Gartner Research

What Forces Are Driving Digital Geopolitics and Where CIOs Should Focus

By Brian Prentice, Gavin Tay, David Groombridge, Tsuneo Fujiwara

28 February 2022

Gartner

What Forces Are Driving Digital Geopolitics and Where CIOs Should Focus

Published 28 February 2022 - ID G00760479 - 17 min read

By Analyst(s): Brian Prentice, Gavin Tay, David Groombridge, Tsuneo Fujiwara

Initiatives: CIO Leadership of Innovation, Disruptive Trends and Emerging Practices

The ubiquity of digital technology is intersecting with the geopolitical aspirations of countries, creating what Gartner refers to as "digital geopolitics," competition in the digital realm between countries. Digital geopolitics will create both new opportunities and challenges for CIOs to manage.

Overview

Impacts

Digital geopolitics is now one of the most disruptive trends that CIOs must address, and impacts will surface in four distinct areas:

- Efforts to establish a domestic technology industry provide CIOs an opportunity for proactive engagement with governments.
- The growing digitalization of national military and security apparatuses will limit the availability of some technologies and within various countries.
- Digital sovereignty will be a primary source of complex, dynamic and expanding compliance obligations for multinational enterprises.
- National competition for control over the governance of cyberspace will impact the operations of multinational enterprises.

Recommendations

To exploit the opportunities and manage the risks associated with the disruptive potential of digital geopolitics, CIOs should:

- Increase the value of innovation programs by localizing specific initiatives in countries that have the best integration between local expertise and access to government co-innovation support.

- Minimize disruptions to enterprise operations by establishing a geopolitical vendor and technology risk center of excellence, chartered with a regular assessment of the exposure of key suppliers to evolving government restrictions.

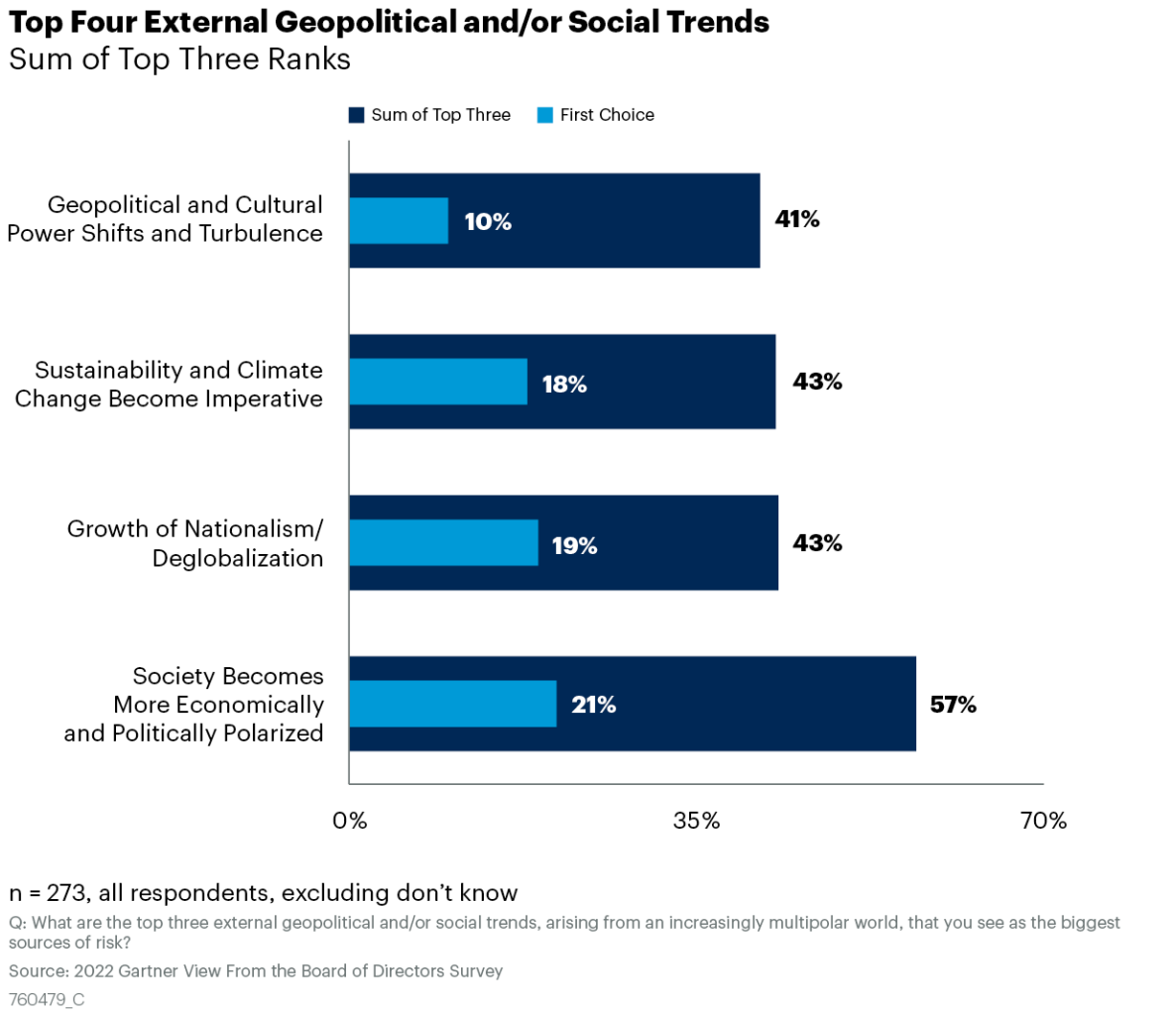
- Ensure that IT strategy and operating models are shaped in accordance with evolving global digital regulations, by tasking enterprise architecture leaders to establish a formalized communication channel with legal counsel.

