MITRE | Center for Strategic Competition

FIVE THINGS TO CONSIDER WHEN ASSESSING THE IMPACT OF PRC DIGITAL INFRASTRUCTURE

Nancy Ross, Kathy Szot, and Maggie Vencill

UPDATED MARCH 2024

Table of Contents

Assessing the myriad factors constituting the increasingly automated, hyperconnected, smart environments deployed globally is challenging. Yet analyzing these factors of the Digital Silk Road initiatives can help inform and guide actions to counter the People's Republic of China's strategy for global digital dominance.

This paper provides updates to MITRE's November 2021 paper "Five Things to Consider When Assessing the Impact of PRC Digital Infrastructure." While the content of the original paper is still sound, recent geo-political and technological changes affecting the Tech Stack and data protection warrant an update.

The ICT Technical Stack

Using a "Tech Stack" approach to frame and organize dynamic and diverse information, communication, and technology (ICT) factors can help analyze and identify potential areas of risk and opportunity. This approach integrates aspects of systems engineering, intelligence collection and analysis, and socio-technical context. The goal is to generate actionable risk analysis to help identify, prioritize, and guide the development of courses of action (COAs) for use by concerned U.S. government entities, allies, and partners.

This paper highlights five considerations related to studying the Tech Stack and explores examples in which the Tech Stack approach was used to assess

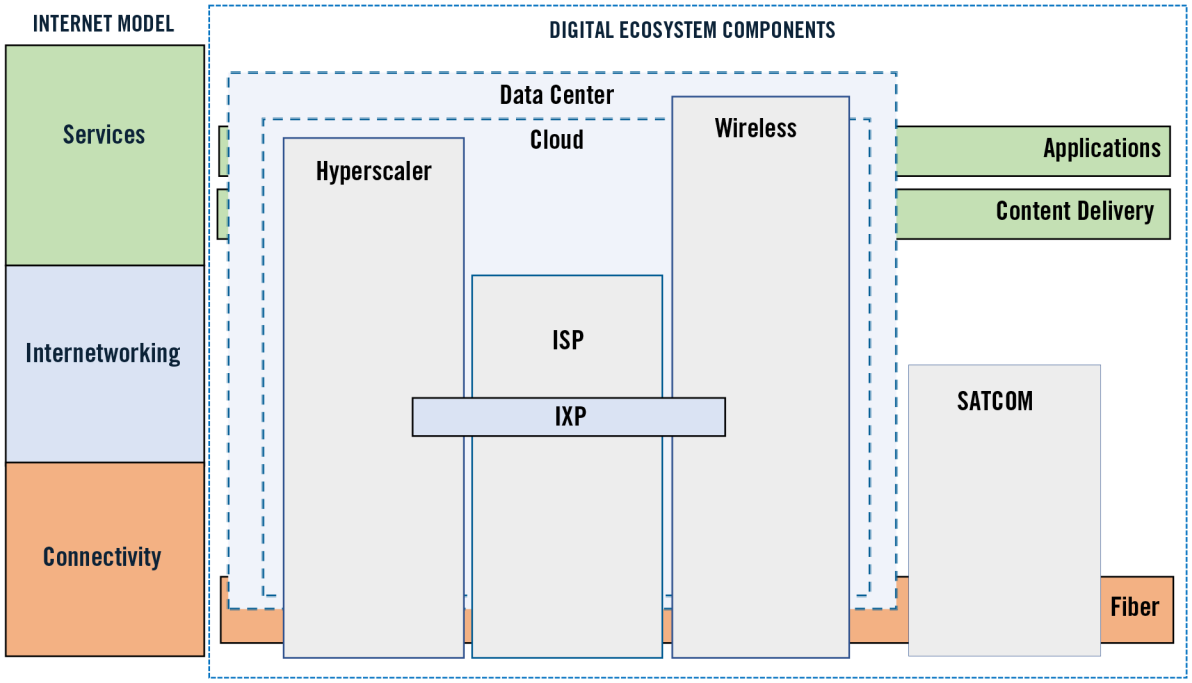

FIGURE 1. SAMPLE ICT ENVIRONMENT

the People's Republic of China's (PRC's) digital infrastructure in Africa.

The basic Tech Stack can be organized around common components found in many ICT environments, aligned generally with the traditional layers of the internet model (e.g., connectivity, internetworking, services). Components may include facilities (e.g., data center, Satellite Communications) and service-related elements (e.g., cloud, wireless, Internet Service Provider) found within an end-to-end ICT environment (see Figure 1). In addition, including end user devices and platforms will contribute to a more holistic understanding of the Tech Stack.

Consideration 1: Start with Systems Thinking

View the environment under study as a system. The system can be decomposed into constituent parts, starting with identification of the relevant digital ecosystem elements.

Analyzing the Tech Stack from a systems engineering perspective encourages the examination of both the technology and the people and processes involved in the system of interest. Actors providing value in the ecosystem may be aligned not only with the ecosystem components and internet layer functionality, but also with overarching systems aspects, such as operations, administration, management, and provisioning as well as relevant ICT-based services and applications. Developing socio-technical context for this data is valuable and can be guided by established best practices in analytic tradecraft and all-source analysis (i.e., capturing details on sourcing, identifying areas of uncertainty, exploring and presenting alternatives). Socio-technical context will provide useful, relevant information beyond what is generally known.

TECH STACKS FACILITATE THE CREATION OF A STRUCTURED VIEW OF THE ICT EMBODIED BY THE PRODUCTS, SERVICES, AND CAPABILITIES THAT COMPOSE CHINA'S DIGITAL SILK ROAD

The following list summarizes relevant points about key Tech Stack components:

1. **Data Centers:** Data centers, as facilities that typically house ICT equipment enabling connectivity, internetworking and services, and data storage, need to be resilient and scalable. They will increasingly be software defined. Sustainable and economical energy and cooling solutions are critical, as is overall operational efficiency. Because different data center models exist, identifying stakeholders with financial interests in the facility may be of use when developing socio-technical context. PRC influence with data centers in Africa can be readily identifiable, or it might be visible only after an investment trail or analysis of partnerships and collaborations. At the time of this study, for example, Wingu.africa is the data center owner and operator of the Djibouti Data Center (DDC), Djibouti City 2 DDC, and Ethio ICT Park DDC in Addis Ababa, Ethiopia, and is building an additional data center in Ethiopia. The controlling interests in Wingu.africa are not fully known. However, Wingu.africa lists many interational ICT operators as its customers, including Chinese state-owned compamies (Wingu Africa, n.d.), (Opiah, 2013). In building the Djibouti City 2 DDC, Wingu.africa has partnered with Djibouti's leading private telecommunications company, TO7 Network, to establish the country's second carrier-neutral data center and the first carrier-neutral cable landing station (Wingu Africa, 2024). Djibouti

Telecom has also been actively involved in expanding and improving ICT infrastructure in Djibouti. The new RAS DIKA data center will be launching in late 2024 in Djibouti City. As a Tier 4 carrier-neutral data center facility in East Africa, the RAS DIKA data center will have direct access to all major international and regional cable systems connecting European, Middle Eastern, and Asian markets with Africa, making Djibouti a strategic ICT hub in the region (Djibouti Telecom, n.d.).[1]

2. **Clouds:** According to the the National Institute of Standards and Technology (NIST) definition, cloud computing includes many different types of services that can be public, private, or some combination thereof. Cloud capabilities are foundational to many ICT solutions, even in developing countries. National data sovereignty concerns may be a possible focus on cloud service provider data handling and data storage locations. Some innovative cloud services, such as with satellite Ground Station as a Service offerings, fuse different ICT components.[2]

3. **ISPs:** Internet Service Providers (ISPs) are companies that provide internet access through broadband services. Connectivity methods (sometimes referred to as "last mile") can be through a variety of means, such as fiber, digital subscriber line (DSL), ethernet, wireless (e.g., mobile or "WiFi"), or satellite. Non-broadband methods include dial-up services via phone lines, although many developing countries in Africa "leap frog" older methods (e.g., dial-up, DSL) and skip to newer methods (e.g., 4G/5G, fiber).

