Journal of International Business Studies (2022) 53, 344–361

www.jibs.net

INVITED RESEARCH NOTE

A general framework of digitization risks in international business

Yadong Luo

Department of Management, Miami Herbert Business School, University of Miami, Coral Gables, FL 33146, USA; Sun Yat-Sen University Business School, Guangzhou, China

Correspondence:
Y Luo, Department of Management, Miami Herbert Business School, University of Miami, Coral Gables, FL 33146, USA
e-mail: yadong@miami.edu

Abstract
Digital global connectivity offers multinational enterprises new opportunities, but it also brings unique risks, an area not yet well examined in international business. This article presents an organizational information-processing framework, which elucidates what (risk types and sources), how (risk assessing and managing), and whom (vulnerable firms) these risks relate to, in a dialectical manner that seeks to combine theoretical insights and managerial actions. We focus on three types of risks (digital interdependence, information security, and regulatory complexity) that MNEs uniquely face, and explain within-country and cross-country risk drivers. We document variances among MNEs in exposure to these risks, proposing that information flow intensity, geographic diversity, international strategy, and global platform participation carry strong implications on the firm's risk exposure and response. Finally, this framework offers actions essential for MNEs, individually and collectively, to manage digital risks, emphasizing processes of building and deploying digital intelligence in pursuit of transnational resilience for cross-border activities that become increasingly digitally connected.
Journal of International Business Studies (2022) **53**, 344–361.
https://doi.org/10.1057/s41267-021-00448-9

Keywords: digital risk; digitization; digital connectivity; risk exposure; risk management

INTRODUCTION

Digitization reshapes international business in a myriad of ways, and presents a new frontier for IB research (e.g., Benito, Petersen, & Welch, 2019; Cantwell, 2009; Hennart, 2019; Nambisan, Zahra, & Luo, 2019; van Tulder, Verbeke, & Piscitello, 2019). Digitally connected global firms reap the benefits of many new opportunities, such as obtaining global resources, reaching foreign customers, and improving efficiency for global operations, but business leaders cannot underrate associated risks. In fact, managing risk forms one of the primary objectives of firms operating internationally (Miller, 1992, 1998; Tong & Reuer, 2007; Werner, Bouthers, & Bouthers, 1996). Yet, IB scholarship has so far only focused on the political, financial, and transactional risks in international business (Rugman, 2009), leaving digitization-related risks largely unaddressed. Threats arising within an increasingly digitized environment prompt the need for more thorough study, opening a host of important questions for the IB research community to explore.

Received: 2 July 2020
Revised: 4 April 2021
Accepted: 10 April 2021
Online publication date: 27 May 2021

Scholars seeking to understand the dangers arising from digital connectivity need to define and delineate the risks, which range from overdependence to cyber attacks. Researchers in the field stand uniquely positioned to examine the ripple effects of information breaches, supply disruption, cyber crimes, and other digital breakdowns, since these disruptions are often global in nature, not confined to one country or region (McKinsey, 2020). Digitization itself entails critical risks, yet digital connectivity technologies, intelligence, and capabilities may be used wisely to curtail them (Chinn, Kaplan, & Weinberg, 2014). This juxtaposition compels us to look at the potential hazards under a unified lens that combines risks and capabilities in digitization and integrates mandates for both global compliance and local adaptation. For an MNE, failure from leadership to address digitization threats could cause huge contagion damages not just to the global operations within the firm and with partner firms in various countries and industries but also to the company's global reputation and the public's goodwill. For this reason, we develop our framework from the information-processing logic (Egelhoff, 1991; Tushman & Nadler, 1978), which holds that information-processing needs increase when uncertainties and risks aggravate, in turn requiring accentuated information-processing capabilities. This theory can also guide us to pinpoint what information related to digital risk (from within-country to cross-country) should be processed, how distinctive digital risks should be aligned differently with information-processing needs and capabilities, and what type of multinational enterprises (MNEs) are particularly vulnerable to potential hazards from a digital environment.

In this study, we define digital globalization as a form of globalization that digitally connects businesses across nations with flows of data, information and knowledge, and digitally enabled flows of goods, services, investment, and capital. We analyze digital risks in global operations and prescribe ways to evaluate and manage them. Our study includes a look at how MNEs can curb these risks both individually and collectively. Additionally, we consider how MNEs diagnose related risk items both within and across countries, followed by the ways to manage these threats through ameliorated information-processing capabilities. We also acknowledge the diversity and divergence of MNEs in their exposure to these risks, since they vary in their level of susceptibility to the digital disruptions that plague global activities. This study highlights that an MNE's information intensity, geographic diversity, international strategy, and platform participation have implications on risk exposure and response. We foresee a pressing need for IB scholars to provide a more nuanced understanding of the identified risks and offer our suggestions to push this frontier forward.

DEFINING DIGITAL RISKS

Risk signifies a probability of a negative occurrence caused by external or internal vulnerabilities that threaten business activities. We define *digital risk* in IB as uncertainty or disruption, caused by digitization forces in countries wherein the MNE operates or competes, that adversely impacts company operations. As globalization enters a new era full of disruptions and adversities, which heighten both new and old IB risks, digital connectivity acts as a double-edged sword, serving as both an enabler for cross-border activities when harnessed properly and a disrupter when not. Digital connectivity is made possible through digital platforms, information and communication technologies (ICT), internet and intranet access, and other digital technology enablers, such as big data, cloud services, and data analytics and intelligence. Digitalization buttresses cross-border transactions, while transmitting a valuable stream of ideas and innovation around the world (Banalieva & Dhanaraj, 2019; Hennart, 2019; Kano, 2018; Tallman, Luo, & Buckley, 2018). Yet, beyond the benefits, inherent risks ensue, with the following three types of digital risks worth elaboration.[1]

Digital Interdependence Risk

Digital interdependence risk manifests as unexpected breakdowns, contagions, and interruptions caused by digital interconnectivity between a focal MNE and its worldwide business partners, vendors, suppliers, distributors, customers, and corporate members in various countries. Digital globalization makes international companies more dependent on others, thus making them subject to more contagion effects from all risks facing them and partnering units (McKinsey, 2020). A more interconnected, digital world magnifies the impacts of external shocks and spreads ripple effects faster. The 2008 financial crisis showed how rapidly the linkages between the world's capital markets can allow contagion to spread.[2] Digital connectivity accelerates and widens the adverse spreading of a

global platform's breakdown, as a whole or in part, reflecting digital fragility due to interdependence.

While digitization bolsters interdependence for businesses that rely on digital connections and platforms, the connectivity also helps international businesses cope better with disruptions and adversities (e.g., COVID-19 pandemic). Thus, digital global connectivity is both a dominant feature of the new era for international business and a critical catalyst to address new adversities and uncertainties in the post-pandemic era. This double-edged sword effect summons scholarly attention in two ways. One, firms vary in their vulnerability to digital risk, and two, firms differ in their ability to circumvent digital risks for global operations. We follow-up on these issues in a later section.

Global Information and Cyber Security Risk

Global information and cybersecurity risk refers to potential loss or harm stemming from an MNE's fragility in its information and communications systems, which may result in cyber attacks or data breaches. Digitization expands the marketplace to a global arena and pushes MNEs to be more dependent on the exchange of information, data, and ICT infrastructure. Global customers are reluctant to use a digital outlet that does not offer privacy protection, and want assurance that the business provides the best possible security, availability, reliability, and performance (Nambisan et al., 2017; UNCTAD, 2015). Accordingly, as information flows across borders, corporate concern for data security grows (EIU, 2014). New technology renders companies vulnerable to threats of security breaches, fraud, disruption of services, and failure to meet service levels, and the vulnerability increases for international businesses. Many MNEs have already undergone security breaches from internal and external sources, a new type of IB risk involving both economic and social symptoms (World Bank, 2016). The indirect damage of such breaches, which might include the loss of valuable data, consumer trust, and business reputation, can be immense and difficult to recover from. For these reasons, firms must think beyond physical security and consider protecting themselves against intangible risks.

Beyond the already well-known cyber crime, cyber terrorism, and cyber espionage phenomena that constitute a national security threat, information security cyber attacks arise as a new type of IB risk for virtually all MNEs. As international transactions and processes become more digitized, global companies find themselves increasingly prone to vicious cyber attacks (Kshetri, 2005). High profile hacks and breaches have already hit many of the world's largest companies. Cyber crime, including consumer data breaches, financial crimes, market manipulation, and theft of intellectual property, costs the global economy about US$400 billion in annual losses.[3] Almost certainly, cyber attacks will multiply and affect more businesses in the future, and companies that lack adequate technological capability and security knowledge are even more susceptible. While tools such as firewalls have become a standard for securing devices and zones, risk management in the digital age requires a big picture, managed-service approach which can protect entire IT ecosystems over time. That is, the focus in cyber security is changing from devices to services.