- Advance executive leaders' and board members' understanding of cross-national competition for control over cyberspace governance and impacts to an enterprise's operations, by leading an annual cyberspace environmental update briefing to executives.

Introduction

Many CIOs are increasingly dealing with digital geopolitical issues, such as trade disputes, legislation coming from one country that impacts global operations, and government-imposed restrictions on the acquisition and use of digital technology. Technology governance issues emanating from the world of cross-country politics are of increasing concern to CIOs (see Figure 1).

Figure 1. Top Four External Geopolitical and/or Social Trends



n = 273, all respondents, excluding don't know

Q: What are the top three external geopolitical and/or social trends, arising from an increasingly multipolar world, that you see as the biggest sources of risk?

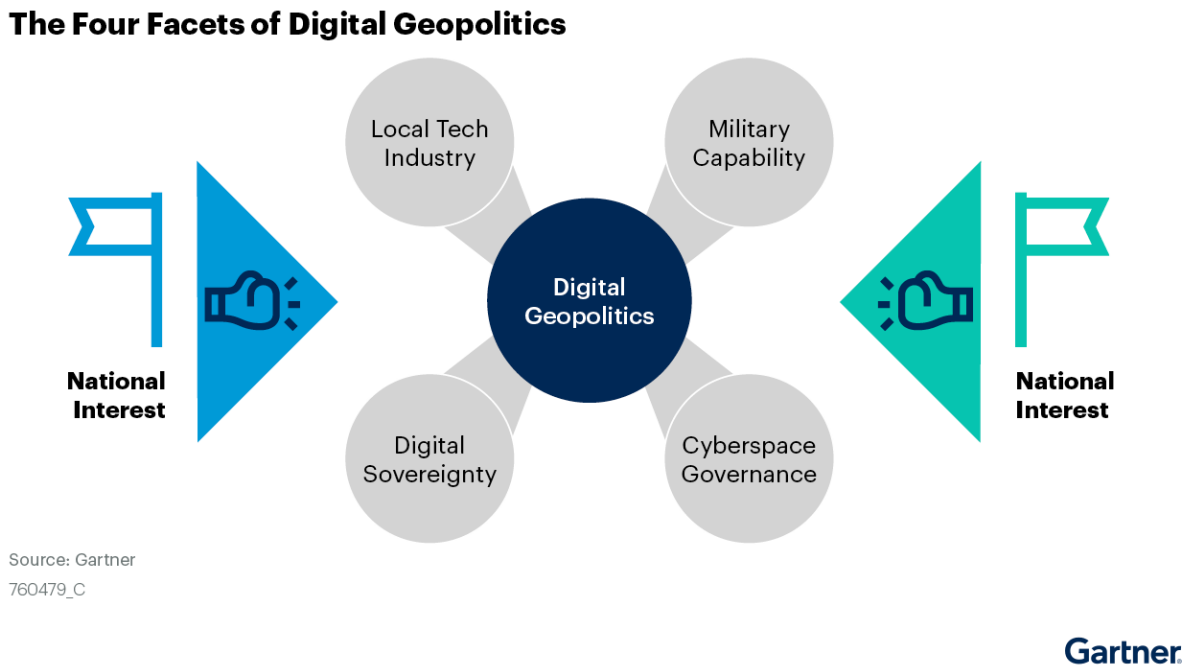
Source: 2022 Gartner View From the Board of Directors Survey

