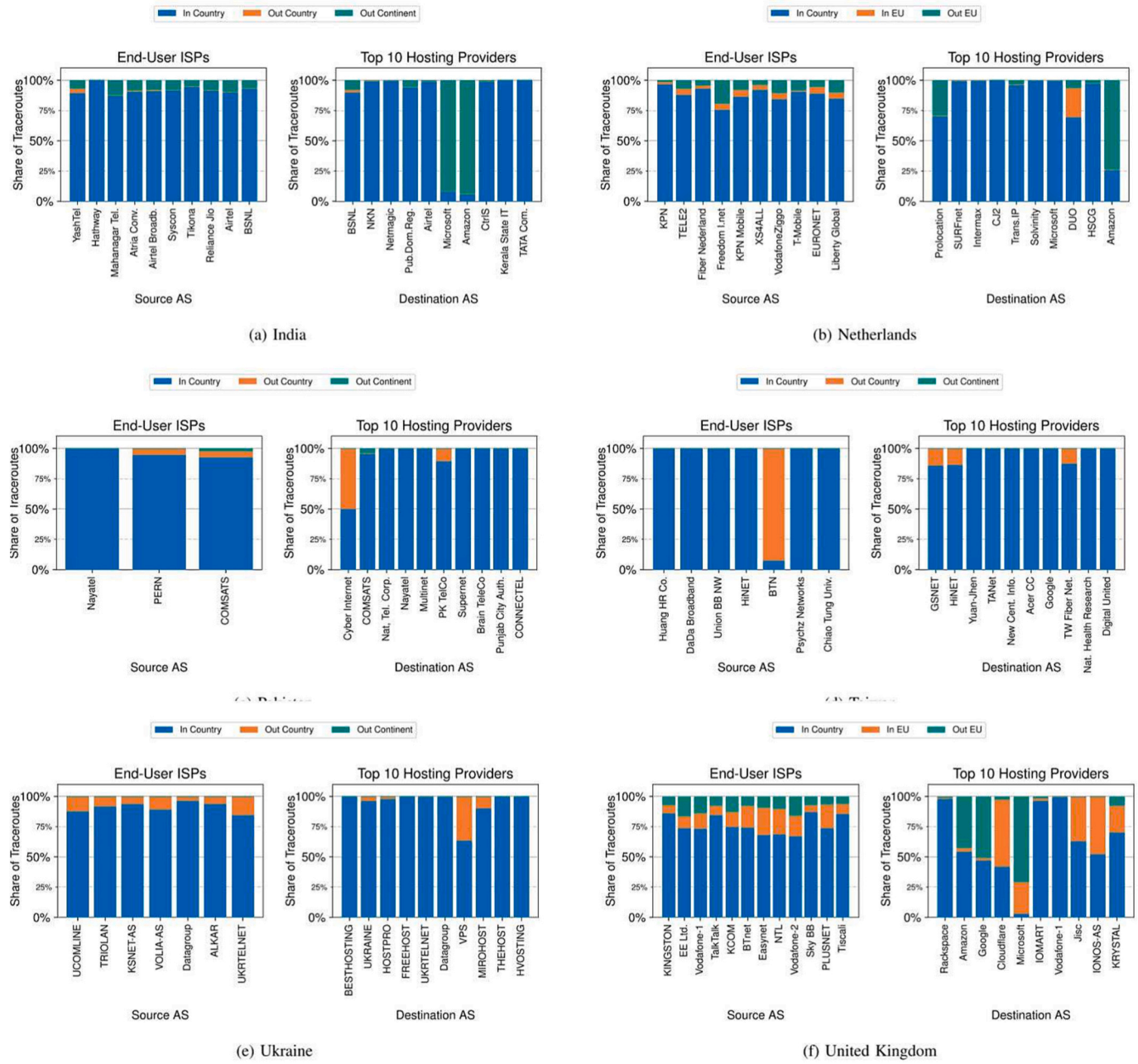

Fig. 4. Overview of the paths taken to government domains that are hosted inside the country itself. (The multiple occurrences of Vodafone (1–3) in Fig. 4f are due to Vodafone using multiple ASNs.)

Kong since our measurements, it would not surprise us if Taiwan routing has now been shifted out of Hong Kong. We note that this routing is due to traffic management of an ISP, which routes domestic traffic to HiNet via parts of its infrastructure located in Hong Kong.

For the Netherlands, see Fig. 4b, traceroutes to the DUO AS—managed by the Dutch government and the largest government-managed AS in terms of hosted Dutch government domains—are routed through Sweden and Denmark for XS4ALL customers. We tie this to the fact that AS 13127 (T-Mobile NL) is the only uplink for AS 22553 (DUO), and KPN (as the AS holder for XS4ALL) does not directly peer with T-Mobile NL. Hence, traffic traverses a Tier 1. This highlights the impact of classical (tiered) Internet topology on where traffic is routed, especially if a hoster only has one or few upstreams.