Digital Regulatory Complexity Risk

Digital regulatory complexity risk occurs due to the many different aspects of digitalization-related regulations, rules, and standards imposed in the various countries where an MNE operates, creating regulatory multiplicity, variance, and incompatibility that exacerbate disruptions to cross-border activities. An amicable institutional environment produces a seamless and consistent user experience around the world (Oxley & Yeung, 2001). However, the increasing level of regulations by many governments, in developed and developing countries alike, cover a number of areas in data protection. The scope of regulations is widening, with additional scrutiny placed on areas like customer protection, digital taxes, information security, and national security. The extent and implications of these regulations directly drive the need to prepare for digital risks. For instance, in preparing for the General Data Protection Regulation in Europe, banks and other financial institutions must take the necessary steps to bolster their digital capabilities, such as adopting sophisticated techniques for customer master data management.[4]

Many governments around the world currently consider limitations on what kind of data can be transmitted beyond country borders and where data must be stored. Some are moving toward regulations that would require companies to use servers physically located within their borders to process and store data generated there. Variations of this type of law exist in Indonesia, Nigeria, Russia, Vietnam, and many others (Manyika, Lund, Bughin, Woetzel, Stamenov, & Dhringra, 2016).

Meanwhile, the Great Firewall of China acts as the combination of legislative actions and technologies enforced by the country's government to regulate the internet domestically. Yet, regulations to protect privacy signify an important part in unleashing the benefits of digital connectivity, since total freewheeling use of the internet, or no governmental restrictions on internet content, may not be advisable due to the dark side of digitization. The privacy of citizens and users of digital connections have to be safeguarded (UNCTAD, 2015).

Sources of Digital Risks

Knowing the underlying sources for the above risks warrants equal attention. MNEs are prone to these threats not only within individual countries but also from supranational forces, demarcating two main sources: within-country and cross-country. Under each, several specific items exist that reflect and contribute to digital risk. In this study, within-country risk items focus on a foreign *target country* and cross-country risk items deal with bilateral or international factors such as home-/host-country relations and geopolitics.

Within-country (target country) sources

Within-country sources entail governmental or regulatory policy restrictions over digital connectivity and digital commerce, as well as policy discrimination and barriers against foreign firms. Legal standards that prevent digital, e-commerce, and internet frauds fall under this category. Other important regulatory items include weak protection over digital intellectual property rights (e.g., artificial intelligence; AI) and poor transparency in enforcing economic and regulatory policies toward digital connectivity. A target country's economic conditions, such as the soundness of key economic sectors (e.g., electronic, internet, ICT) and its ability to connect with the world, will significantly impact a foreign firm's global connectivity. A myriad of physical conditions also affect the country's digital risks. These include broadband supply (fiber optics, 4G or 5G coverage), international internet bandwidth, internet data routes, mobile telecommunications, communications satellite, network infrastructure, data centers, cloud investment, big data investment, and Internet of Things investment by governmental and private sectors (UNCTAD, 2015; World Bank, 2016).

Cross-country sources

Geopolitics becomes a primary factor within the category of cross-country sources. Amid the trade disputes between the United States and numerous countries (China, in particular), many governments' scrutiny of takeovers by foreign companies has increased, with a sharper focus on the implications for national security and technological advantage associated with ICT and other digital developments. Accordingly, a growing divergence in digitization systems and ICT standards between economies exists (e.g., one based on US-led norms and rules and the other around China's in the 5G network).[5] Deteriorating home-/host-country ties further exacerbate this complexity. MNEs can easily get hit by worsened bilateral relationships between home and host countries (or regions).[6] Additionally, the digital era makes MNEs more susceptible to risks caused by international events unfolding beyond the foreign target country, including terrorism and cyber attacks. Digital technologies have made it easier for criminal groups or individuals to conduct foreign assaults, in secret or by proxy, putting businesses on the front line (Kshetri, 2005).

VARYING EXPOSURE TO DIGITAL RISKS

Figure 1 exhibits our framework, highlighting the key concepts and their interrelationships behind MNE management of digital risks. We construct this framework based on the information-processing theory, which establishes that organizations can be seen as information-processing systems that must deal with work-related uncertainty (Egelhoff, 1982; Tushman & Nadler, 1978), with information technologies among the essential capabilities necessary to curb this uncertainty (Daft, 1992). As detailed below, we make several major points: first, digital threats increase operational complexity, and thus information-processing demands. Second, MNEs vary in their exposure to digital risks due to their firm-specific dynamics and consequently vary in information processing requirements, with those with higher levels of information and data intensity, geographic diversity, and global platform participation being particularly vulnerable. Third, MNEs will manage such requirements by instituting and accentuating information-processing capabilities or mechanisms, such as risk analytics, digital intelligence, risk control, and collective actions. Lastly, success in managing digital hazards requires not only a fit between information processing requirements and information processing capabilities but also between the type of digital

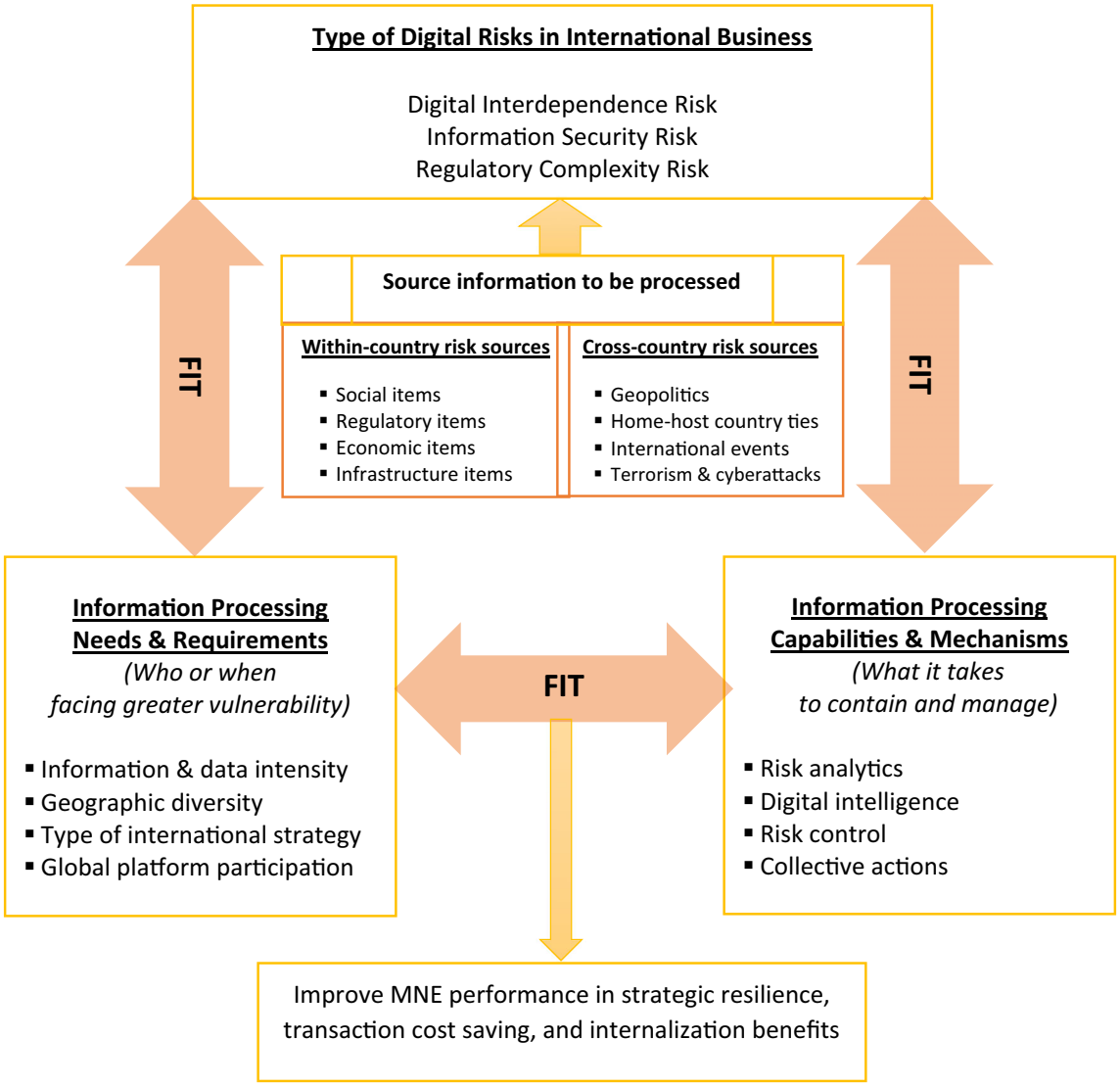

Figure 1 An information-processing framework of IB digital risks.

risks and the corresponding information-processing needs and capabilities. This fit carries strong efficiency and cost implications, as MNEs differ in their dependence on and sensitivity to varying digitization disruptions that affect global operations. The information-processing theory shares with the transaction cost economics line of thought in the importance of cost saving in information processing, but more notably, it sheds light on the information-processing mechanisms and capabilities furnished by organizational design.