4. **IXPs:** Internet Exchange Points (IXPs) facilitate the interconnection of networks and exchange of internet traffic, ensuring data can be more efficiently and resiliently routed between senders and recipients. IXPs are viewed as a "fundamental bootstrapping step in the development of a region's communication infrastructure" (Bottger et al., 2019). The number of IXPs in Africa has more than doubled in the past 10 years, aided in part by the Africa 80/20 initiatve sponsored by the Internet Society (Internet Society, 2021). The ability to route traffic locally results in several gains, including lower latency and costs, and is also linked to data sovereignty interests and maintaining national data residency.

5. **Hyperscalers:** Hyperscalers are companies that focus on extremely large-scale, efficient, and cost-optimized delivery and management of compute, storage, and networking capabilities. Hyperscaler facilities may include IXPs and Content Delivery Network nodes. Hyperscaler companies are sometimes categorized as operators (e.g., Amazon, Google, Facebook, Microsoft, Alibaba) and others as platform companies (e.g., Oracle, Baidu, China Telecom) (Miller, 2019). Real Estate Investment Trust (REIT) companies (e.g., Equinix, Digital Realty) that lease space are also important stakeholders in this category (Thompson, 2019).

6. **Wireless:** Wireless providers offer mobile and "WiFi" services. Many developing countries have used wireless to leap frog legacy telecom technologies, such as using 2G/3G/4G-based mobile technologies to provide voice and data services instead of copper cable–based infrastructure. As a result, developing countries may have a different set of mobile network evolution issues. For instance, some elements of economic development cannot be skipped over with leap frogging to new technology. Nations still need to provide the core infrastructure such as education, internet access, roads, plumbing, and electricity, in addition to strong social institutions to sustain technology growth. The current focus in many parts of the world is deployment of 5G-based capabilties. The PRC has been working to establish a leadership role

in 5G, with active roles in industry standards as well as application of 5G in targeted vertical industries such as transportation and logistics.

7 **SATCOM:** Satellite Communications (SATCOM) refers to the use of satellite technology in the field of communications. Common SATCOM services are voice and video calling, internet, fax, television, and radio channels. SATCOM provides communication capabilities spanning long distances and operates under conditions that are either infeasible or impractical for other forms of communication (Ross N.,Digital Silk Road PEACE: Satellite Connections to the ICT. 2021). SATCOM is used by commercial, private, military/defense, and disaster relief operations. In addition to SATCOM satellites, some navigational satellites (e.g., GPS, Beidou) and military satellites connect into the ICT ecosystem.

While the discussion on systems thinking began with a decomposition effort, an understanding of the integrated, holistic environment should not be minimized, especially as it concerns critical aspects such as systems integration activities and entities. Understanding the value chain may help focus that effort. Additionally, some ICT environments can be viewed as part of a larger system. For example, smart environments are often linked together, such as the PRC "Shekou" model (Dutton, Kardon, & Kennedy, 2020) that binds ports, parks, and cities into an interrelated and ultimately integrated system.

Consideration 2: Maintain Data Awareness and Protection

Along with a focus on the components and functional layers of the internet model, the data that is associated with the system also requires attention. ICT environments are inherently data rich and are continuing to increase in data volume, in terms of both data transmitted and received (i.e., bandwidth) and the quantity and type of data created and consumed by interconnected devices. Data-driven technologies such as artificial intelligence (AI) and digital twins benefit from access to "big data" data sets, and evolving software-defined infrastructure can use data to improve adaptability, defenses, and performance. The integrity, privacy, and availability of data is essential to effectively utilizing "big data" within a smart (e.g., intelligent) network. Awareness of the types of data in an environment is required to improve data assurance. Once awareness is achieved, then the associated data governance, protection, and sharing considerations can be included in Tech Stack–related analyses. Following the path of service chains and workflows can help reveal the nature and types of data within the system. Service chain data examples include (1) data submitted by users as part of a service (e.g., user credentials); (2) data about system users gathered by system operators (e.g., user account information, tracking of data usage); (3) management data (e.g., operational status of equipment, traffic statistics, error logs); (4) enabling data (e.g., location data utilized by mobile apps, video used by automated vehicles); and (5) data from sensors embedded within the intelligent system (e.g., position, movement of smart/intelligent containers).

Hyperscalers are increasingly building data residency functionality into their data storage solutions, as well as establishing new data centers in a growing number of geographies. For example, Huawei initially leased data center capacity to provide cloud service offerings in South Africa in 2019 (Huawei Cloud Staff Writer,

2019),[3] and has since expanded its strategy by financing and constructing new data centers in partnership with countries, such as Senegal, that are seeking to repatriate their state data and platforms (Reuter Staff, 2021).

PRC-related companies creating intelligent port solutions (e.g., China Merchants Group, IZP Technologies) appear to be establishing solutions that are predicated on creation and exploitation of big data analytics. Furthermore, while some analysis and use of the data may occur near the data sources (e.g., within the port), the proximity of seaports to high-bandwidth undersea connections (e.g., Pakistan East Africa Connecting Europe [PEACE] cable project) facilitates the secure transport of large volumes of port data (and related Port-Park-City data) to distant data centers (e.g., the One Belt One Road big data centers based in China) (Ross & Szot, 2021). Use of port-generated or -related data is of particular concern when indications of potential dual use (i.e., civilian and military) with ICT have been identified with PRC activities in locations such as Djibouti (Lorber, Szot, & Amrosio-Hemphill, 2021).

The need for secure, trusted, interoperable solutions to share data within and across environments is needed for ICT environments, especially those that include multiple embedded components and stakeholders. Smart ports, which include seaports and airports, are a prime example. There is industry recognition of this need; however, efforts to address it are still nascent. The European Union DataPorts project was funded in 2020 to explore creation of an integrated data platform with associated data governance, to enable sharing of data among seaport stakeholders in a secure, private, and trusted manner (Big Data Value (Public-Private Partnership), 2021). Traxens, one of the firms involved in the project, has a smart container solution that provides data on position, movement, ambient temperature, door opening, and shocks (Caceres, 2020). Traxens's first investor was the company CMA CGM (CMA CGM, 2019), which is closely aligned with China Merchants Port Holding Company (CMPort) and an investor in the Djibouti International Container Terminal (Lorber, 2021). Advanced software-enabled cranes are another example. In February 2024, the United States announced a plan to invest billions of dollars to manufacture cargo cranes to replace PRC-built cranes currently used at many U.S. ports. Because they are made by a Chinese state-owned company, these cranes present espionage and logistics threats. Cranes at some ports used by the U.S. military were also flagged as surveillance threats. These types of surveillance threats pose the potential for infiltrating the nation's critical infrastructure by Chinese hackers, which could allow them to detonate crippling cyberattacks.[4]

Consideration 3: Determine Who Is in Control

Control and influence are important dimensions of discussion of the ICT Tech Stack. After decomposing the end-to-end ICT system of interest, and identifying the data that flows within it, consider which entities are managing and controlling the infrastructure and data. This consideration is focused on the ICT digital ecosystem as much as it is on the actors and their objectives, which incorporates insights from accompanying socio-technical analysis. Aspects of particular interest are (1) open platforms and industry standards, (2) partners and collaborators, and (3) effects and impacts.