7. Government practices and strategies

The collected data has revealed that the different governments in our sample have adopted different practices in terms of digital autonomy. One could argue these practices represent *revealed* strategies. How do they compare to the *stated* strategies articulated by these governments? Have governments explicitly pursued these outcomes? For each of the countries, we briefly summarize evidence on the stated strategy and how it compares to the observed practice.

7.1. Ukraine

The official government strategy places big emphasis on Ukraine's digital transformation as a part of political identity-building in Ukraine, with open tenders for all government IT projects fitting within the national anti-corruption policy. Ukraine's digital infrastructure has been considered at high risk of attacks as a part of hybrid warfare. (Ministry of Digital Transformation of Ukraine, 2022). During the 2014 conflict with Russia, Ukraine has suffered a number of high-profile cyber-attacks: BlackEnergy in 2015; the cyber-attack on the Ministry of Finance in 2016, and NotPetya in 2017. After the latter, the Law on the Main Foundations of Cybersecurity was adopted in 2017, marking a major milestone in the national cybersecurity policy (*Zakon Ukrayiny pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny. [Law of Ukraine on the main provisional foundations of cybersecurity of Ukraine],* 2017). However, requirements for government website hosting providers and infrastructure have remained unregulated and get decided ad hoc by government agencies. There are no requirements and no controls regarding hosting infrastructures for the websites of the central government or local government entities, which poses security risks. (Sean Brian Townsend, personal communication, January 31, 2022). Open tenders for all government IT projects, resulting in the number of small providers splitting the market, fit within the national anti-corruption policy. Thus, centralizing a part of Ukrainian government resources on a Russian cloud provider, as we observed in our data, directly contradicts government strategy of establishing autonomy from Russia in the ongoing conflict, while protecting these resources from the future cyber-attacks that are likely to come from Russia. A recent example is a series of cyber-attacks on government websites and services in January 2022, in the lead up to the Russian invasion. These were likely possible through hacking the infrastructure of a "commercial party with administrative access rights to the web resources affected by the attack". (Press Office of the Ministry of Digital Transformation of Ukraine, 2022).

The strategy is consistent with the practices we observed from our measurements. The pursuit of digital autonomy in light of the geopolitical events and cyber-attacks has materialized in the de facto situation of most government websites being hosted within the country by the national commercial providers, with the anti-corruption procurement strategy resulting in the number of (relatively) small providers dividing the market and operating independently. Some attempts to organize the market have been made through providing low-threshold website services for the smaller official institutions. The absence of centralized policies for the government entities ordering website-related services from the commercial providers may have resulted in creating security risks.

After our data collection was completed, in the lead-up to the Russian invasion of Ukraine, the Ukrainian parliament adopted a law that allowed the transfer of government data to the public cloud. After the invasion, this transfer was indeed implemented. We discuss this in Section 8.

7.2. Taiwan

The official strategy of Taiwan included "Strengthening of Government Service Network (GSN) backbone network services" and organizing "The Ubiquitous Network Government Program" to connect infrastructure, integrate central government and local government services" (National Development Council (NDC), 2023b) with emphasis on efficacy and convenience. "Consolidation of internal data centers" is mentioned as a part of "Digital Government". (National Development Council (NDC), 2023a). Furthermore, the National Cyber Security Program of Taiwan (2021 to 2024) (Information and Taskforce, 2021) in the Fifth Phase of Development Plan (2017–2020) included boosting the independence of the cyber security industry as one of the major goals. The "Government websites service management regulation framework" (National Development Council (NDC), 2023c) from the National Development Council contains a set of suggested guidelines for government websites, with emphasis on accessibility, compatibility, and recommending open-source codes (Yachi Chiang, personal communication, February 1, 2022).

The official strategy underlines efficiency, accessibility, compatibility, and independence of cybersecurity industry. There are no explicit requirements for hosting of government websites, the use of cloud providers, or the routing of traffic. One explanation could be that it is sensitive to explicitly refer to sovereignty or autonomy, since that is a highly contested concept within the relationship with China. Yet our measurements showed that hosting is exclusively within the country itself. In terms of routing, a lot of traffic remains domestic, but some dependency on international routing, partially via Hong Kong, is visible. Similarly to Ukraine, we can conclude that observed practices are the product of explicit strategy (such as using market mechanisms to achieve efficiency) and an implicit understanding of the geopolitical situation in which the country operates.

7.3. India

Unlike most of the other countries examined in this paper, Indian government has got a dedicated website titled "Guidelines for Indian Government Websites". The website features a Compliance Matrix with a checklist of mandatory guidelines, which include the criterion of "website is hosted in a data center in India having the following facilities" Guidelines for Indian Government Websites, 2022). The relevant official document from 2009, "Guidelines for Indian government websites", contains a section dedicated to Website Hosting: "Generally, websites/portals/web applications are hosted on special purpose servers in a Data Centre" (Ministry of Communications and Information Technology, Government of India, 2009) complete with an extensive list of security requirements. National Informatics Center, a government-affiliated entity that hosts 65% of their domains, has formulated Guidelines for Indian Government Websites. This strategy corresponds well to our empirical observations of government domains being predominantly hosted on in-country government networks, with the most significant hosting provider being a government entity and with consistent use of dedicated systems that host only government sites.