According to the information-processing theory, complexity and uncertainty in performing cross-unit operations or duties derive from such sources as task complexity, task interdependence between subunits, and task environment dynamism (Tushman & Nadler, 1978). These three sources combine to influence the degree of work-related uncertainty or complexity faced by the firm. As the ambiguity or intricacy increases, so does the need for processing higher levels or more types of information (Egelhoff, 1991). In a digital setting, task complexity is likely to rise when the MNE's information and data intensity increases. Likewise, task interdependence may intensify when the MNE more actively participates in global platforms or adopts a more globally integrated strategy (as opposed to multi-domestic). Meanwhile, environmental dynamism becomes amplified when the firm expands its geographic diversity, whether in terms of global supply chain or foreign market expansion (Kano, Tsang, & Yeung, 2020). For these

reasons, we emphasize information and data intensity, geographic diversity, type of international strategy, and global platform participation as the critical determinants of information-processing demands for digitally connected activities, and accordingly as contributing factors of firm-specific exposure and digital risk vulnerabilities.

Information and Data Intensity

MNEs diverge in their information and data intensity: that is, some firms rely more than others on information and data flows that connect with either internal members or external players. Executives establish a digital architecture to work with global suppliers, connect to worldwide customers, virtually cooperate with global teams, and enable internal communication and data sharing for a global workforce. This architecture consists of global enterprise resource planning (ERP), human capital management (HCM), customer relationship management (CRM), a data management platform (DMP), cloud computing, and a social marketing platform, among other features to manage worldwide resources and relationships. However, these systems are more essential and pivotal to some firms (e.g., IBM) than to others (e.g., Disney). While distance, space, and time-related governance issues may decrease in importance due to digital connectivity (Monaghan, Tippmann, & Coviello, 2020), organizing and monitoring costs associated with connectivity will increase (Luo, 2021; Rangan & Sengul, 2009).

The information-processing theory holds that the requirements for processing information are greater if a firm is more prone to information breaches and external shocks (Egelhoff, 1991). Thus, firms with higher information and data intensity are likely more susceptible to *cyber security risk* and *regulatory risk*. In the current geopolitical environment, ICT has become a battlefield for new techno-nationalism. Several countries, especially technological powerhouses, vie for ICT technologies and standards to accentuate their economic dominance and market power (Sacks, 2020). As ICT becomes a foundational infrastructure in the digital age, many MNEs' global value chain activities are obstructed by cross-country regulatory differences and even tensions in ICT spheres (UNCTAD, 2015). Since digital infrastructure (e.g., automated processes, strong AI-supported algorithms, and cloud computing) plays a significant role in a company's global supply chain and production network, MNE leaders often find it difficult to relocate from one country to another (Adner & Kapoor, 2010; Bruno & Shin, 2014). In addition, as noted earlier, amid the growing trade tensions, governmental scrutiny of takeovers by foreign companies has increased, with a sharper focus on the implications for national security associated with digital technologies (McKinsey, 2020).

Geographic Diversity

We define geographic diversity as the extent to which an MNE has internationalized its businesses (from supply chain to market expansion) and globally diversified across regions and countries. A highly diversified MNE has an overarching geographical presence and a depth of business globalization. As this diversity increases, an MNE becomes more exposed to digital risks for several reasons. First, the MNE with higher diversity must deal with greater geographic coverage, in turn exposing itself to digital threats (physical and institutional) in more countries. Diversity intensifies an MNE's interdependence with foreign resources, regulators, competitors, partners, vendors, platforms, and other ecosystem players (Dellestrand & Kappen, 2012), leaving the firm to encounter accentuated interdependence risks, information security risks, and regulatory risks in various countries. In fact, the higher the diversity, the more information-processing nodes are involved (both intra- and cross-country items), and, as a result, the higher the digital risks that arise from both inter- and intra-organizational exchanges (Benito et al., 2019; Chinn et al., 2014; Stallkamp & Schotter, 2021).

Moreover, as diversity ascends, an MNE's leaders must cope with a growing complexity of global activities dispersed in various regions and countries. Coordination within the MNE system and with outside business stakeholders becomes more intricate (Benito et al., 2019). This complexity actually compels many executives to invest more to improve the organization's digital architecture (e.g., ERP, HCM, CRM, global talent bank, data management platform, together with cloud computing and data analytics) in the quest to manage digital risks. With continued global expansion, leaders of multinationals need to use digital technologies to better design a global value chain system, better serve global customers, and better manage other kinds of cross-border flows in an orchestrated manner (Buckley & Strange, 2015). This endeavor, however, can make the MNE more vulnerable to internet and intranet breakdowns,

information leakages, and poor digital infrastructures in multiple countries. Further, as diversity increases, the MNE experiences growing pressure to process both within-country (within individual target countries) and cross-country information for risk assessment. Cross-country risk items, notably global geopolitics, home-/host-country ties, and international events (COVID-19 pandemic in particular), more forcefully affect highly diversified companies. This discussion suggests that as geographic diversity increases, MNEs will undergo stronger information-processing requirements for digital risk management and become more exposed to *all three digital risks*.

International Strategy

Leaders of MNEs use three basic strategies to compete globally: multidomestic, global, and hybrid or transnational (Bartlett & Ghoshal, 1989). A multidomestic strategy, or local adaptation orientation, which focuses on competition within each country and emphasizes the segmentation of foreign markets by national boundaries, marks high local adaptation and responsiveness in respective countries where the MNE subunits compete. Strategic and operating decisions are decentralized to foreign subunits in order to custom-tailor products and services to local markets. For this reason, this strategy exposes the MNE to more within-country digital risks encompassing regulatory, infrastructural, economic, and social items, as previously explained. A multidomestic strategy also requires less intra-network communication, coordination, and integration (Bartlett & Ghoshal, 1989) and thus lowers the demand for intra-MNE digitization interdependence and interconnection.

A global strategy assumes more standardization of products across national markets. Foreign subunits are presumed interdependent, with headquarters focused on attaining integration between them (Prahalad & Doz, 1987). This strategy leverages a global economy of scale and opportunities to use innovations developed at home. SAP Business One, an integrated ERP solution for global businesses and their foreign subsidiaries and suppliers worldwide, represents an example of a specific digital architecture implementing this strategy. The application's flexible and scalable core solution supports expansion and allows for future growth and innovation. This architecture offers a single code base to meet legal and language requirements of countries around the world. In addition, all business functions come in one package, which makes them easy to set up, optimize, and use. Integration with other systems is simple and possible via certified standard integration packages or open application programming interfaces. This kind of architecture helps under the global strategy, or higher global integration orientation, since the MNE faces more cross-country risk forces, such as home- and host-country trade ties and geopolitics that affect digital globalization.

A transnational strategy sits between the multidomestic and global ones (Prahalad & Doz, 1987). This hybrid strategy seeks to achieve both global efficiency and local responsiveness and requires a shared vision and individual commitment through an integrated yet flexible organizational network (Baaij & Slangen, 2013). MNE leaders adopting this strategy aim to fulfill two purposes: stimulating intra-firm communication to avoid conflicts between integration and localization, and increasing flexibility and discretion to foreign subunits. Firms using the hybrid strategy must transfer distinctive competencies within the network, while heeding pressures for local responsiveness (Bartlett & Ghoshal, 1989). These dual mandates cement the information-processing demands in a way that forces the digitization design to satisfy variances and contingencies, in which foreign subunits must be sufficiently differentiated to confront diverse demands, markets, and policy environments (Sturgeon, 2020). Competence building and global learning do not reside in the home country alone, but can develop in any of the MNE's worldwide operations. Consequently, MNEs maintain the flow of skills and information in a multidirectional fashion (i.e., from any unit to others), but the flexibility increases exposure to all digitalization threats previously identified. For example, risks of interdependence with global ecosystems will be higher when the multinational seeks local adaptation and differentiation, and, meanwhile, risks of interdependence with corporate members will be higher when it pursues global integration and standardization. Therefore, we envision that MNEs adopting the transnational strategy will be more exposed to the three types of digital dangers than those adopting either the global or the multidomestic strategy.