Some ICT components of interest may be labeled as open, vendor-neutral, or may be identified as

compliant with industry standards or agreements. While these may be viewed as positive attributes, adherence to these principles and references bears further examination to gain insights into their primary influencers. The type and nature of changes to industry standards and technical contributions for ICT domains may indicate strong influences made by industry actors, such as has been identified with PRC activities (Moeller, Vencill, Gilbert, & Mozahebi, 2021). Industry groups such as the International Port Community Systems Association (IPCSA) need to be subject to this type of scrutiny as well. Influence analysis also applies to contributors of open-source software. Identifying the operators of ICT systems is also important, as is awareness of the suppliers of management, business, and operational support systems. Systems integrators also have a potentially influential role in how components are incorporated into and managed in the overall system.

Partnerships and collaborations are another source of potential influence. A detailed understanding of the ICT supply chain can yield important knowledge. Aspects of supply chain risk management may be applicable in this regard, helping to identify all the firms that may have an impact on the system operation. The potential concern for hardware backdoors (e.g., code inside hardware or firmware of computer chips enabling easier access for hackers) inserted within the manufacturing process has been raised. An example is undersea cable systems that carry data and connect to the ICT (Schadlow, 2020).

Collaboration may also obfuscate synergistic threats. China Merchants Group (CMG), the state-owned parent company of the Djibouti port partner CMPort (referenced above) operates other subsidiary organizations supporting the People's Liberation Army power projection activities.[5] CMG partners with China's state-owned LOGINK,[6] a unified digital logistics and trade platform that collects and aggregates vast quantities of global logistics information in the course of its work to increase international clients and build logistics standards. Thus, through CMG (or software-enabled crane companies) the PRC stands to expand its foreign logistics infrastructure and through LOGINK its digital logistics infrastructure. CMG also has military ties, and these relationships have the potential to provide China with crucial offensive or defensive logistics information in a conflict.[7]

Some governments impose blocking or control measures (e.g., filtering, censorship) on content in ICT systems at the national level for information or data entering and/or leaving a country, sometimes referred to as a "digital iron curtain" or "great firewall." The PRC and Russia provide well-known examples of countries establishing control boundaries between their national networks and the global internet. There are concerns that other countries will implement and exercise the capability. As a recent illustration, control over social media platform content is the focus of the recent Twitter block imposed by the government of Nigeria (BBC News Staff, 2021).

Consideration 4: Explore Evolving Technology

The rapidly changing and evolving ICT technology space has many dimensions. The increase in transformation to software-defined functions and infrastructure as code is an important trend within the ICT industry. One result of this trend is that the digital ecosystem component definitions and locations are more dynamic than with prior, traditional networks. For example, the 5G Core service-based architecture includes a modular, cloud-native-based structure that allows for virtualized functions to be specified individually and enables interaction between functions using service-based application programming interfaces.

This approach can be coupled with software-defined networking (SDN) and network functions virtualization concepts, and use of centralized control and orchestration capability. The software-defined infrastructure trend holds benefits from an agility, resiliency, efficiency, and potential cost-effectiveness perspective. However, it also presents new challenges when assessing where PRC-related products may be in use or where PRC entities may have control or influence within ICT systems.

Smart ports are environments where many technologies are being combined and integrated in different ways to achieve specific goals, such as reducing labor costs, improving security and safety, and increasing work efficiency. AI, Internet of Things (IoT), cloud computing, big data, edge computing, and security are integral to the 5G-based smart port solutions that China Mobile has been developing with Huawei and Shanghai Zhenhua Heavy Industries Company Limited (ZPMC) (ZPMC, 2020). The 5G domain can serve as a valuable focal point for identifying where impactful PRC technology-related actions are occurring and potentially posing risks (Medin & Louis, 2019). Specific 5G use cases noted for smart ports include smart tallying/inventory, remote control of Rubber Tyre Gantry cranes, and unmanned container trucks (5G City, 2021). Specific applications running on the multi-access edge computing (MEC) platform include a machine vision application, augmented reality assistance application, autonomous driving application, and remote-control application. BeiDou's global navigation satellite system supports port operation vehicles, ships, and port operation equipment for positioning, monitoring, and collision avoidance (Shuhui, 2019). The integration of these technologies in the context of port workflows can offer value to port stakeholders, but they also pose potential risk regarding data collection, analysis, and exploitation, in addition to being potential points of control and manipulation with port-related data.

Two other PRC areas of interest are Huawei's development of its Harmony mobile operating system (OS) and application of AI. HarmonyOS is intended to compete with Android, and some predict that Huawei may target African countries as markets for mobile and IoT devices based on this operating system (Olander, 2021). Applications of AI within smart environments are another area on which to focus. While the technology may offer solutions to help address challenges such as traffic congestion within cities, significant privacy and surveillance-related concerns (Toh & Erasmus, 2019) are already being raised with projects such as Alibaba's ET Brain for smart cities (called City Brain) (Li, 2018). ET Brain is also being applied to the aviation, industrial, and agricultural sectors. These Alibaba examples, like Huawei's "Safe Cities" (Hillman & McCalpin, 2019)[8] highlight complex systems that involve integration of multiple ICT technologies, and that present a potentially significant risk for PRC implementations.

Consideration 5: Identify Areas of Potential Risk

Identification of risk is dependent on threats and vulnerabilities, probabilities, and impact, along with potential countermeasures or mitigations. Tech Stacks may be helpful in determining high-level risks by guiding associated information collection and organization for further analysis, which may reveal previously uncovered general patterns or trends. As one example, an analysis of smart and intelligent port solutions identified PRC entities that are known to be actively developing and deploying intelligent port solutions. More in-depth study determined that the PRC's influence and presence is more pervasive than

previously realized, specifically in areas such as port operating systems, logistics, and big data analytics (Lorber, Szot, & Amrosio-Hemphill, 2021).

Tech Stack–guided analyses may reveal potential risk of vendor lock-in (e.g., cost of switching to a different vendor is so high that moving to a new solution is not feasible) with ICT solutions, especially when coupled with social technical context. The Digital Silk Road (DSR) project's use of this approach helped identify a pattern of the PRC's influence in specific parts of the digital ecosystem (e.g., data centers, cable landing stations) and in certain ICT environments (e.g., intelligent ports). This type of analysis can also highlight where a more open framework (e.g., for smart ports) may enable increased competition and innovative solutions, such as is being pursued with 5G O-RAN efforts (Gilbert, Houchens, Moeller, Mozaheb, & Vencill, 2021).