7.4. Pakistan

The Government of Pakistan issued a 2019 document titled "Critical analysis of various Web Domains of Organizations hosted outside Pakistan" (National Telecom and Information Technology Security Board, Government of Pakistan, 2019). It revealed that an investigation was carried out in 2018, with over 500 departments maintaining their websites outside of Pakistan and data stored on the servers beyond the national borders. This still the pattern that we observed in our measurements in 2020. The strategy seems to be that the government wants to move away from this situation. A call for proposal for the relevant stakeholders was announced "to arrest this tendency", with a preliminary action plan and responsible persons being appointed. Similarly, the "E-mail & Internet policy for the federal government" mentions that "All Government Organizations and their related setups should migrate to the official government portal (www.pakistan.gov.pk), unless there are compelling reasons to continue on their own web site" (Cabinet.gov.pk, 2023, Art. 9b). The official governmental website mentions that "NITB has a dynamic team of developers who competently develop ICT applications as per the need of Ministries and Government Departments." (National Information Technology Board, 2023). While the government strategy seems to be to move away from the pattern of hosting domains on a very diverse set of foreign provider networks, since it is seen as problematic for a number of reasons, at the time of our data collection, there was no reflection of the intended changes being realized.

7.5. United Kingdom

One the goals of U.K. National Cyber Strategy is "Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace." (HM Government, 2022). The U.K. is seeking to become "a leading cyber power" and wants to have control over critical technologies. That being said, a different part of government has published guidance in a "Service Manual " for running "great public services" with non-classified information (GOV.UK, 2021). This guidance includes prioritizing public cloud hosting, choosing one of the options (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) with GOV.UK PaaS available; recommendations for using the Digital Marketplace for finding suppliers that offer "value for money", "avoid long contracts with a single company". Indeed, also in the current Government Digital Strategy, we find the goal to use "commodity hardware or cloud-based software instead of building something that is needlessly government specific". (Fiebig et al., 2023). These guidelines correspond with the observed pattern of relying predominantly on commercial hosters and cloud providers, many of them U.S. based, but with infrastructure points of presence located in the U.K.

7.6. The Netherlands

The "Digital Resilience Strategy" as well as the current "I-Strategy Central Government" (I-strategie Rijk 2021–2025: Digitale weerbaarheid, 2022) mention that Dutch digital autonomy is under threat as a result of influence by foreign state actors. The latter furthermore notes that "the spread [of government services] across providers is inadequate, also because of insufficient Dutch supply". And it observes a "movement toward the cloud", which leads the strategy to ask for the development of a "strategic policy on the use of cloud services". This should address the concerns associated with this movement and include elements like setting up a "government cloud", participating in a European collaboration like Gaia-X, and setting up agreements with the large cloud providers. These strategic directions fit with the practices observed in our data. The pattern shows pragmatism. Dutch ministries are responsible for their own IT provisioning and they all make their own choices, often favoring the convenience of contracting with private providers. This means the government infrastructure is a patchwork of mostly private providers. Thus, the government as a whole has no clear way to enforce policies such as contracting only with Dutch providers or avoiding U.S. cloud operators. In 2011, the Dutch Ministry of the Interior and Kingdom Relations advised against the usage of commercial cloud services by Dutch government ministries, because of their perceived immaturity and insecurity of available cloud offerings (Nationaal Cyber Security Centrum (NCSC) and Ministerie van Justitie en Veiligheid, 2020). Yet, Dutch government domains are distributed across a substantial number of commercial hosting providers, both national and foreign, as well as located in U.S. cloud providers. The transfer of data to U.S. providers is legally supported by the E.U.-U.S. Privacy Shield, which also highlights the complexities that arise when this legal framework is successfully challenged, as it has been in the past.

Overall, the Dutch pattern reflects the fact that sovereignty was not really a concern until recently, as well as the fact that even now, this concern is located in departments concerned with national security policies, while the IT infrastructure is being run by departments that are executing e-government policies and focusing on procurement and provisioning.

8. Discussion

If we follow the E.U. and define digital sovereignty as the ability to assert control over digital infrastructure, data and capabilities, then we can see that some governments push strongly for sovereignty. India's government is hosting 98.0% of its domains in country and Taiwan is a close second with 97.4%. In these countries, we also see a majority of government domains hosted on systems operated by the government itself, rather than commercial providers. Notwithstanding this in-country hosting, we do find a portion of the traffic between citizens and government domains to be routed outside the country – in the case of Taiwan even via Hong Kong, which is under control of China, its geopolitical adversary.

Other countries, like the Netherlands, Ukraine and especially the U.K., locate their IT with commercial providers, including cloud providers, and a portion of which are located outside their own jurisdiction. Traffic, thus, also regularly crosses boundaries. Pakistan has an interesting mix of relying on a government-owned provider inside its borders and on commercial providers in the U.S. and Europe. The latter could be understood as a risk tradeoff: large and mature U.S. providers are likely more resilient than domestic providers against attacks from actors associated with India, and American ownership may even make it a less attractive target for Indian (state) actors. The exposure to access by U.S. and European intelligence agencies is perhaps deemed a lower risk to its sovereignty than those posed by India.