Global Ecosystems

Today, few MNEs or industries stand immune to the influence of digital global platforms and ecosystems (Li, Chen, Yi, Mao, & Liao, 2019; Nambisan et al., 2019; Stallkamp & Schotter,

2021). The unabated digitization that has occurred in many countries and industries imply that companies must view their offerings not just as standalone entities but as part of a broader, connected system. Moreover, these offerings increasingly comprise digital assets that can be easily transported across national and organizational boundaries, and changed and recombined to cater to the needs of a particular foreign market (Boudreau, 2010; Nambisan et al., 2017). Meanwhile, data lie at the core of an MNE's digital platform and ecosystem strategy. When a platform has global reach, one assumes that data can be moved around national borders, but this assumption becomes increasingly questioned as governments in almost all parts of the world impose certain restrictions on how, when, or to what extent companies can transfer data across their borders (World Bank, 2016). Such evidence shows the duality of both rewards and risks behind global platforms and ecosystems.

MNEs that depend more on global platforms and ecosystems are expected to face greater needs for information processing. Firms that participate in more diverse and intricate ecosystems may confront larger digital risks. To start, these firms will encounter higher interdependence risks and contagion effects within the ecosystem. In a cross-cultural and cross-border setting, finding common ground and common values between an MNE and its partners may become more difficult (Bock, Opsahl, George, & Gann, 2011; Kano, 2018). For example, disparities in information-processing-related policies between a company's home country and foreign ecosystem members may present a critical challenge when attempting to engage with partners in digital innovation. When the "who owns what" question cannot be clearly answered, leaders of firms could feel the need to narrow their areas of direct engagement due to higher than expected digital risks.

Secondly, conflicts and coordination prove difficult to manage within global ecosystems, which tend to be loosely coupled (Nambisan et al., 2019). This reality prompts challenges for members, individually or collectively, in controlling digital risks. When cross-border differences in digitization environments are small, top managers may have the possibility to adopt more direct coordination practices. However, substantial differences may lead managers to wall-off their decision-making process and rely more on enhancing the visibility of partner activities rather than coordinating them. In addition, firms more dependent on ecosystems are subject to higher infrastructural and institutional threats related to digitization. Engagement with broadened platforms demands a common set of rules and policies to minimize the possibility for one partner to derive undue advantage and lower the overall uncertainty in collaborative activities. Because of these reasons, we postulate that MNEs actively participating in more diverse and complex global platforms and ecosystems will be more exposed to the three digital risks.

MANAGING DIGITAL RISKS

Managing the threats from digital connectivity demands information-processing capabilities. The information-processing theory holds that the effectiveness of governing operations performed by various subunits in different locations lies in the match between the information-processing needs and information-processing capabilities of the firm, manifested in information technologies and diligence as well as risk control mechanisms (Tushman & Nadler, 1978). Egelhoff (1991) documents that this match has significant implications for MNEs and that headquarters' organizational monitoring and control forms a critical component of the information-processing capabilities. As we elaborate below, risk analytics, digital intelligence, risk control, and collective actions are among the key information-processing capabilities required for managing digital risks.

Risk Analytics

Risk analytics involves a set of qualitative and quantitative techniques used to identify and assess sources or factors that may jeopardize the success of digital activities. The analysis also helps to define preventive measures to reduce the probability of these factors from occurring, as well as to identify countermeasures to deal with these constraints. The information-processing theory integrates concepts of uncertainty and risks with information-processing mechanisms to assess the congruence between what is required for information processing and the firm's preparedness to satisfy this requirement (Tushman & Nadler, 1978). Risk analytics produces intelligence to help achieve the equivalence.

Qualitative approaches use a substantial amount of expert insight, judgmental inputs, and subjective analysis. Executives from headquarters may dispatch a team of specialists (such as from IT, global

supply chain, intellectual property rights, marketing, or other) to work together with foreign subsidiary specialists to identify and analyze the digitization risk environment and offer potential solutions. MNE leaders can also evaluate risks through due diligence coordinated by a headquarters team composed of experts from related functions and areas (e.g., internal control, ICT, global planning, crisis management, and supply chain).

Through quantitative analytics, digital threats can be tabulated and analyzed by integrated computer simulation, modeling, machine learning, data automation, complexity analytics, and AI, among others. Under this approach, management employs or creates sophisticated tools to monitor and analyze behavior and activities in real time and for globally dispersed activities inside and outside of the company. For instance, AI-based analytics platforms can manage global supply chain risks by integrating varied information about suppliers, from their geographical and geopolitical environments to their financial risk, sustainability, and corporate social responsibility scores (Chinn et al., 2014). Similarly, AI systems can detect, monitor, and repel cyber attacks by identifying software with certain distinguishing features – for example, a tendency to consume a large amount of processing power or transmit a large quantity of data – and then closing down the attack. In the global finance sector, machine learning has successfully detected credit card fraud for multinational banks (Chinn et al., 2014).[7]

While both qualitative and quantitative analytics are needed in dealing with all digitization threats, we assume that the qualitative approach becomes more important to address digital regulatory risk. Many governments have neither afforded a restriction-free open internet policy nor adequately protected the privacy of internet users, becoming a critical impediment to the value of digital connections (Potrafke, 2015; World Bank, 2016). Probing such institutional risks depends heavily on due diligence, on-the-field intelligence, and seasoned expert input. In comparison, quantitative analytics seems more relevant for evaluating cyber security and interdependence risks. Global internet breaches can disable a system infrastructure or pilfer confidential information, such as customer credit card numbers, social security numbers, and business transactions (Gregory, Henfridsson, Kaganer, & Kyriakou, 2020). Quantitative analytics like data science and AI-based risk stimulation can help deeply diagnose the causes and effects of digital dependence risk (Chinn et al., 2014).

Digital Intelligence

Managing digital risks requires not only investment in digital technologies (e.g., bolster information security) but also sharpening corporate digital intelligence in identifying, containing, controlling, and neutralizing these risks. We define *digital intelligence* as the ability to capture opportunities, appropriate values, and alleviate risks through digital tools. More than just the ability to use digital technologies (e.g., social, mobile, analytics, cloud, and cyber security) and risk analytics noted above, this form of intelligence addresses the what, why, where, when, who, how, and how much of digital technology to improve operational efficiency, identify risk roots, and help design viable solutions to mitigate digital hazards. Digital intelligence transcends connectivity technologies into valuable information, real-time forecasts, and inter-firm and intra-firm sharing improvement, which in turn significantly helps managers make critical business decisions.

Digital intelligence goes beyond risk analytics teams. Instead, individual employees, subunits, leadership, and the organization as a whole need to possess this form of intelligence (Luo, 2021). Research suggests that a strong organizational commitment to digital intelligence, including by leadership, must exist to minimize the MNE's global exposure to digital dangers and to handle these hazards (Yoo, Boland, Lyytinen, & Majchrzak, 2012). A firm that develops its own digital intelligence among its worldwide units can more easily address digitization-enabled opportunities and threats. This intelligence supports the management of resource interdependence with other firms, the safeguarding of information security, the identification of new global rivals, and the assessment of institutional risks in both target country and elsewhere (Rangan & Sengul, 2009). Further, connectivity intelligence involves an MNE's organizational capability in nurturing cross-border, inter-unit collaboration, thus curtailing structural inertia and bureaucratic hurdles that could counteract risk management and bolster network-based or ecosystem-specific advantages derived from global partnerships (Boudreau, 2010; Breton-Miller & Miller, 2015). Finally, digital intelligence is imperative to curbing third-party risks, those associated with outsourcing to third-party vendors or service providers (Boudreau, 2010). Some reports hold that

this intelligence helps reduce an MNE's vulnerabilities related to intellectual property, data, operations, finances, customer information, or other sensitive information (Bruno & Shin, 2014).