Given the global reliance on connectivity, risks related to internet disruptions are also of concern. Studies on internet disruptions have revealed several categories of events, and that different approaches are used when those disruptions are intentional (i.e., not an environmental or accidental outage) (Belson, 2019). Content blocking, throttling, and sub-national and national shutdowns are different categories of intentional disruptions. The risk of intentional disruptions is a greater concern with authoritarian governments that seek to control their citizens' use of the internet. Understanding how intentional disruptions are enabled (e.g., Domain Name System (DNS) blocking, Internet Protocol (IP) blocking, Unified Resource Locator (URL) blocking) (Internet Society, 2017), and specifically with which portions of the ICT digital ecosystem (e.g., cloud provider, ISP) this is accomplished, allows for more effective risk assessment. While this risk is well known in countries like Russia, which has publicly announced testing the separation of the country's networks from the global internet (Marrow & Antonov, 2021), in developing countries in Africa intentional disruption risks may not be well understood. Identification of the actors controlling the relevant ICT components and network operator roles may aid in better understanding the risk of intentional disruptions within the ICT digital ecosystem.

An increasing need to protect data traversing the ICT digital ecosystem presents an opportunity for the U.S. government, private sector, and allies and partners abroad to bolster efforts to protect, secure, and reinforce subsea cables. In addition to countering growing cybersecurity threats from adversaries, securing and protecting the physical infrastructure underpinning internet communication worldwide provides a key opportunity to prevent espionage and disruption while ensuring vital data flows necessary for economic and national security (Sherman, 2021).[9] Network management systems to centralize control over components, such as reconfigurable optical add/drop multiplexers and robotic patch bays in remote network operations centers, are growing in use and introduce new levels of operational security risk. The explosive growth of cloud computing, along with the growing complexity of Tech Stacks, is also increasing the volume and sensitivity of data. For instance, the LOGINK platform (first discussed in Consideration 3) presents the risk that Chinese companies may obtain commercial or military advantage as a result of disrupting or blocking the information flow to some countries while simultaneously routing it to China (Vidal, 2023). Ensuring development of more open Tech Stacks and operational transparency may reduce the risk of surreptitious collection of sensitive data.

Tech Stack Examples

Tech Stack views can be oriented, framed, and filtered to assist with analyzing various aspects of technical competition and provide a basis for comparative analysis. For instance, a smart city or smart port Tech Stack view can provide an overall ICT context, including data producers and consumers embedded within that specific ecosystem. Alternatively, Tech Stack views can provide an in-depth focus on technology advances or research and development efforts for technologies such as SDN, automation and use of AI, and so on. Tech Stacks also provide the basis for temporal analysis about the evolution of ICT capabilities over time.

The following Tech Stack examples illustrate some approaches used to highlight and analyze risk related to PRC digital dominance.

Djibouti Tech Stack

Limited information regarding the Djibouti ICT environment is available; however, based on insights gained from press releases and industry articles, Djibouti's Vision 2035, think tank analyses, and other public sources, a Tech Stack view specific to Djibouti was developed. While not meant to be exhaustive, it reflects notable actors in their relative space in the ecosystem (see Figure 2).

Telecom Djibouti's Tech Stack is dominated by Djibouti Telecom, currently the monopoly provider serving as ISP, wireless provider, and application provider for the its mobile payment service, D-money. Djibouti announced plans to sell a minority stake in Djibouti Telecom; however, details about the privitization effort are limited (Agence France Presse, 2021). Identified PRC entities in the Djibouti Tech Stack include Huawei Marine Networks, ChinaNetCenter (also known as Quantil

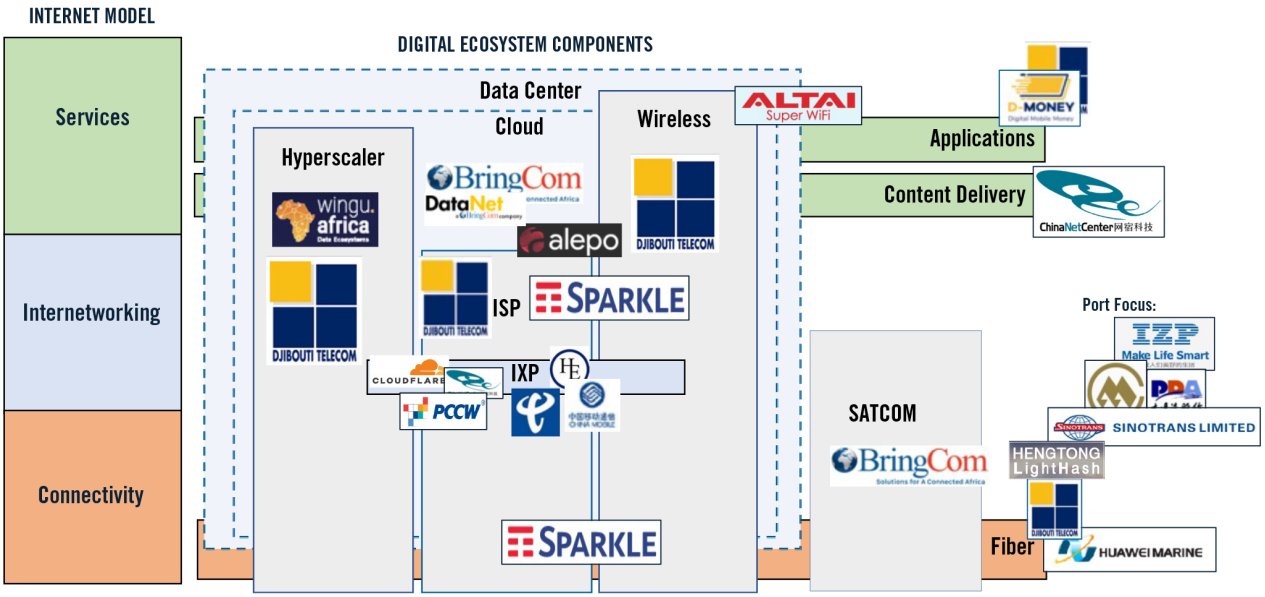

FIGURE 2. DJIBOUTI TECH STACK. JULY 2021: DJIBOUTI ANNOUNCED IT WILL BE SELLING A "SIGNIFICANT MINORITY STAKE" IN DJIBOUTI TELECOM. NOTE: COMPANY LOGOS INCLUDED ABOVE ARE REPRESENTATIVE AND POSITIONED BASED ON KEY PRODUCTS, SERVICES, AND KNOWN CAPABILITIES.

Networks), Hengtong LightHash, China Telecom Global, PCCW, and Altai Super WiFi, in addition to port-specific firms such as China Merchants Group, IZP, and Sinotrans.

While much focus has been on PRC engagement, there is also a Western dimension to the Djibouti Tech Stack. BringCom and Alepo are two of the U.S. firms that have been identified.[10] BringCom provides satellite teleport services and has recently completed fiber deployment and acquisition of a Ugandan ISP, and is offering cloud and enterprise services in Djibouti and several other African countries (BringCom: Solutions for a Connected Africa, n.d.). Alepo is a provider of operational support system (OSS) and business support system (BSS) platforms that aid telcom providers in the efficient operation of their networks and delivery of customer services.[11] Alepo's partners include Altai Super WiFi, a Hong Kong–based firm whose Super WiFi A8 series–based station solution is currently deployed in Djibouti's Doraleh Container terminal ports, providing wireless coverage for daily port operations (Altai Technologies, 2018).