All in all, we observe that there are degrees of freedom in terms of sovereignty. While the Internet is often characterized as intrinsically borderless or at least non-territorial, the government practices we observe do show the influence of geographical boundaries. Some governments have achieved higher degrees of autonomy than other, even though none of them can claim full autonomy. We see that countries with more antagonistic environments have opted for higher degrees of sovereignty in terms of jurisdiction, though some still rely on the private sector rather than government-owned providers. Governments have achieved this without following the autocratic models of China (i.e., the "Great Firewall") and, to a lesser extent, Russia.

An interesting aspect of the different patterns we observed is the procurement process of public infrastructure. For Ukraine, we saw that a streamlined acquisition process offered by a commercial provider to—especially smaller—government entities, leads to prompt adoption. Specifically, we saw the accumulation of gov.ua. domains with one hosting provider who provides an acquisition and tendering process for Ukrainian local councils' websites. It led—without any top-down government intervention or policy—to the adoption of this service. This is consistent with a broader pattern across most countries where the location of government domains follows factors like convenience and

efficiency, such as those associated with commercial cloud and hosting infrastructures. A similar influence of procurement can be seen with the G-Cloud initiative (Chandra & Bhadoria, 2012) in the U.K. The U.K. government adopted a national cloud strategy, which streamlines the acquisition process towards those services, especially for smaller government entities. As a result of this, we see the dominance of U.S. cloud providers in the provision on government infrastructure, different to all other countries in our study. In the Netherlands, we also observed the presence of U.S. cloud providers, even though the government had an official advice in place since 2011 to avoid cloud services because of their perceived insecurity (Nationaal Cyber Security Centrum (NCSC) and Ministerie van Justitie en Veiligheid, 2020).

The observed government practices are often coupled only loosely to official strategies, especially to security strategies. This likely reflects the fact that the strategies around national security are developed by different government departments than those that handle the procurement of IT infrastructure. The latter were more concerned with supporting the digitalization of government services than with national security. Only recently, are we seeing the strategies in these two bureaucratic stovepipes becoming more connected. This is also visible in the recent flurry of E.U. regulation, such as the Digital Services Act, the Digital Markets Act and the A.I. Act, in which increasingly economic concerns and opportunities are coupled with geopolitical and geo-economic concerns (Broeders, Cristiano, & Kaminska, 2023). Sovereignty concerns play an important role in the motivation for these governmental interventions.

In sum, we found a wide range examples of dependencies on foreign providers, from small sites about individual social events for the local population to, most surprisingly, the website of U.K.'s intelligence agency MI5 hosted with an Austrian shared hoster. These diverse patterns have different impacts on digital sovereignty, from marginal to substantial. While it may be true that the Dutch government might not be very concerned with hosting sensitive services in fellow-E.U. member state Germany, or even in the post-Brexit U.K., we note that this exposure does exist and that trade-offs are made, either explicitly or implicitly, when deciding where to host services.

We are not suggesting that these dependencies are intrinsically wrong. They present one type of risk among others. It depends on the overall threat landscape whether that risk is worth taking, in order to avoid other larger risks. A clear illustration that such tradeoff can be seen as strengthening sovereignty was provided recently by Ukraine. In February 2022, just a week before the Russian invasion, the parliament adopted a law to allow the government to transfer its data to the public cloud. In the weeks that followed, the government transferred key governmental data and IT services to Microsoft and Amazon (Microsoft, 2022; Mitchell, 2022). In light of the invasion and long-distance missile attacks by the Russian military, this strategy clearly provided Ukraine more sovereignty, in the sense that it maintained more control over digital resources than when they would have been captured or destroyed. In other words, territorialization does not always increase autonomy. In this case, the opposite could have been true. A similar example is provided by Pakistan, with its heavy reliance on U.S. providers. It reflects the risks of domestic hosting in terms of disruptions in availability and lower resilience against the attacks of actors associated with geopolitical rivals, most notably India.

Governments and other stakeholders have to perform their own risk assessment when deciding where to host services. In what Krasner (1999) calls interdependence sovereignty the issue is *control* on cross-border movement, rather than just the legal practice of the territoriality of data (flows). Also, strategic autonomy in the digital sphere is usually not phrased in a narrow, autarkical way: cooperation is sometimes the best way forward or can simply not be avoided. In the end, the state has to evaluate its options in maintaining its ability to perform its underlying functions independently.

However, in the context of this risk assessment stakeholders should not only consider the direct impact of cloud hosting for specific services. As Fiebig et al. (2023) document for universities, reduced digital sovereignty—even for resources that in themselves may not be critical—might erode the domestic capacity to provide infrastructures for services where it is critical. This effect, which is also discussed more generally by Nemitz (2018) and Christl and Spiekermann (2016), can then have a spill-over effect. The continuous normalization of outsourcing infrastructure tasks for non-essential services, nations might end up losing the option for those services where the impact on digital sovereignty is substantial. Incidentally, we have recently seen signals that this mechanic might be at play in the context of COVID-19 tracing apps, where Australia, among others, hosted essential health infrastructure services in Google and AWS infrastructure (Ahmed et al., 2020).