Based on the information-processing theory, we suggest that MNEs that properly align digitization intelligence with the corporate elements exposed to digital risks perform better in global competition than those poorly aligning the two. Digital intelligence stands as an important enabler for organizational resilience, risk and crisis management, and strategic responses to uncertainties and adversities (Banalieva & Dhanaraj, 2019; Jean, Sinkovics, & Cavusgil, 2010). This acuteness helps the firm withstand or rapidly recover from operational disruptions (including digital disruptions) or hardships that significantly impede its core businesses and global operations. Evidence shows that digital intelligence allows the MNE to more easily identify the alternatives, build responding processes and guidelines (e.g., business continuity planning), and prepare just-in-case scenarios (McKinsey, 2020). For instance, a digital intelligence structure strengthens the multinational's sensitivity to emerging threats and underpins its swift mobilization of global resources in the face of global uncertainty (Chinn et al.).[8]

Risk Control

We define risk control as the set of methods by which firm leaders take action to maintain control over third parties so as to reduce or eliminate potential digital risks. Risk exposure will be contained if the firm exercises greater control of vulnerable activities conducted by parties outside the MNE (Breton-Miller & Miller, 2015). These third parties are not only located in numerous countries but also vary in type, including global suppliers, distributors, open-source platforms, technology vendors, industry designers, or R&D co-developers. Mainly, the firm must achieve the right level of governance, both initially and perpetually, around such areas as security, business continuity, and data. Also, MNE leaders need to reassess risk issues over time, such as whether or not the firm should depend on a single cloud provider, outsourcing a critical part of the customer journey to a single third party, or automation of core processes.

A number of MNEs (e.g., IBM, Cisco, and SAP) have already built global risk squads: cross-functional and cross-border teams formed from a variety of different disciplines and business units responsible for advancing risk control over external players. The importance of such exposure-risk control has been validated in corporate finance (Bruno & Shin, 2014; Hazlehurst & Brouthers, 2019). McKinsey (2020) reports that multinationals that are competent in exercising control over foreign suppliers and vendors with greater precision and efficiency enabled by digital intelligence perform significantly better than their global competitors.

Collective Actions

Addressing digital risks necessitates collective actions by MNEs and other organizations that share interests in dealing with the common threats, such as digital regulatory complexity risk and cyber security risk. Improving physical and institutional digital infrastructure rests on the shoulders of both governments and private sectors (including MNEs), as well as other players such as international economic organizations and industrial associations (Chen, Shaheer, & Li, 2019; UNCTAD, 2015). Hence, the nature of digital risks compels cross-country, cross-border cooperation. Individual governments need to foster contributions by and collaboration with private sectors, including those from foreign countries, promoting a sustainable, pro-business digital infrastructure within which the private sector can flourish. Governments should also set clearer rules around online content, election integrity, privacy, and data portability, as well as create a pro-competition and transparent policy setting that helps drive investment and innovation in digital infrastructure and activities (World Bank, 2016). Creative solutions, like co-investment via public–private partnerships, should be facilitated for this purpose. In fact, governments themselves need to innovate their own digital infrastructure, shifting more administrative and public services to online and mobile phones. Research shows that digital connectivity offers noticeable advantages in terms of administrative efficiency, resilience, and ubiquity of access for all citizens (Friedman, 2007; Sacks, 2020).

MNEs themselves undoubtedly act as critical players for improving digital technologies in their role as digital enablers. Firms also serve to link foreign economies with the outside world through various activities. One form includes working with host-country governments on digital openness for more efficient flows of production factors within their globally coordinated networks, in turn better leveraging a host-country's comparative advantages (Sacks, 2020). MNEs can also work with each other

to meet market demands for digital products and services. Moreover, improving institutional infrastructure for digitization strongly depends on the country's development in science, education, and innovation, areas in which MNEs may actively help, such as through investment in scientific research and human capital development (EIU, 2014). Also, executives of multinationals can, and should, work together with host-country governments to encourage, support, and safeguard intellectual property rights to encourage enterprises to make large outlays in digital technology R&D activities.[9] As new digitization-related industries or services emerge, MNEs can help host-country governments establish technical and quality standards for the focal industries and related or supporting industries.

A digital environment (both technological and institutional) is still evolving in virtually all economies, meaning that it is not yet exogenous to international business. This trait opens opportunities for MNEs to reshape both institutional and physical attributes of digital environments, through their technological contributions and policy influences, in a way that nurtures the growth of all businesses, as suggested by UNCTAD (2015). Also, the above collective actions help to harmonize some essential standards for digital globalization (e.g., technology norms like 5G, taxation code for digital platforms, information protection protocols), thus easing information processing in dealing with regulatory and technological incompatibilities in different countries and stimulating the long-term growth of MNEs. Lastly, multinational firms are stakeholders in wider industrial, economic, and social systems. Solutions that solve for an individual company at the expense of or neglecting the interests of others will create mistrust and damage the business in the longer term (Turkina & Van Assche, 2018; Verbeke & Greidanus, 2009). Conversely, support to customers, partners, and societal systems in a time of drastic disruptions can potentially create lasting goodwill and trust. A key element of dealing with economic stress is to live our values precisely when we are most likely to forget them.

The fit between the information-processing capabilities explained above (risk analytics, digital intelligence, risk control, and collective actions) and the information-processing requirements discussed earlier has performance consequences. Indeed, the information-processing theory holds that this fit bears performance implications (Tushman & Nadler, 1978). MNEs can be more resilient to environmental disruptions when they are equipped with information-processing capabilities that meet the demands of information-processing requirements (Williams, Gruber, Sutcliffe, Shepherd, & Zhao, 2017). In the digital globalization context, matching needs with capabilities can result in improvement in strategic resilience, transaction cost saving, and internationalization advantages. The aptitude helps firm leaders reach an optimized balance between where they need to invest and what they may achieve, or between where risk exposures occur and how to curtail them. Egelhoff (1991) suggests, too, that the fit boosts transaction cost saving because it optimizes *needed* investment for information processing that is scalable and transferable across countries in which the MNE operates. Similarly, Rugman and Verbeke (2003) document that the capability to develop optimal internal coordination and control mechanisms, taking into account cost and benefit congruence, is an essential, firm-specific competence leading to internalization advantages. Such optimal coordination and congruence arise when the above fit occurs. Table 1 highlights firm variance in risk exposure and risk management as well as performance implications, all anchored in the information-processing logic.

DISCUSSION

Digitization symbolizes the fourth industrial revolution. While digital connectivity may vary across countries, industries, and businesses, and may change due to disruptions in global geopolitics, public health crises, and world economy slowdowns, engagement in this form of network connections unquestionably continues and even strengthens. MNEs are both enablers and beneficiaries of such connectivity, changing the essence of international business. To a large extent, digital connections are country (or location) agnostic since they can be made available (and used) across national boundaries with lower costs incurred than through traditional IB connections (Friedman, 2007; Grossman & Helpman, 2015). This quality allows companies to market their digitally-enabled products and services globally with ease. Further, digital technologies and intelligence are generative, or easily modified and combined with other technologies – by companies other than those that created them in the first place – to deliver newer sets of capabilities (Jacobides, Cennamo, & Gawer,

Table 1 Managing digital risks in IB: configurations and propositions

Information processing logic	Exposure to digital risks (information-processing requirements)
Task characteristics such as information intensity determines information-processing needs	A: MNEs with higher *information and data intensity* will be exposed more to digital risks, especially cyber security risk and regulatory complexity risk B: MNEs with higher information and data intensity will more strongly need to decipher intra- and cross-country risk items
Task complexity and uncertainty determines information-processing demands	A: MNEs with higher *geographic diversity* will be exposed more to digital risks, including interdependence risk, cyber security risk, and regulatory complexity risk B: MNEs with higher *geographic diversity* will more strongly need to diagnose intra- and cross-country risk items
Task interdependence among subunits and adaptation pressure heighten information-processing requirements	A: MNEs adopting *transnational strategy* will be exposed more to all three digital risks than those adopting multi-domestic or global strategy B: MNEs with higher *global integration* will more strongly need to assess cross-country risk items, while MNEs with higher local adaptation will more strongly need to assess within-country risk items
Task dependence on and connectivity with other firms accentuate information-processing needs	A: MNEs depending more on *global platforms and ecosystems* will be exposed more to digital risks, especially interdependence risk and cyber security risk B: MNEs depending more on *global platforms and ecosystems* will more strongly need to assess intra- and cross-country risk items
	Managing digital risks (information-processing capabilities)
Firms need to build information-processing capabilities to meet information-processing requirements	A: *Risk analytics, digital intelligence, risk control, and collective actions* are among the key information-processing capabilities needed to manage digital risks for international business B: These capabilities are deployed to assess, contain, and mitigate uncertainty, complexity, and risks associated with digital globalization
Information processing capabilities must fit with information-processing demands for organizing effectiveness	A: MNEs exposed more to institutional risk will need to focus more on *qualitative risk analytics* while those exposed more to information security risk and interdependence risk will focus more on *both quantitative and qualitative risk analytics* B: Improved *risk analytics* is essential to satisfy increased information-processing requirements, particularly those caused by information and data intensity, geographic diversity, and global platform participation
Information technologies and intelligence are among critical capabilities to process information	A: MNEs exposed more to interdependence risk and cyber security risk will more greatly need *digital intelligence* B: Improved *digital intelligence* is essential to satisfy increased information-processing requirements, heightened by information or data intensity, geographic diversity, transnational strategy, and global platform participation
The fit between information-processing needs and capabilities is an orchestrated effort, and control is a critical capability of this kind	A: MNEs exposed more to interdependence risk and cyber security risk will more greatly need control over third parties B: Improved risk control is essential to satisfy increased information-processing requirements, particularly those escalated by geographic diversity, transnational strategy, and global platform participation
Managing task and institutional environment complexity and uncertainty needs some joint actions by all members facing them	A: MNEs exposed more to regulatory complexity risk and interdependence risk will need more emphasis on collective actions by MNEs facing the same environment B: Improved collective actions are imperative to satisfy increased information-processing requirements, particularly those fortified by global platform participation and geographic diversity
The information-processing needs–capability fit fosters firm performance	The fit between information-processing requirements and information-processing capabilities and between digital risk types and these requirements or capabilities ameliorate MNE performance in organizational resilience, transaction cost reduction, and internalization advantages