760479_C

Gartner

Digital geopolitics is the specific set of expressions of the competition between nations (or unions of nations) in the realm of digital technology and cyberspace. As a rapidly evolving disruptive trend, it is likely to take leading CIOs three to five years to reorient the IT organization to proactively respond to the challenges coming out of digital geopolitics. But this evolution is not transitory, as managing digital geopolitics will become a permanent part of IT governance, moving forward. CIOs will need to get acquainted with this new reality and prepare for its impacts (see Figure 2).

Figure 2. The Four Facets of Digital Geopolitics



Digital geopolitics comprises four distinct facets of government behavior, each of which creates its own impacts. CIOs will have to take action on these impacts, by managing or exploiting them. These facets are:

1. The need for government to build a local technology industry
2. The need to achieve necessary military capability
3. Efforts to protect digital sovereignty
4. The desire to exert direct control over the governance of cyberspace

Impacts and Recommendations

Efforts to Establish a Domestic Technology Industry Provide CIOs an Opportunity for Proactive Engagement With Governments

Gartner forecasts that global IT spending will exceed $4.2 trillion by the end of 2021, significantly larger than 2019 spending of $3.8 trillion. [1] That is set to grow to $16 trillion by 2030. [2]

A market that is this large, growing this fast and of this strategic importance and requires neither a specific national resource advantage nor significant capital expenditure, makes high technology an area of great interest for public policymakers around the world. Few industry sectors provide a country the same type of tax and employment possibilities.

For decades, governments have sought proactive measures to attract high-technology investments. [3] Early efforts by governments focused on local investment mandates (for example, Australian government's offsets program in the mid-1980s), which then evolved into tax incentives and technology hubs (for example, Malaysia's Multimedia Super Corridor, Zhongguancun in Beijing's Haidian district and Porto Digital in Sao Paulo). It should be noted, however, that many technology hubs are really about attracting technology providers into dedicated office complexes — they're a local real estate investment bid, rather than a way to establish a local technology industry.

The big shift in strategy has been going on for about a decade. Governments are increasingly focused on organically growing their local high-tech industries. To achieve this, they're shifting their focus to attracting investment in high-tech R&D, not high-tech companies.

Recognizing that such efforts are contingent on funding and talent, governments are applying two common tactics. In the absence of local venture capital infrastructure, governments are creating high-tech R&D subsidies. Examples include Taiwan's Pilot Industries Research, Development and Upgrade Program [4] and the European Union's €1.1 billion European Innovation Council. [5] Coupled with these investment subsidies are education and visa programs targeted at high-tech workers (for example, Australia's Global Talent Independent Program, and United Arab Emirates' National Program for Coders, which includes "golden visas").

So, why does this matter to an enterprise CIO? The first point to understand is that, where the other forces driving digital geopolitics are resulting in new governance obligations or changing environmental factors that need to be managed, the drive by governments to create a local high-tech industry creates new opportunities for CIOs to exploit.

Those opportunities accrue to the CIOs who perceive their own internal digital innovation efforts as R&D activities meant to yield digital assets. By combining this perspective with the realization that reglobalization is increasingly decentralizing the operations of multinational enterprises, CIOs can selectively target digital innovation initiatives to countries with the best combination of subsidies and talent.

If local subsidies are limited to local small or midsize firms, multinational CIOs can explore options such as working with startups through direct investment or equity swaps for intellectual property.

This should not be seen solely as a way to reduce the cost of innovation. Just as important is the possibility of assisting the enterprise in becoming established as a multilocal company. This aligns with the objectives of the governments providing the support, and it helps the enterprise in gaining access to local policymakers.