This resonates with the wider discussion around the centralization of power towards large platforms, e.g., Amazon AWS, Microsoft with their Azure platform, or the popular offerings of Digital Ocean. With more and more services provided by these platforms, dependencies increase between states and these providers (Christl & Spiekermann, 2016; Nemitz, 2018). The question then arises whether foreign nations may put pressure on large platform providers to enforce policies on customers from certain states, or to selectively reveal data under statutes like the CLOUD act (Rojszczak, 2020). In the Western world, this might be less of a major concern due to a perceived traditional trust relationship among the states—though it is unlikely that any domestic security and intelligence agency would find this trust enough assurance for the security of governmental data. Moreover, at the E.U. level dependencies on U.S. digital infrastructure and the role of big tech has become increasingly problematized, as can be seen from recent legislation such as the AI Act, the Digital Services Act and the Digital Markets Acts (DSA/DMA). If we move outside of the those presumed trust relationships, these very issues are brought into sharp focus, as in the example of NATO's concerns about Chinese companies (Huawei) becoming an infrastructural cornerstone in western 5G networks (Rojszczak, 2020). Various countries have adopted policies to restrict the adoption of Huawei's products in critical parts of the 5G network, without naming the company or even China directly. While 5G is out of scope for our study, it does underline the recalibration process that is underway around national dependencies on foreign technology.

In sum, we do not claim that every foreign dependency is an erosion of digital sovereignty – it might actually strengthen it, under certain conditions. Nor do we claim that the appropriate risk strategy is to always rely on domestic solutions. Instead, we argue that policy makers should consider our results and carefully weigh the trade-offs that are, and are not, reasonable given the specific services they are hosting and potential spill-over effects widespread non-domestic hosting may have. Whether digital sovereignty is truly a desirable and feasible objective is still ongoing (Barker, 2020). Regardless of the stance one takes in that discussion, our empirical data sheds light on the extent to which autonomy is realized by various countries for their governmental domains.

9. Conclusion

We analyzed government domains for six countries facing sensitive relations with neighbors or allies: India, the Netherlands, Pakistan, Taiwan, Ukraine, and the United Kingdom. Through traceroute measurements, passive DNS data and geolocation, we determine where and how domains are hosted, as well as the network paths taken by citizens' traffic to them. We found very different strategies across the six countries, reflecting their response to the geopolitical environment. While some governments retain more sovereignty than others, none can claim true autonomy, while some even depend on infrastructure hosted by geopolitical antagonists. We should not equate territoriality with autonomy. There are difficult tradeoffs involved among various risks and dependencies. Under some conditions, such as the threat of an invasion or the lack of a domestic capability to secure digital infrastructure, a government might better safeguard its sovereignty by relying on friendly

and powerful foreign providers.

We hope that by empirically showing the diversity in these patterns, governments have a better understanding of their options when making their own risk-tradeoffs. Our findings suggest that, yes, for many countries more sovereignty is feasible. We are not arguing that more autonomy is always better. The debate on whether striving for more digital sovereignty or autonomy is actually desirable is still ongoing. Some have mockingly characterized it as "autarky" (Barker, 2020). It was not our aim to answer the question of whether this goal is worthwhile. States should decide how they want to manage these risks. The rapid emergence of the issue of digital sovereignty on national and international policy agendas suggest that governments at least think these issues merit closer inspection.

Funding

This work has been supported by the European Commission through the H2020 program in project CyberSec4Europe (Grant No.830929) and by funding from the Ministry of the Interior and Kingdom Relations of the Netherlands, under TU Delft ref. number M75B07.

Declaration of Competing Interest

none

Appendix 1

Table 1
Number of probes, targets and hosting providers per country.

Country	Probes	Targets	Providers
India	40	644	136
The Netherlands	221	435	126
Pakistan	3	224	92
Taiwan	10	238	22
Ukraine	43	608	257
United Kingdom	269	547	219

References

Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., … Jha, S. K. (2020). A survey of COVID-19 contact tracing apps. *IEEE Access, 8*, 134577–134601.

Barker, T. (2020). Europe can't win the tech war it just started: The European Union is running in circles in pursuit of "Digital Sovereignty". Foreign Policy. Retrieved at: https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/. (Accessed 12 May 2020).

Barrinha, A., & Christou, G. (2022). Speaking sovereignty: the EU in the cyber domain. *European Security, 31*(3), 356–376. https://doi.org/10.1080/09662839.2022.2102895

Broeders, D., Adamson, L., & Creemers, R. (2019). *Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace*. The Hague Program for Cyber Norms Policy Brief.

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *JCMS: Journal of Common Market Studies, 61*(5), 1123–1431. https://doi.org/10.1111/jcms.13462.