Power, which is an important facet of ICT infrastructure, bears mention here. The "DDC's main power supply is generated from renewable hydro sources located in Ethiopia" and is served by the same substation power distribution facility as the two cable landing stations in Djibouti (Balancing Act Staff, 2018).[12] In the 2020 announcement of its Cape Town Region opening, Amazon Web Services (AWS) noted that its offering is "comprised of three availability zones, each zone with one or more separate data centers each with independent power, networking, and connectivity" (Amazon Web Services Staff, n.d.), highlighting the importance of power to data center resiliency.

Internet Exchange Point (IXP) Component View

A deeper look at the IXP component of the Djibouti Tech Stack was undertaken in an effort to gain additional insights into the technical capabilities and actors within the Djibouti ICT landscape. The Djibouti Internet Exchange Point (DjIX) is housed as a separate facility within the DDC (see Figure 3). DjIX, launched in 2016, is reported to have 14 connected networks with a combined peak traffic rate of 11Gbps (National Institute of Standards and Technology, 2021). By examining the publicly available peering information for DjIX, we can learn more about the providers and networks that are interconnected in Djibouti. Most of this connectivity is transit traffic due to the significant cable landing activity in Djibouti and its strategic geographical position in eastern Africa. This is consistent with socio-technical observations regarding the "digital paradox" in Djibouti (China Merchants Port Holdings Company Limited, 2021), where international data traffic uses Djibouti as a transit point and significantly less traffic is originated or destined for users within Djibouti.

Examining DDC peering information, we observe the presence of Quantil Networks, also known as Wangsu S&T or ChinaNetCenter, a PRC content delivery provider. WIOCC, jointly owned by 14 major African telcos, including Djibouti Telecom, is also present. Attributes found in this peering information may offer some insight into other facets of the ICT environment, such as the capacity of the interconnections and whether they are IPv6 and/or IPv4 capable. Multiple sites[13] offer peering information, and there may be value in comparing data from several reliable sources. On the DDC's website, both China Mobile International (AS 58453) and China Telecom (AS 4134) are listed as networks that peer directly with the DDC,

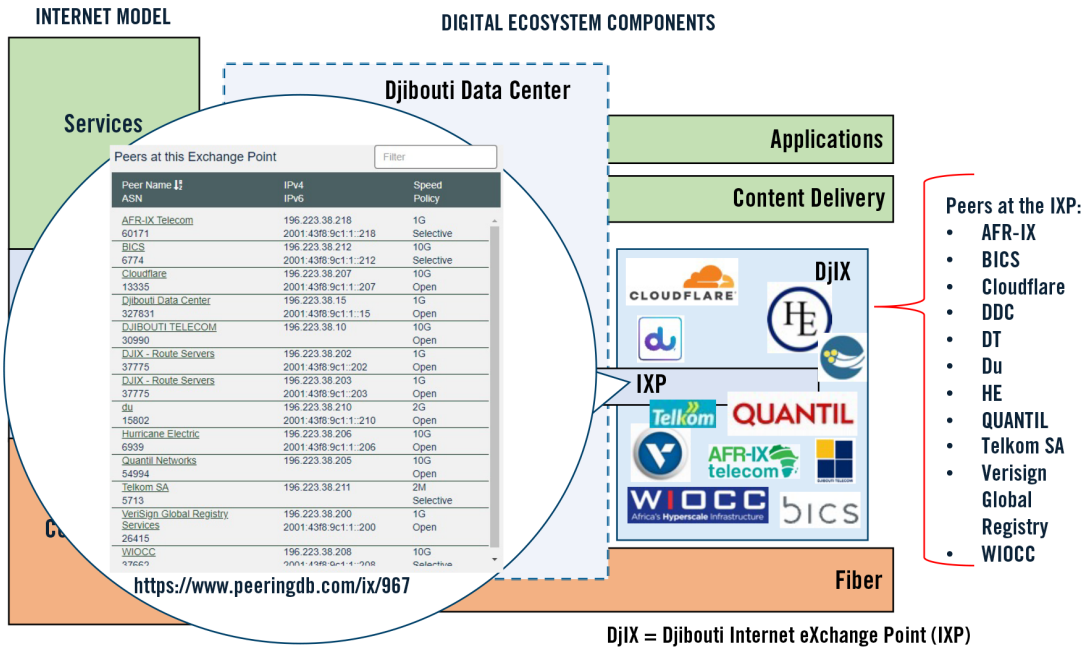

FIGURE 3. DDC AND DJIX: AN IXP VIEW

with both operating at 10G port speeds and both IPv4 and IPv6 capable. In 2016, China Telecom announced that DDC was chosen as an expansion, colocation, and interconnection location (O'Brien, 2019). Peering information for Djibouti Telecom reflects other public peering exchange points (e.g., DE-CIX, DjIX, France-IX) in addition to private peering arrangements, including Interxion in Marseille. MRS2 is the Marseille data center where the PEACE cable landing station resides; Djibouti Telecom is peered at both Marseille data centers: MRS2 and MRS1. The connection with DE-CIX in Marseilles is 20G, with both supporting IPv6 and IPv4.

Tech Stack Extensions

Another way that that PRC ICT influence and activity was explored was via "extensions" to the ICT Tech Stack. In other words, specific portions of the end-to-end ICT environment, such as the undersea cable and satellite connectivity into the ICT Tech Stack, were examined more closely. The DSR task studied the PEACE cable system due to its PRC ownership, with particular focus on the landings in Djibouti and Marseille. Connections from undersea cable systems to the Tech Stack occur in the connectivity layer via terrestrial cable after it has transitioned from the submarine segment. Undersea cables connect via cable landing stations that convert optical signals to digital signals. When satellite system connections are via a teleport, that converts satellite signals to digital signals. See the companion whitepapers (Ross, Digital Silk Road PEACE: Undersea Cable Connections to the ICT, 2021), (Ross, Digital Silk Road PEACE: Satellite Connections to the ICT, 2021) on these topics for further technical details as well as identification of potential areas of risk and mitigations.

Smart Port System Framework

The development of the Smart Port System Framework, this paper's final example of Tech Stack usage, was compiled to enable better understanding and organization of facets of seaports for further analysis. The framework as depicted in Figure 4 was inspired by elements of leading smart ports and smart cities projects. This ICT-centric framework aided in the data collection and analysis of the ports, especially where the PRC is actively involved. The analysis included PRC activities in the IPCSA, which is an industry group that supports initiatives related to the development of port community systems in both seaports and airports.

In building on the Tech Stack foundation, a sensor layer was added to the Smart Port System Framework illustration for emphasis. Through this addition, a more focused approach is taken to the devices that are interconnected within this environment. A sensor is a connected device whose primary or ancillary functions include collecting information and acting, potentially autonomously, based on its instantiation of connectivity, internetworking and services, and applications that it contains.

The final addition to the framework was considering the intelligent operations within the port. This effectively positions the various use cases of interest alongside the relevant sensors/devices, digital ecosystem components, and layers of the internet model. While Figure 4 does not provide a precise positioning of some of these elements, it does draw attention to the multitude of connected devices and the workflows in which they are involved, and ideally highlights the various points of value to port stakeholders.

The PRC is actively leading intelligent port development, bringing together PRC state-owned entities, firms, and partners to research, trial, and implement advanced capabilities that will enable ports to meet their goals of improved efficiency, safety, and labor/cost savings. These advancements help the PRC move closer to its goal of leading the global supply chain. Please refer to the Smart Ports paper (Ross & Szot, 2021) for further details, observations, and recommendations.