2018; Nambisan et al., 2017). Such generativity, resulting from their openness and re-combinability, allows for rapidly refashioning the value proposition of products, services, and business models to fit both globalized and localized needs.

However, digital connectivity, as a new context for both established and emerging international firms, also presents enormous risks. While we recognize the proliferation of research addressing the benefits of digitization, we observe that the field remains largely silent on the dark side of this prevalent issue. Digital connectivity makes many firms more dependent on others, and thus subject to more contagion effects from all threats facing them and others. The impact of external shocks becomes magnified in a more digitally interconnected world, and ripple effects spread faster. For instance, digital connectivity makes global reputation maintenance and crisis management immensely critical, intricate, and sensitive. Contagion effects that jeopardize an MNE's worldwide reputation are multiplied through social media and other connectivity channels. In assessing the overall environment, many conclude that the future success of MNEs lies not in whether they invest, adopt, and participate in digital connectivity but in *how* they harness digitization-enabled new opportunities while circumventing digitization-cased new risks associated with global operations (Potrafke, 2015; Rangan & Sengul, 2009; World Bank, 2016).

We enrich research on IB risks in several ways. To start with, we illustrate new forms of digital dangers in international business. This contribution may broaden our understanding of IB risks and affords a fuller picture of both rewards and risks of digital globalization. We reveal that digital threats occur in multiple forms, including as interdependence risk, information security risk, and regulatory complexity risk. Underlying these challenges are geopolitical, economic, technological, sociocultural, and legal forces that jointly come into play in not just an individual target country (national level) but across countries (supranational level). We show how MNE executives can examine within-country risk items specific to a foreign target country (e.g., regulatory, social, economic, and infrastructural items), as well as cross-country risk items that are effectuated across countries (e.g., global geopolitics, home-/host-country relations, international events, and terrorism and cyber attacks).

We offer an information-processing framework toward digital risks. The information-processing theory describes organizations as information-processing systems whose basic function is to create the most appropriate configuration of work units (as well as the linkages between these units) to facilitate the effective collection, processing, and distribution of information (Tushman & Nadler, 1978). We apply this theory to stress the importance of aligning, or creating a fit between, information-processing requirements deriving from digital risk exposure and the information-processing capabilities through which to manage these risks. Meanwhile, we extend this theory by emphasizing two other fits: between digital risk type and information-processing needs, and between digital risk type and information-processing mechanisms. This notion of fit is in accordance with not only the transaction cost logic (minimizing information-processing cost) but also the internalization logic (improved monitoring of interconnected tasks exposed to digital risks). It follows that these fits or alignments may have strong performance implications for organizational resilience, transaction cost saving, and internalization advantages, which concurs with the dominant logic of internalization theory (e.g., Rugman & Verbeke, 2003). While these points remain in need of empirical validation, the information-processing theory assumes that organizing and governing various subunits will become more effective, and make the MNE more resilient when information-processing needs match information-processing capabilities in a complex and risky environment.

We depict this theory as a proper guide as it allows us to specify MNEs that vary in their international strategies and in their exposure to risks. Firm-specific traits, such as information intensity, geographic diversity, international strategy, and platform participation, significantly shape the firm's susceptibility to digital risks. Demystifying risk types also permits us to look at configurations between these global traits and specific threats. For instance, we suggest that, when geographic diversity increases, information security risk and regulatory complexity risk are amplified. In the context of platform technology, the nature of, or the way of participating in and interacting with, global platforms and ecosystems carries disparate risk implications. MNEs depending more on global platforms and ecosystems are more exposed to digital risks. If such platforms and ecosystems carry more diversity in cultural backgrounds, strategic objectives, global experiences, and collaboration history, this risk exposure becomes further aggravated. Also, we point out that MNEs with higher

flexibility in their own global supply and production systems will rely less on ecosystems, hence be less exposed to digital hazards, notably, interdependence risk and cyber security risk.

In addition, we consider actions that MNE leaders need to take, detailing risk assessment and risk management approaches. We offer a set of actions relating to risk analytics, digital intelligence, risk control, and collective actions essential for managing digital risks. Importantly, digital intelligence transforms digital technologies into valuable information, real-time forecasts, operational decision-making, and inter-firm and intra-firm sharing, which in turn significantly help to streamline global operations without taking undue risks. To contain threats from connectivity, MNEs must be able to exert control over third parties in key functions or businesses that are vulnerable to these risks, calling for further actions to build global risk squads comprised of cross-functional and cross-border team members responsible for managing both the technical and managerial aspects of the stated risks. We advocate for collective actions – working together with other MNEs and local firms and with home- and host-country governments – to ameliorate digital infrastructure (physical and institutional) challenges and boost business continuity and country competitiveness. The logic of cooperation between MNEs and governments (e.g., Luo, 2001) applies well to the improvement of the digital globalization environment.

Finally, we point out the importance of congruence between digital risks, firm exposure, and risk management capabilities. As explained, MNEs vary in their exposure to these risks but also vary in the ability to manage them. Some MNEs can endure more digital risks as long as they are equipped with technological and organizational competencies that are sufficient to suppress the risks. We argue that MNEs with better alignment of the digital risks that they face with both information-processing requirements (e.g., information intensity, geographic diversity, and type of international strategy) and information-processing capabilities (e.g., digital intelligence, risk analytics, and risk control) can perform better in strategic resilience, transaction cost saving, and internalization advantages.

FUTURE RESEARCH

Over the past decades, digital globalization has spawned research on the competitive advantages of digital connectivity. However, in combination with other credible threats, such as new geopolitics, deglobalization sentiment, public health crises, and global supply chain breakdowns, digital risks are on the perpetual rise. IB research has not yet adequately attended to this reality. We view the dangers arising from digital connections as a new, yet increasingly critical, type of IB risk, and offer our suggestions for future research, which in part addresses this study's limitations.

First, we submit a logic of alignment between digital risk processing and digital risk managing capabilities. Yet, another important alignment exists: the fit between digitization *opportunities* and risks. In general, executives may be willing to take more digital risks if they foresee more opportunities or more gains from digital globalization pursuits, a typical risk–return positivity assumption (Bowman, 1980; Miller, 1998). The prospect theory adds additional insights by including firm-specific reference dependence (Kahneman & Tversky, 1979). That is, faced with a risky choice leading to gains, parties are risk-averse, preferring solutions that lead to a lower expected utility but with a higher certainty (concave value function). However, when faced with a risky choice leading to losses, they are risk-seeking, preferring solutions that lead to a lower expected utility as long as it has the potential to avoid losses (convex value function). In particular, executives may underestimate merely probable outcomes in comparison to assured outcomes. Per this theory, parties attribute excessive weight to events with low probability and insufficient weight to events with high probability. Leaders of MNEs that are newer or less experienced in digital globalization seem to have a higher propensity to follow this risk attitude or preference. Future research that specifies the opportunity–risk alignment would need to consider this prospect logic along with firm-specific digital intelligence, experience, and risk-managing capabilities in dealing with both general/global and country-specific digital risks and disruptions.