Cabinet.gov.pk. (2020). E-mail & Internet policy for the federal government. Retrieved from https://cabinet.gov.pk/SiteImage/Policy/internet-and-emails-policy.pdf.

Chander, A., & Lê, U. (2015). Data nationalism. *The Emory Law Journal, 677*.

Chandra, D. G., & Bhadoria, R. S. (2012, November). Cloud computing model for national e-governance plan (NeGP). In *IEEE 2012 Fourth International Conference on Computational Intelligence and Communication Networks* (pp. 520–524).

Christakis, T. (2020). *'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy. Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute*. https://doi.org/10.2139/ssrn.3748098

Christl, W., & Spiekermann, S. (2016). *Networks of control. A report on corporate surveillance, digital tracking, big data & privacy. Facultas*.

Clarity Project. #2753217418. (2021). Retrieved from https://clarity-project.info/tenderer/2753217418. (Accessed 28 June 2021).

Cojocar, L., Kim, J., Patel, M., Tsai, L., Saroiu, S., Wolman, A., & Mutlu, O. (2020, May). Are we susceptible to Rowhammer? An end-to-end methodology for cloud providers. In *2020 IEEE symposium on security and privacy (SP)* (pp. 712–728).

Creemers, R. (2020). China's conception of cyber sovereignty: rhetoric and realization. In D. Broeders, & B. van den Berg (Eds.), *Governing cyberspace: Behaviour, power and diplomacy*. London: Rowman & Littlefield.

Doffman, Z. (2020, April 18). *Russia and China 'hijack' your Internet traffic: Here's what you do. Forbes*. Retrieved from https://www.forbes.com/sites/zakdoffman/2020/04/18/russia-and-china-behind-internet-hijack-risk-heres-how-to-check-youre-now-secure/ (Accessed 11 May 2020).

Dönni, D., Machado, G. S., Tsiaras, C., & Stiller, B. (2015, June). Schengen routing: a compliance analysis. In *IFIP international conference on autonomous infrastructure, management and security* (pp. 100–112). Cham: Springer.

Douzet, F., Pétiniaud, L., Salamatian, L., Limonier, K., Salamatian, K., & Alchus, T. (2020). Measuring the fragmentation of the Internet: The case of the Border Gateway Protocol (BGP) during the Ukrainian crisis. In *2020 12th international conference on cyber conflict (CyCon)* (pp. 157–182). https://doi.org/10.23919/CyCon49761.2020.9131726

Drake, W., Cerf, V., & Kleinwaechter, W. (2016). *Internet fragmentation: An overview*. Geneva: World Economic Forum Future of the Internet Initiative White Paper. Retrieved from https://www.weforum.org/reports/internet-fragmentation-an-overview. (Accessed 28 April 2022).

Du, B., Candela, M., Huffaker, B., Snoeren, A. C., & Claffy, K. C. (2020). RIPE IPmap active geolocation: Mechanism and performance evaluation. *ACM SIGCOMM Computer Communication Review, 50*(2), 3–10. https://doi.org/10.1145/3402413.3402415

Farsight Security. (2023). *Passive DNS historical Internet database: Farsight DNSDB*. Retrieved from https://www.farsightsecurity.com/solutions/dnsdb/ (Accessed 28 June 2021).

Faulconbridge, G. (2021). UK cyber spy chief says: quantum computing is closer but beware the risk. *Reuters*, (April 23, 2021). Retrieved from UK cyber spy chief says: quantum computing is closer but beware the risk | Reuters. Accessed May 20, 2023.

Fiebig, T., Gürses, S., Gañán, C. H., Kotkamp, E., Kuipers, F., Lindorfer, M., … Sari, T. (2023). Heads in the Clouds? Measuring Universities' Migration to Public Clouds: Implications for Privacy & Academic Freedom. *Proceedings on Privacy Enhancing Technologies Symposium (Proc. PETS), 2023*, 2023-2.

GOV.UK. (2021). *Service manual. Deciding how to host your service* (Last update 2021, 25 March). Retrieved from https://www.gov.uk/service-manual/technology/deciding-how-to-host-your-service. (Accessed 28 April 2022).

H.M. Government. (2022, February 7). *Policy paper. National Cyber Strategy. 2022*. Retrieved from https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022. (Accessed 28 April 2022).

Guidelines for Indian Government Websites. (2022). Compliance Matrix. . Retrieved from.https://guidelines.india.gov.in/compliance-matrix/#1585239298471-fd39317c-8b66 Accessed April 28, 2022.

Hildebrandt, M. (2013). Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace. *University of Toronto Law Journal, 63*(2), 196–224.

Hsiao, H. C., Kim, T. H. J., Ku, Y. M., Chang, C. M., Chen, H. F., Chen, Y. J., … Jeng, W. (2019, May). An investigation of cyber autonomy on government websites. In *Proceedings of the world wide web conference* (pp. 2814–2821).

ICANN. (2023). Registration Data Access Protocol (RDAP). https://www.icann.org/rdap. (Accessed 28 June 2021).