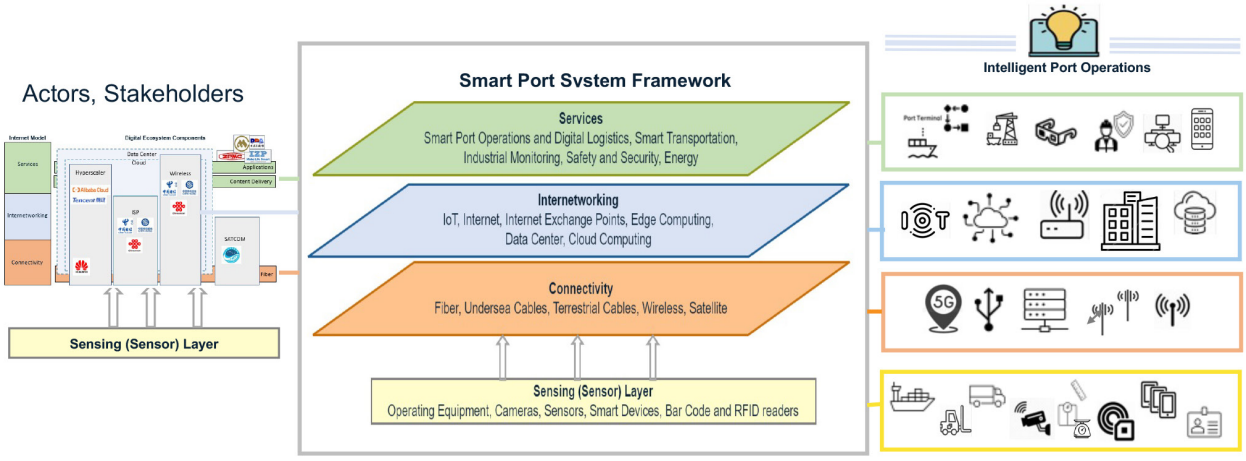

FIGURE 4. SMART PORT SYSTEM FRAMEWORK. A SMART PORT INTEGRATES SENSING AND ICT CAPABILITIES TO ENABLE EFFICIENT INFORMATION MANAGEMENT AND AUTOMATED OPERATIONS.

Final Observations on DSR Tech Stacks

DSR Tech Stacks was valuable for organizing, investigating, and assessing implications from various points of view, such as for a country (e.g., Djibouti), an ecosystem component (e.g., IXP), a technology domain (e.g., 5G), and an environment (e.g., smart port). High-level Tech Stack views are notional and should be viewed as a guide to be adapted to the specific ICT area under study. Tech Stack content may be current for only a limited period, requiring refresh of dynamic aspects such as emerging or evolving technologies (including new vulnerabilities or mitigations), ICT regulatory or policy positions, changes impacting actors (e.g., elections, new product releases, company acquisitions, partnerships, investments), and updates from industry organizations (e.g., standards development).

The DSR Tech Stack activities were based entirely on information from public sources. Much like software development approaches that "code low, deploy high" (Raytheon Technologies, 2020), there may be value for some stakeholders in making use of this approach in an unclassified environment and then porting the results for use in other secure settings.

Findings from associated analyses can provide valuable input to the development of COAs, modeling, or serious games (e.g., a paper-based modeling game). Patterns of interest may be revealed through study of these environments, helping to identify areas for further study. Early indications of trends may also be revealed. For example, some recently identified evidence of PRC activity in and around Mombasa could reflect an expansion or shift of PRC investment and focus from Djibouti to adjacent areas of strategic interest.

Working through the five considerations can prove valuable for identifying the most significant technologies, architectures, actors, partnerships, and government and commercial activities that are relevant to ICT environments under study.

About the Authors

Nancy Ross is an Infrastructure Engineer in the Cloud, Network, and Digital Service Engineering department of MITRE Labs. Nancy provides technical and leadership expertise on enterprise architecture, network engineering, cloud, and IoT. Prior to joining MITRE, Nancy served as Senior Vice President, Service Operations at Avaya Government Solutions leading government, commercial, and international telecommunications operations.

Kathy Szot is a Cybersecurity Engineer in the Cloud, Network, and Digital Service Engineering department of MITRE Labs. Kathy provides technical and leadership expertise pertaining to communications infrastructure, cybersecurity, and network engineering. Prior to joining MITRE, Kathy held multiple roles within Verizon at the Director and Distinguished Member of Technical Staff levels.

Maggie Vencill is a Technical Program Manager at the Center for Policy and Strategic Competition. Maggie is an experienced project leader who provides expertise in the area of strategic competition and technology protection to multiple government agencies. Additionally, Maggie is a certified Lean Six Sigma Black Belt with more than 20 years of experience in the commercial and government sectors.

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

The views, opinions, and/or findings contained herein are those of the authors and should not be construed as an official government position, policy, or decision unless designated by other documentation.

Endnotes

[1] Smart Africa - An Overview and Djibouti Telecom's Contributions - Djibouti Telecom, accessed February 2024.

[2] Examples include https://aws.amazon.com/ground-station/ and https://azure.microsoft.com/en-us/blog/introducing-azure-orbital-process-satellite-data-at-cloudscale/

[3] Huawei noted that it "is leasing a data centre in Johannesburg from a partner from where it is deploying localised public cloud services based on local industry policies, customer requirements and partner conditions."

[4] U.S. to Invest Billions to Replace China-Made Cranes at Nation's Ports, https://www.wsj.com/politics/national-security/u-s-to-invest-billions-to-replace-china-made-cranes-at-nations-ports-d451ef8f?mod=hp_lead_pos1, Dustin Volz, Gordon Lubold, February 21, 2024.

[5] China Maritime Report No. 4: Civil Transport in PLA Power Projection, CMSI China Maritime Reports, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1003&context=cmsi-maritime-reports, Connor M. Kennedy, December 2019.

[6] LOGINK: Risks from China's Promotion of a Global Logistics Management Platform, https://www.uscc.gov/research/logink-risks-chinas-promotion-global-logistics-management-platform, U.S.-China Economic and Security Review Commission, Staff Issue Brief, September 20, 2022.

[7] China's LOGINK Logistics Platform and Its Strategic Potential for Economic, Political, and Military Power Projection. Baker Institute for Public Policy, https://www.bakerinstitute.org/research/chinas-logink-logistics-platform-and-its-strategic-potential-economic-political-and, Gabriel Collins, Jack Bianchi, April 25, 2023.

[8] Note: Huawei "Safe Cities" have been identified in Ghana, South Africa, Mauritius, Botswana, Nigeria, Ivory Coast, Uganda, Madagascar, Kenya, Ethiopia, Angola, and Cameroon.

[9] Cyber Defense across the Ocean Floor: The Geopolitics of Submarine Cable Security, Cyber defense across the ocean floor: The geopolitics of submarine cable security - Atlantic Council, Justin Sherman, September 13, 2021.

[10] Alepo described Djibouti Telecom (DT) as "its long standing client" in 2015 when it was announced that DT would be upgrading to the latest version of Alepo's Service Enabler platform, which is considered "a complete carrier-grade BSS/OSS framework." While it is not known whether Alepo is working with DT on 5G, it claims to be "one of the industry's leading 5G Core vendors" and that it has "tactfully designed a 5GC solution comprising cloud-native 3GPP standards-compliant 5GC network functions (NFs) responsible for implementing subscription services, providing secured connectivity to subscribers, and handling charging and policy management."