Second, an MNE's digital risk managing system is composed of not only corporate or regional headquarters which orchestrates the system to execute the digital strategies but also foreign subsidiaries, scattered in various countries where digitization infrastructures vastly diverge. These subsidiaries are the main entities actually exposed to both the within-country and cross-country risk items noted above. They are also situated in key nodes of intra-MNE and inter-MNE boundaries spanning global operations (Song & Shin, 2008; Turkina & Van

Assche, 2018), thus holding a central and frontier position in dealing with the identified risks. As future research embraces people and processes in analyzing digital global connectivity, these subsidiary roles warrant attention in their co-designing, executing, and revamping of an MNE's digital architecture that is both globally synchronized (to ensure global compliance and control) and locally differentiated (to nourish national adaptation). Another valuable quest lies in unifying the literature of parent–subsidiary links with digitization risk management. This literature speaks clearly of varying strategic roles played by various subsidiaries in cross-border knowledge flows, innovation contribution, resource deployment, and global integration (e.g., Birkinshaw, Morrison, & Hulland, 1995; Kogut & Zander, 1993). Many such activities are undertaken digitally, thus widely exposed to digital risks. What it takes to motivate subsidiaries to contribute to the MNE's total solution to the balancing act between digital connectivity opportunities and digital risk mitigation merits further exploration.

Third, our framework does not specify how MNEs should improve their organizational design (e.g., structure, power delegation) to satisfy the fit between information-processing requirements and information-processing capabilities. This match calls for structural or behavioral support or adjustment, allowing the corresponding requirements and capabilities to create more sustained values for the organization (Daft, 1992). Future research should proceed further from our framework to examine how an MNE's organizational design evolves in the digital era to achieve the needed fit. That is, future research needs to consider this alignment as one of the key drivers or guides for organizational change and evolutions.

Lastly, as global environments become more uncertain, disrupted, and contentious (Sacks, 2020), MNE leaders face increasing pressure to simultaneously satisfy competing ends and balance incompatible and even contradictory forces, compelling them to be more ambidextrous in multiple fashions (Gibson & Birkinshaw, 2004). Managing digital risks also demands such ambidexterity. We have already alluded to an MNE's need to balance global compliance and local differentiation, as well as digitally-enabled opportunities and involved risks. Yet, required ambidexterity in this setting also extends to flexibility and efficiency, collaboration and control, and stability and adaptability, in addition to open innovation and intellectual (including digital know-how) protection. In fact, we envision that an MNE's digitization architecture itself (digital technologies, intelligence, and processes) creates an important internal platform that fosters the firm's ambidexterity. Unlike other organizational control architectures, the digital one affords more discretion to front-line units (thus flexibility) while easing orchestration (thus efficiency), and endows more complementarity of internal and external resources through ecosystem sharing (Li et al., 2019; Nambisan et al., 2019). More research is merited to delve into how digitization architecture works in nurturing an MNE's cross-border, boundary spanning activities within an organization, between organizations, and between the organization and environments, in turn bolstering its strategic resilience.

CONCLUSION

Digital global connectivity embodies a dominant feature of the new era of international business and acts as a critical catalyst to address rising uncertainties. However, digitization itself carries a myriad of risks, a pivotal issue for global operations, and yet one that has received little attention, theoretically or empirically. Managing risks constitutes one of the central issues in international business, but has long been based on assumptions of tangible, often heavy barriers involved with flows of physical goods, services, investments, and capital, rather than intangible, dwindled barriers associated with instant flows of ideas, data, and knowledge. Nested within the information-processing logic, this article presents a general framework that describes types of digital risks in IB, explains within-country and cross-country items that drive these risks, and specifies divergence of MNEs in levels of exposure to the threats, since they differ in their dependence on and susceptibility to digitization disruptions that affect global activities. Following this reasoning, we propose that an MNE's information intensity, geographic diversity, choice of international strategy, and flexibility of ecosystem participation bear strong repercussions on its risk exposure and risk management. Finally, this framework offers a unique view toward essential actions needed by MNEs, individually and collectively, to circumvent digital risks, emphasizing the importance and process of building, deploying, and harnessing digital intelligence in the simultaneous pursuit of local adaptation, transnational resilience,

and global orchestration for cross-border activities that prevalently become digitally underpinned.

ACKNOWLEDGEMENTS

The author appreciates Professor Alain Verbeke and the three anonymous reviewers for providing insightful comments and excellent suggestions.

NOTES

[1]Other less primary connectivity-related risks may exist. For instance, global reputation risk could be amplified due to digitization. Contagion effects that jeopardize the MNE's worldwide reputation due to corporate or executive wrongdoing multiply through social media. In a digitally connected world, even menial misconducts, if repeated, can lead to a downfall. The demise of a few can engulf a whole industry when the transactions are based on trust in the fulfilment of future promises.

[2]The globalization of financial systems and the acceleration of information transmission have increased the risk of financial crises, as a crisis in one country can spread to others and lead to worldwide urgency. The US-China trade war makes such interdependence risks even greater. Global supply chain redesigning and relocation become more costly and cumbersome for both US companies (who have a significant portion of their supply chain in China) and Chinese firms (who depend on many US-based, high-tech components such as chips).

[3]A study reported by *Fortune* (January 23, 2015) estimates that cyber crime costs the global economy some $400 billion in annual losses, which can include consumer data breaches, financial crimes, market manipulation, and theft of intellectual property.

[4]The institutional environment for digital global connectivity is comprised of numerous players aside from national governments. Some supranational agencies (e.g., International Telecommunication Union) are also key players, affecting the digital infrastructure of MNEs.

[5]Many multinationals suffer from this system discrepancy as the US government imposes bans on the sale of semiconductors to Chinese telecoms and on American companies using Chinese-made equipment in critical networks. Several US allies, including Australia, Canada, and Japan, have followed suit, blocking local firms from using Huawei's technology in the development of their country's 5G network.

[6]After Brexit, for instance, companies in the United Kingdom may pay more in complying with the European Union's General Data Protection Regulation, while EU companies face higher cross-border taxation and administrative burden in the UK when conducting digital commerce.

[7]These big banks use systems that have been programmed on historical payments data to monitor potentially fraudulent activity and block suspicious transactions. Financial institutions also use automated systems to monitor their traders by linking trading information with other behavioral information, such as e-mail traffic, calendar items, office building check-in and check-out times, and even telephone calls.

[8]For example, Johnson & Johnson's digital intelligence has played a critical role during the Covid-19 health crisis. J&J uses product flow visualization and risk analysis tools to get foreign supplies to its manufacturing plants through alternative paths. The company also uses simulation tools to increase manufacturing capacity, smart glass technology to help quality experts work remotely, global collaboration tools to use real-time data for researchers working on a vaccine, and digital interactions to enable healthcare professionals around the world.

[9]IBM has long done so in China, for example. The IBM Research China Center has emphasized innovation in the areas of cognitive credit risk analysis, cognitive compliance, and blockchain services and solutions. The activity not only helps China's FinTech (i.e., financial services fueled by new technologies in blockchain, cognitive computing, mobile, and cloud) but also assists in transforming financial services around the world.

REFERENCES

Adner, R., & Kapoor, R. 2010. Value creation in innovation ecosystems: How the structure of technological interdependence affects firm performance in new technology generations. *Strategic Management Journal,* 31(3): 306–333.

Baaij, M. G., & Slangen, A. H. 2013. The role of headquarters-subsidiary geographic distance in strategic decisions by spatially disaggregated headquarters. *Journal of International Business Studies,* 44(9): 941–952.