Information, N., & Taskforce, C. S. (2021, June 8). National Cyber Security Program of Taiwan (2021 to 2024). Retrieved from https://nicst.ey.gov.tw/en/FD815304EBFFE6FC/639d32e8-2a07-40da-b033-bc6c95d015ce. (Accessed 28 April 2022).

Internet Society. (2018, September). The Internet and extra-territorial application of laws. Retrieved from https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws.pdf Accessed April 28, 2022.

I-strategie Rijk 2021—2025: Digitale weerbaarheid. (2022). Digitale Overheid. Retrieved from https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/i-strategie-rijk-2021-2025/digitale-weerbaarheid/. (Accessed 28 April 2022).

Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy*. Princeton: Princeton University Press.

Kurowska, X. (2020). What does Russia want in cyber diplomacy? A primer. In D. Broeders, & B. van den Berg (Eds.), *Governing cyberspace: behaviour, power and diplomacy*. London: Rowman & Littlefield.

Lone, Q., Korczyński, M., Gañán, C., & van Eeten, M. (2020). SAVing the Internet: Explaining the adoption of source address validation by Internet service providers. In *Proceedings of the 19th workshop on the economics of information security (WEIS)*.

Maurer, T. (2019). A dose of realism: The contestation and politics of cyber norms. *Hague Journal on the Rule of Law, 12*, 283–305.

Maurer, T., Skierka, I., & Morgus, R. (2015). Technological sovereignty: missing the point?. In *IEEE 2015 7th international conference on Cyber conflict: Architectures in cyberspace (CyCon)* (pp. 53–68). Retrieved from http://ieeexplore.ieee.org/abstract/document/7158468/.

Microsoft. (2022). Defending Ukraine: Early Lessons from the Cyber War. Retrieved from https://aka.ms/June22SpecialReport Accessed June 27, 2022.

Ministerie van Algemene Zaken. (2020). *Websiteregister Rijksoverheid* [State Website Registry]. Retrieved from https://www.communicatierijk.nl/vakkennis/rijkswebsites/verplichte-richtlijnen/websiteregister-rijksoverheid Accessed September 24, 2020.

Ministry of Communications and Information Technology, Government of India. (2009, January). Guidelines for Indian Government Websites. Retrieved from http://egovstandards.gov.in/sites/default/files/GOI%20Web%20Guidelines.pdf Accessed April 28, 2022.

Ministry of Digital Transformation of Ukraine. (2022, January 21). Ukraine must prevent discrediting all the achievements of digital transformation – outcomes of the NCCC meeting. Retrieved from https://www.kmu.gov.ua/en/news/ukrayina-maye-zapobigti-diskreditaciyi-usih-nadban-cifrovoyi-transformaciyi-rezultati-zasidannya-nkck. (Accessed 28 April 2022).

Mitchell, R. (2022 December 15). How Amazon put Ukraine's 'government in a box' — and saved its economy from Russia. *Los Angeles Times*. Retrieved from How Amazon is helping Ukraine in its war against Russia by putting its "government in a box" - Los Angeles Times (latimes.com). Accessed May 20, 2023.

Moerel, L., & Timmers, P. (2021). Reflections on Digital Sovereignty. In *EU Cyber Direct*. Retrieved from https://eucyberdirect.eu/wp-content/uploads/2021/01/rif_timmersmoerel-final-for-publication.pdf. (Accessed 28 April 2020).

Monsees, L., & Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security, 31*(3), 377–394. https://doi.org/10.1080/09662839.2022.2101883

Mueller, M. (2017). *Will the Internet fragment? Sovereignty, globalization and cyberspace*. John Wiley & Sons.

Mueller, M. L. (2020). Against Sovereignty in Cyberspace. *International Studies Review, 22*(4), 779–801.

Nationaal Cyber Security Centrum (NCSC), & Ministerie van Justitie en Veiligheid. (2020, June 11). *(Publieke) clouddienstverlening; Enkele ervaringen uit onze cloud journey* [Public cloud service providing; some experieces from our cloud journey]. Retrieved from https://www.ncsc.nl/binaries/ncsc/documenten/rapporten/juni/ervaringsdocument/20/cloudervaringsdocument/Cloudervaringsdocument+NCSC.pdf Accessed November 12, 2020.

National Development Council (NDC). (2023a). Digital Government. Retrieved from https://www.ndc.gov.tw/en/Content_List.aspx?n=EAF760724C4E24A5 Accessed April 28, 2022.

National Development Council (NDC). (2023b). The evolution of e-government development in Taiwan 1998–2016. Retrieved from https://www.ndc.gov.tw/en/News_Content.aspx?n=8C362E80B990A55C&sms=1DB6C6A8871CA043&s=6C189EEA98A3CA17.

National Development Council (NDC). (2023c). Zhèngfǔ wǎngzhàn fúwù guǎnlǐ guīfàn [Government Website Service Management Specification]. Retrieved from https://www.webguide.nat.gov.tw/cp.aspx?n=554&s=460 Accessed April 28, 2022.