[11] A related PRC note: Alibaba's Whale Cloud company (based on an acquisition of ZTESoft) also offers cloud and OSS/BSS services specifcally targeted to African telecom providers; MTN Rwanda is using Whale Cloud's digital BSS suite to transform legacy systems, including billing and Customer Relations Management platforms. To date, no indication of Whale Cloud use in Djibouti has been found.

[12] In this 2018 interview with the DDC Chairman John Melick III, he notes that the Djiboutian cable landing stations are both operated by Djibouti Telecom.

[13] Examples of sites include peeringdb.com (note that historical data from this site has been used to analyze trends over time with IXP expansions and associated impacts, ref: https://arxiv.org/pdf/1810.10963.pdf), Looking Glass Data (providing insight to routing tables, useful with troubleshooting routing issues, ref: https://bgp4.as/looking-glasses), and location-specific data such as found at http://www.djiboutidatacenter.com/en/page/peering-networks.

References

1. 5G City. (2021, April 1). China Ningbo 5G/MEC Smart Port. Retrieved October 2021, from YouTube: https://www.youtube.com/watch?v=hY-fQOP67p
2. Accenture. (2020). Hyperscale Your Cloud Journey. Retrieved October 2021, from https://www.accenture.com/_acnmedia/PDF-143/Accenture-Hyperscale-Cloud-Journey.pdf. Page unavailable March 2024.
3. Agence France Presse. (2021, July 11). Djibouti to Sell Minority Stake in State-Owned Telco. Retrieved October 2021, from https://www.barrons.com/news/djibouti-to-sell-minority-stake-in-state-owned-telco-01626011706
4. Alepo. (n.d.). 5G Core (5GC) Network Solutions. Retrieved October 2021, from https://www.alepo.com/solutions/5g-core-network-solutions/
5. Alepo. (n.d.). Operations Support System. Retrieved October 2021, from https://www.alepo.com/products-services/operations-support-system-oss-solution/
6. Altai Technologies. (2018). Altai Automates Container Port in Africa. Retrieved October 2021, from https://www.altaitechnologies.com/wp-content/uploads/2020/06/200604-Case-Study-Altai-Automates-Container-Port-in-Africa.pdf
7. Amazon Web Services Staff. (n.d.). The AWS Africa (Cape Town) Region: Dream, Build, Grow. Retrieved October 2021, from https://aws.amazon.com/local/africa/cape-town/
8. Balancing Act Staff. (2018, September 28). Djibouti Data Centre's John Melick III on Two New International Cable Connections for the Region and Operating Neutral, Third Party Combined Landing Stations and Data Centres. Retrieved October 2021, from Balancing Act: https://www.balancingact-africa.com/news/telecoms-en/44062/djibouti-data-centres-john-melick-iii-on-two-new-international-cable-connections-for-the-region-and-operating-neutral-third-party-combined-landing-stations-and-data-centres. Page unavailable March 2024.
9. BBC News Staff. (2021, June). Nigeria's Twitter Ban: Government Orders Prosecution of Violators. Retrieved October 2021, from BBC News: https://www.bbc.com/news/world-africa-57368535
10. Belson, D. (2019, December 18). From Content Blocking to National Shutdowns: Understanding Internet Disruptions. Retrieved October 2021, from Internet Society: https://www.internetsociety.org/blog/2019/12/from-content-blocking-to-national-shutdowns-understanding-internet-disruptions/
11. Big Data Value (Public-Private Partnership). (2021, June 29). DataPorts - A Data Platform for the Connection of Cognitive Ports. Retrieved October 19, 2021, from YouTube: https://www.youtube.com/watch?v=4IPiiKdysyU

12. Bottger, T., et al. (2019, July 9). Shaping the Internet: 10 Years of IXP Growth. Retrieved October 28, 2021, from https://arxiv.org/pdf/1810.10963.pdf

13. BringCom: Solutions for a Connected Africa. (n.d.). Cloud & Connectivity Services. Retrieved October 2021, from https://www.bringcom.com/services/cloud-connectivity-services/. Page unavailable March 2024.

14. Caceres, S. (2020, November 4). A Data Platform for the Cognitive Ports of the Future. Retrieved October 2021, from YouTube: https://www.youtube.com/watch?v=ec5X-hTqn8U

15. Champion, M. (2019, June 11). The U.S. China Race for Tech Dominance is the Worst Game of Twister Ever. Retrieved October 2021, from Bloomberg: https://www.bloomberg.com/news/articles/2019-06-12/the-digital-iron-curtain-looks-like-spaghetti. Page unavailable March 2024.

16. China Merchants Port Holdings Company Limited. (2021, November 3). TL Companies in the United States. Retrieved October 2021, from http://www.cmport.com.hk/EN/business/Detail.aspx?id=10000819

17. CMA CGM. (2019, May 23). CMA CGM is Ordering 50,000 Traxens Trackers, Increasing Its Offer of Connected Containers. Retrieved October 2021, from http://www.cma-cgm.com/news/2565/cma-cgm-is-ordering-50-000-traxens-trackers-increasing-its-offer-of-connected-containers

18. Djibouti Telecom. (n.d.). About Djibouti Telecom. Retrieved February 26, 2024, from https://international.djiboutitelecom.dj/about/

19. Dutton, P. A., Kardon, L. B., & and Kennedy, C. M. (2020, April). China Maritime Report No. 6: Djibouti: China's First Overseas Strategic Strongpoint. Retrieved April 2021, from U.S. Naval War College: https://digital-commons.usnwc.edu/cmsi-maritime-reports/6/

20. Gilbert, C., Houchens, J., Moeller, C., Mozaheb, A., & Vencill, M. (2021, May). The Case for U.S. Leadership in Trusted 5G Infrastructure. Retrieved October 2021, from https://www.mitre.org/sites/default/files/publications/pr-21-1488-the-case-for-u.s.-leadership-in-trusted-5G-infrastructure.pdf

21. Gulati, A. (2015, April 28). Djibouti Telecom Modernizes Fixed Broadband Network with Alepo BSS/OSS Upgrade. Retrieved October 2021, from https://www.alepo.com/djibouti-telecom-modernizes-fixed-broadband-network-with-alepo-bssoss-upgrade/

22. Hillman, J. E., & McCalpin, M. (2019, November). Watching Huawei's "Safe Cities". Retrieved October 2021, from https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/191030_HillmanMcCalpin_HuaweiSafeCity_layout_v4.pdf

23. Huawei Cloud Staff Writer. (2019, March 5). Huawei Cloud Now Available in South Africa. Retrieved October 2021, from Huawei: https://businesstech.co.za/news/cloud-hosting/303386/huawei-cloud-now-available-in-south-africa/

24. Ilyushina, M., Hodge, N., & Gold, H. (2019, November 1). Russia Rolls Out Its "Sovereign Internet." Is It Building a Digital Iron Curtain? Retrieved October 2021, from CNN Business: https://www.cnn.com/2019/11/01/tech/russia-internet-law/index.html

25. Internet Society. (2017, March 24). Internet Society Perspectives on Internet Content Blocking: An Overview. Retrieved October 2021, from https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

26. Internet Society. (2020, June 22). Growning the Internet--Explainer: What Is an Internet Exchange Point (IXP)? Retrieved October 2021, from https://www.internetsociety.org/resources/doc/2020/explainer-what-is-an-internet-exchange-point-ixp/

27. Internet Society. (2021, July 6). Growing the Internet--Moving toward an Interconnected Africa: The 80/20 Initiative. Retrieved October 2021, from https://www.internetsociety.org/resources/doc/2021/moving-toward-an-interconnected-africa-the-80-20-initiative/

28. Kende, M. (2021, July). Moving toward an Interconnected Africa. Retrieved October 2021, from Internet Society: https://www.internetsociety.org/wp-content/uploads/2021/07/2021-Moving-toward-an-Interconnected-Africa-EN.pdf

29. Li, J. (2018, September 5). Introduction to Alibaba ET CIty Brain. Retrieved October 2021, from YouTube: https://www.youtube.com/watch?v=mX6hzp6OcYw

30. Lorber, M. (2021). Djibouti Digital Silk Road Case Study: PEACE Cable Actors and Objectives. McLean, VA: The MITRE Corporation.