Banalieva, E., & Dhanaraj, C. 2019. Internalization theory for the digital economy. *Journal of International Business Studies,* 50(8): 1372–1387.
Bartlett, C. A., & Ghoshal, S. 1989. *Managing across borders*. Boston, MA: Harvard Business School Press.
Benito, G., Petersen, B., & Welch, L. 2019. The global value chain and internalization theory. *Journal of International Business Studies,* 50: 1414–1423.
Birkinshaw, J., Morrison, A., & Hulland, J. 1995. Structural and competitive determinants of a global integration strategy. *Strategic Management Journal,* 16: 637–655.
Bock, A. J., Opsahl, T., George, G., & Gann, D. M. 2011. The effects of culture and structure on strategic flexibility during business model innovation. *Journal of Management Studies,* 49(2): 279–305.
Boudreau, K. 2010. Open platform strategies and innovation: Granting access vs. devolving control. *Management Science,* 56(10): 1849–1872.
Bowman, E. H. 1980. A risk-return paradox for strategic management. *Sloan Management Review ,* 1980: 17–31.
Breton-Miller, I., & Miller, D. 2015. The paradox of resource vulnerability: Considerations for organizational curatorship. *Strategic Management Journal,* 36(3): 397–415.
Bruno, V., & Shin, H. 2014. Globalization of corporate risk taking. *Journal of International Business Studies,* 45: 800–820.
Buckley, P., & Strange, R. 2015. The governance of the global factory: Location and control of world economic activity. *Academy of Management Perspectives,* 29(2): 237–249.
Cantwell, J. A. 2009. Innovation and information technology in the MNE. In A. M. Rugman (Ed.), *The Oxford handbook of international business* (2 ed.). Oxford: Oxford University Press.
Chen, L., Shaheer, N., Yi, J., & Li, S. 2019. The international penetration of ibusiness firms: Network effects, liabilities of outsidership and country clout. *Journal of International Business Studies,* 50: 172–192.
Chinn, D., Kaplan, J. & Weinberg, A. 2014. *Risk and responsibility in a hyper-connected world: Implications for enterprises*. McKinsey & Company and the World Economic Forum, January, 2014.
Daft, R. 1992. *Organization theory and design*. St. Paul, MN: West Publishing.
Dellestrand, H., & Kappen, P. 2012. The effects of spatial and contextual factors on headquarters resource allocation to MNE subsidiaries. *Journal of International Business Studies,* 43(3): 219–243.
Egelhoff, W. G. 1982. Strategy and structure in multinational corporations: An information processing approach. *Administrative Science Quarterly,* 27(3): 435–458.
Egelhoff, W. G. 1991. Information processing theory and the multinational enterprise. *Journal of International Business Studies,* 22(3): 341–368.
EIU (Economist Intelligence Unit). 2014. *Networked manufacturing: The digital future*. April 2014.
Friedman, T. L. 2007. *The world is flat 3.0: A brief history of the twenty-first century*. Surrey: Picador.
Gibson, C. B., & Birkinshaw, J. 2004. The antecedents, consequences, and mediating role of organizational ambidexterity. *Academy of Management Journal,* 47: 209–226.
Gregory, R., Henfridsson, O., Kaganer, E., & Kyriakou, H. 2020. The role of artificial intelligence and data network effects for creating user value. *Academy of Management Review.*. https://doi.org/10.5465/amr.2019.0178.
Grossman, G., & Helpman, E. 2015. Globalization and growth. *American Economic Review,* 105(5): 100–104.
Hazlehurst, C., & Brouthers, K. D. 2019. IB and strategy research on "new" information and communication technologies: Guidance for future research. In R. Van Tulder, A. Verbeke, & L. Piscitello (Eds.), *International business in the information and digital age*London: Emerald.
Hennart, J. F. 2019. Digitalized service multinationals and international business theory. *Journal of International Business Studies,* 50: 1388–1400.
Jacobides, M. G., Cennamo, C., & Gawer, A. 2018. Towards a theory of ecosystems. *Strategic Management Journal,* 39(8): 2255–2276.
Jean, R.-J., Sinkovics, R., & Cavusgil, S. T. 2010. Enhancing international customer–supplier relationships through IT resources: A study of Taiwanese electronics suppliers. *Journal of International Business Studies,* 41: 1218–1239.
Kahneman, D., & Tversky, A. 1979. Prospect theory: An analysis of decision under risk. *Econometrica,* 47(2): 263–281.
Kano, L. 2018. Global value chain governance: A relational perspective. *Journal of International Business Studies,* 49: 684–705.
Kano, L., Tsang, E. W. K., & Yeung, H. W. 2020. Global value chains: A review of the multi-disciplinary literature. *Journal of International Business Studies,* 51: 577–622.
Kshetri, N. 2005. Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management,* 11(4): 541–562.
Kogut, B., & Zander, U. 1993. Knowledge of the firm and the evolutionary theory of the multinational corporation. *Journal of International Business Studies,* 24(4): 625–645.
Li, J., Chen, L., Yi, J., Mao, J., & Liao, J. 2019. Ecosystem-specific advantages in international digital commerce. *Journal of International Business Studies,* 50(9): 1448–1463.
Luo, Y. 2001. Toward a cooperative view of MNC-host government relations. Building blocks and performance implications. *Journal of International Business Studies,* 32: 401–419.
Luo, Y. 2021. New OLI advantages in digital globalization. *International Business Review,* 30(2): 101797.
Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K., & Dhringra, D. 2016. *Digital globalization: The new era of global flows*. McKinsey Global Institute.
McKinsey 2020. *Risk, resilience, and rebalancing in global value chains*. New York: McKinsey Global Institute.
Miller, K. D. 1992. A framework for integrated risk management in international business. *Journal of International Business Studies,* 23(2): 311–331.
Miller, K. D. 1998. Economic exposure and integrated risk management. *Strategic Management Journal,* 19: 497–514.
Monaghan, S., Tippmann, E., & Coviello, N. 2020. Born digitals: Thoughts on their internationalization and a research agenda. *Journal of International Business Studies,* 51(1): 11–22.
Nambisan, S., Lyytinen, K. J., Majchrzak, A., & Song, M. (2017). Digital innovation management: Reinventing innovation management research in a digital world. *MIS Quarterly, 4*(1), 223–238.
Nambisan, S., Zahra, S., & Luo, Y. 2019. Global platforms and ecosystems: Implications for international business theories. *Journal of International Business Studies,* 50(9): 1464–1486.
Oxley, J., & Yeung, B. 2001. E-commerce readiness: Institutional environment and international competitiveness. *Journal of International Business Studies,* 32: 705–723.
Potrafke, N. 2015. The evidence on globalization. *World Economy,* 38(3): 509–552.
Prahalad, C. K., & Doz, Y. 1987. *The multinational mission: Balancing local demands and global vision*. New York: Free Press.
Rangan, S., & Sengul, M. 2009. Information technology and transnational integration: Theory and evidence on the evolution of the modern multinational enterprise. *Journal of International Business Studies,* 40(9): 1496–1514.
Rugman, A. M. (2009). *The oxford handbook of international business* (2nd ed.). Oxford, UK: Oxford UniversityPress.
Rugman, A. M., & Verbeke, A. 2003. Extending the theory of multinational enterprise: Internalization and strategic management perspectives. *Journal of International Business Studies,* 34(2): 125–137.

Sacks, J. 2020. *The ages of globalization: Geography, technology and institutions*. New York: Columbia University Press.
Song, J., & Shin, J. 2008. The paradox of technological capabilities: A study of knowledge sourcing from host countries of overseas R&D operations. *Journal of International Business Studies,* 39(2): 291–303.
Stallkamp, M., & Schotter, A. P. J. 2021. Platforms without borders? The international strategies of digital platform firms. *Global Strategy Journal,* 11(1): 58–80.
Sturgeon, T. (2020). Upgrading strategies for the digital economy. *Global Strategy Journal,* In press.
Tallman, S., Luo, Y., & Buckley, P. 2018. Business models in global competition. *Global Strategy Journal,* 8(4): 517–535.
Tong, T., & Reuer, J. 2007. Real options in multinational corporations: Organizational challenges and risk implications. *Journal of International Business Studies,* 38: 215–230.
Turkina, E., & Van Assche, A. 2018. Global connectedness and local innovation in industrial clusters. *Journal of International Business Studies,* 49: 706–728.
Tushman, M. L., & Nadler, D. A. 1978. Information processing as an integrating concept in organizational design. *Academy of Management Review,* 3: 613–624.
UNCTAD. 2013. *Global value chains and development: Investment and value added trade in the global economy*. Geneva, Switzerland.
UNCTAD. 2015. *Information economy report: Unlocking the potential of E-commerce for developing countries*. Geneva, Switzerland.
van Tulder, R., Verbeke, A., & Piscitello, L. 2019. *International business in the information and digital age*. London: Emerald.
Verbeke, A., & Greidanus, N. S. 2009. The end of the opportunism vs trust debate: Bounded reliability as a new envelope concept in research on MNE governance. *Journal of International Business Studies,* 40(9): 1471–1495.
Werner, S., Brouthers, L., & Bouthers, K. 1996. International risk and perceived environmental uncertainty: The dimensionality and internal consistency of Miller's measure. *Journal of International Business Studies,* 27: 571–587.
Williams, T. A., Gruber, D. A., Sutcliffe, K. M., Shepherd, D. A., & Zhao, E. 2017. Organizational response to adversity: Fusing crisis management and resilience research streams. *Academy of Management Annals,* 11(2): 733–769.
World Bank. 2016. World Development Report 2016: Digital dividends. Washington DC, United States.
Yoo, Y., Boland, R., Lyytinen, K., & Majchrzak, A. 2012. Organizing for innovation in the digitized world. *Organization Science,* 23(5): 1213–1522.

ABOUT THE AUTHOR

Yadong Luo is the Emery M. Findley Distinguished Chair and Professor of Management at Miami Herbert Business School, University of Miami. His research interests include global strategy, international management, and emerging economy businesses.

Accepted by Alain Verbeke, Editor-in-Chief, 10 April 2021. This article has been with the author for one revision.