National Information Technology Board. (2023). Web hosting, software application & development. Retrieved from https://nitb.gov.pk/Detail/YzE1ODI0OTAtMjJmNS00NDVjLTg2YjctYTE1Y2U4Y2NkODdl. (Accessed 28 April 2022).

National Telecom and Information Technology Security Board, Government of Pakistan. (2019, December 17). Critical Analysis of Various Web Domains of Organizations hosted outside Pakistan. Retrieved from https://www.sindh.gov.pk/files/Master/Critical-Analysis.pdf. (Accessed 28 April 2022).

Nemitz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. In , *376. Philosophical transactions of the Royal Society A: mathematical, physical and engineering sciences* (p. 2133).

Poese, I., Uhlig, S., Kaafar, M. A., Donnet, B., & Gueye, B. (2011). IP geolocation databases: Unreliable? *ACM SIGCOMM Computer Communication Review, 41*(2), 53–56. https://doi.org/10.1145/1971162.1971171

Pohle, J. (2020). *Digital sovereignty. A new key concept of digital policy in Germany and Europe*. Berlin: Konrad-Adenauer-Stiftung. Retrieved from https://www.kas.de/en/web/guest/single-title/-/content/digitale-souveraenitaet Accessed April 28, 2022.

Pohlmann, N., Sparenberg, M., Siromaschenko, I., & Kilden, K. (2014). Secure communication and digital sovereignty in Europe. In *Proceedings of the 16th information security solutions Europe conference, October 2014*.

RIPE Network Coordination Centre. (2023b). RIPE Atlas. Retrieved from https://www.ripe.net/analyse/internet-measurements/atlas. (Accessed 31 August 2020).

RIPE Network Coordination Centre. (2023c). What is RIPE Atlas?. Retrieved from https://atlas.ripe.net/about/ Accessed September 9, 2020.

RIPE Network Coordination Centre. RIPEstat (2023). Historical WHOIS. Retrieved from. "https://stat.ripe.net/widget/historical-whois?pk_vid=fac55c350f3d8fa31607272904a2e27b#w.resource=80.245.112.0/20&w.time=2013–04-04T05:57:03" (Accessed June 28, 2021).

Demchak, C., & Dombrowski, P. (2013). Cyber Westphalia: asserting state prerogatives in cyberspace. *Georgetown University Press. Georgetown Journal of International Affairs (2013-14)Special Issue: International Engagement on Cyber III: State Building on a New Frontier* (pp. 29–38).

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009, November). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 199–212).

Robertson, J. (2021, September 2). Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role. *Bloomberg.com*. Retrieved from https://www.bloomberg.com/news/features/2021-09-02/juniper-mystery-attacks-traced-to-pentagon-role-and-chinese-hackers. (Accessed 9 October 2021).

Rojszczak, M. (2020). CLOUD act agreements from an EU perspective. *Computer Law and Security Review, 38*, Article 105442. https://doi.org/10.1016/j.clsr.2020.105442

Schneier, B. (2019, November 22). The NSA Warns of TLS Inspection. Schneier on Security. Retrieved from https://www.schneier.com/blog/archives/2019/11/the_nsa_warns_o.html. (Accessed 18 November 2020).

Shavitt, Y., & Zilberman, N. (2011). A geolocation databases study. *IEEE Journal on Selected Areas in Communications, 29*(10), 2044–2056. https://doi.org/10.1109/JSAC.2011.111214

Simonite, T. (2016). NSA Says It "Must Act Now" Against the Quantum Computing Threat. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/2016/02/03/162433/nsa-says-it-must-act-now-against-the-quantum-computing-threat/ Accessed May 20, 2023.

Singanamalla, S., Jang, E. H. B., Anderson, R., Kohno, T., & Heimerl, K. (2020, October). Accept the risk and continue: Measuring the long tail of government https adoption. In *Proceedings of the ACM Internet Measurement Conference* (pp. 577–597).

Stadnik, I. (2021). Control by infrastructure: Political ambitions meet technical implementations in RuNet. *First Monday, 26*(5). https://doi.org/10.5210/fm.v26i5.11693

Taylor, R. D. (2020). "Data localization": The Internet in the balance. *Telecommunications Policy, 44*(8), Article 102003. https://doi.org/10.1016/j.telpol.2020.102003

Von der Leyen, U. (2019, November 27). *Speech in the European Parliament Plenary Session. 2019*. Retrieved from https://ec.europa.eu/info/sites/default/files/president-elect-speech-original_1.pdf. (Accessed 28 April 2022).

Weber, M. (2004). *The vocation lectures. "Science as a vocation" and "Politics as a vocation"*. Indianapolis: Hackett Publishing Company.

Wolf, J. (2010 November 19). *Pentagon says "aware" of China Internet rerouting*. Reuters. Retrieved from https://www.reuters.com/article/us-cyber-china-pentagon-idUSTRE6AI4HJ20101119. (Accessed 13 September 2021).

Zakon Ukrayiny pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny. [Law of Ukraine on the main provisional foundations of cybersecurity of Ukraine]. Vidomosti Verkhovnoyi Rady, №45, Art. 403). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text, (2017) Accessed April 28, 2022.