31. Lorber, M., Szot, K., & Amrosio-Hemphill, T. (2021). We Connect the World: "Point-Line-Plane" Strategy along the Silk Road. McLean, VA: The MITRE Corporation.

32. Marrow, A., & Antonov, D. (2021, July 22). Russia Disconnects from Internet in Tests as It Bolsters Security - RBC Daily. Retrieved October 2021, from Reuters: https://www.reuters.com/technology/russia-disconnected-global-internet-tests-rbc-daily-2021-07-22/

33. Medin, M., & Louis, G. (2019). The 5G Ecosystem: Risks & Opportunities for DoD. Washington, DC: Defense Innovation Board. Retrieved from https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF

34. Miller, R. (2019, September 10). Who Are the Data Center's Industry's Hyperscale Players? Retrieved October 2021, from Data Center Frontier: https://datacenterfrontier.com/data-centers-industry-hyperscale-players/

35. Moeller, C., Vencill, M., Gilbert, C., & Mozahebi, A. (2021, February 12). Securing Western Leadership in Global 5G Standards and Patents. Retrieved October 2021, from https://www.mitre.org/sites/default/files/publications/pr-21-0045-securing-western-leadership-in-global-5g-standards-and-patents.pdf

36. Morris, A. (2016, December 8). China Telecom Global Picks Djibouti as Hub for East Africa Expansion. Retrieved October 2021, from Connecting Africa: http://www.connectingafrica.com/document.asp?doc_id=728852

37. National Institute of Standards and Technology. (2021, October 12). NIST Cloud Computing Program - NCCP. Retrieved October 2021, from https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp

38. O'Brien, D. (2019, October 10). China's Global Reach: Surveillance and Censorship beyond the Great Firewall. Retrieved October 2021, from Electric Frontier Foundation: https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall

39. Olander, E. (2021, June 4). Why Huawei's Much Ridiculed New OS Could Still Have a Big Impact in Africa. Retrieved October 2021, from The ChinAfrica Projct: https://chinaafricaproject.com/podcasts/why-huaweis-much-ridiculed-new-os-could-still-have-a-big-impact-in-africa/

40. Opiah, A. (2013, October 9). Infiltrating Data Centres in the Horn Of Africa. Retrieved October 2021, from Warsan: https://thewarsan.com/infiltrating-data-centres-in-the-horn-of-africa-abigail-opiah/

41. Raytheon Technologies. (2020, March 12). Code Low, Deploy High. Retrieved October 2021, from Raytheon Intelligence & Space: https://www.raytheonintelligenceandspace.com/news/feature/code-low-deploy-high

42. Reuter Staff. (2021, June 22). Senegal Aims for Digital Sovereignty with New China-Backed Data Centre. Retrieved October 2021, from Reuters: https://www.reuters.com/article/senegal-datacenter-idINL5N2O44D3
43. Ross, N. (2021). Digital Silk Road PEACE: Satellite Connections to the ICT. McLean, VA: The MITRE Corporation.
44. Ross, N. (2021). Digital Silk Road PEACE: Undersea Cable Connections to the ICT. McLean, VA: The MITRE Corporation.
45. Ross, N., & Szot, K. (2021). MTR210314 Smart Ports: How They Play a Key Role in the Great Power Competition. McLean, VA: The MITRE Corporation.
46. Schadlow, N. (2020, July 1). Protecting Undersea Cables Must Be Made a National Security Priority. Retrieved October 2021, from Hudson Institute: https://www.hudson.org/research/16195-protecting-undersea-cables-must-be-made-a-national-security-priority
47. Schmore, R., & Kwoun, J. (2021, Jan-Feb). Analytic Tradecraft Standards. Military Review. Retrieved October 2021, from https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2021/Kwoun-Tradecraft-Standards/
48. Sherman, J. (2021, September 13). Atlantic Council. Retrieved February 26, 2024, from https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/
49. Shuhui, W. (2019). Smart Port Construction. China-ASEAN Port Cities Cooperation Network International Exchange and Training. Qinzhou: Economic Management School, Beibu Gulf University.
50. Speedcheck Wiki. (n.d.). Internet Service Provider (ISP). Retrieved October 2021, from https://www.speedcheck.org/wiki/isp/
51. Thompson, A. (2019, July 10). 5 Top Data Center REITs to Consider. Retrieved October 2021, from Consulting WP: https://www.reits.org/investing/5-top-data-center-reits-to-consider/
52. Toh, M., & Erasmus, L. (2019, January 15). Alibaba's "City Brain" Is Slashing Congestion in Its Hometown. Retrieved October 2021, from CNN Business: https://www.cnn.com/2019/01/15/tech/alibaba-city-brain-hangzhou/index.html
53. Tuber, D., & Giotsas, V. (2021, September 16). Unboxing the Last Mile: Introducing Last Mile Insights. Retrieved October 2021, from Cloudflare: https://blog.cloudflare.com/last-mile-insights/
54. Vidal, A. (2023, July 25). Center for Maritime Strategy. Retrieved February 26, 2024, from https://centerformaritimestrategy.org/publications/securing-maritime-data-the-battle-against-chinas-logink-in-u-s-and-european-ports/
55. Whale Cloud. (2021, May 7). MTN Rwanda Accelerates Digital Transformation with Whale Cloud Digital BSS Suite. Retrieved October 2021, from https://online.iwhalecloud.com/NewsDetail/70
56. Wingu Africa. (2023, February 29). Wingu Africa. Retrieved from www.wingu.africa
57. Wingu Africa. (2024, February 22). Wingu Africa. Retrieved from www.wingu.africa
58. Wingu Africa. (2024, February 29). Wingu.Africa/Our Locations. Retrieved from https://www.wingu.africa/our-locations/djibouti-city-2-djibouti/

59. Wingu Africa. (n.d.). Who We Are: Regional Data Centers Offering Open Access and Carrier Neutrality. Retrieved October 2021, from https://www.wingu.africa/about/. Page unavailable March 2024.

60. WIOCC. (n.d.). Shareholders. Retrieved October 2021, from https://wiocc.net/shareholders-2/

61. ZPMC. (2020, October 21). 5G Smart Port: The World's Most Widely Deployed 5G Smart Port Solution. Retrieved October 2021, from YouTube: https://www.youtube.com/watch?v=24pjf1t7luQ