Recommendation

- To increase the value of an innovation program, localize specific initiatives into countries that have the best integration between local expertise and access to government co-innovation support.

The Growing Digitalization of National Military and Security Apparatuses Will Limit the Availability of Some Technologies Within Various Countries

Modern societies are rapidly digitalizing — and that includes a country's military and security apparatus. There are two facets that impact enterprises and CIOs. The first deals with the emerging sphere of cyberwarfare. The other is the digitalization of existing warfighting and security technologies.

Most of a CIO's attention to this topic is on the former. For very good reasons, CIOs understand that their enterprises can be the target of state-sanctioned cybercrime or, in the event of a "hot war," the target of direct attacks individually or as part of a broader national infrastructure (for example, water supply, electricity grid and financial systems).

Less appreciated by CIOs is the need to plan for the downstream impacts of the decisions that governments are making themselves to deal with both facets of a digitalized military and security apparatus. The most pressing impact is the growing restrictions being placed on some suppliers or even technologies.

Many CIOs might remember the 1990s and the export restrictions that were placed on data encryption technology enforced by the U.S. government's defense trade regulations. For eight years, multinational enterprises had to deal with substandard security technology as the Software Publishers Association and numerous technology providers negotiated for the eventual end to these restrictions in 2000. [6]

That once distant memory is coming back to haunt enterprises. Export restrictions have had an ongoing impact on the digital technology landscape. The 1996 Wassenaar Arrangement has been a continuous source of frustration. The latest reminder of this fact is the restrictions being placed on Huawei's 5G technology, based on concerns held by numerous countries on the potential risk of surveillance back doors. Retaliation in China toward suppliers such as Ericsson is forcing that company to reduce its presence in China. [7] In 2021 alone, the U.S. added seven Chinese supercomputing companies to its Bureau of Industry and Security's Entity List. [8]

But this is not strictly a matter of keeping suppliers out of a country or region. Defense and security considerations will also result in efforts to keep suppliers in. While the EU and the U.K. are lagging in many areas of digital technology, quantum computing is an area that they're competitive. Decision makers recognize how important quantum computing will be in military matters, [9] but also recognize the need to create the conditions for local quantum computing providers to stay in the U.K. and EU. The result is both direct government investment, [10] coupled with efforts to create "buy local" conditions. [11]

What all this means for CIOs is that they can no longer take for granted that all technology used by the enterprise for its operations will be available to any country in which it operates. CIOs will likely find themselves in a world with both restricted and mandated suppliers. The technology environment of the enterprise will become more complicated. Vendor management strategies will need to be revised, and costs will rise. These are the result of environmental factors out of the CIO's direct control. What is under the CIO's control is the ability to manage the environment better than competitors.

Recommendation

- To minimize disruptions to enterprise operations, establish a geopolitical vendor and technology risk center of excellence, chartered with a regular assessment of the exposure of key suppliers to evolving government restrictions.

Digital Sovereignty Will Be a Primary Source of Complex Compliance Obligations for Multinationals

CIOs have long understood that becoming locked into a vendor's technology means that a supplier can exert control of the operations of an enterprise. As digital infrastructure has now become critical to the function of a modern society, this same concern has taken on a macroeconomic manifestation.

The terms most used to represent the collection of actions taken by governments to avoid their own version of vendor lock-in is called “tech sovereignty,” “digital sovereignty” or “cyber sovereignty.” As succinctly put by Ursula von der Leyen, president of the European Commission:

- “‘tech sovereignty’ … describes the capability that Europe must have to make its own choices, based on its own values, respecting its own rules.” [12]

Digital sovereignty should be understood as the reactive response by governments to the power that foreign hyperscale providers — the digital giants (including Apple, Alphabet, Facebook, Amazon, Tencent, Alibaba and Baidu) — are capable of exerting on the nation’s economy and society.

As the hyperscale providers’ market dominance expands, governments outside the U.S. and China want to:

1. Ensure hyperscale providers adhere to accepted local business practices
2. Avoid scenarios where hyperscale providers operate in their jurisdictions, based on legislative and regulatory conditions set by foreign governments
3. Eliminate foreign interference in the proper function of their societies

The last point deserves some additional examination. The central aim of all technology providers is to successfully define and control a ubiquitous standard. This standard could be as specific as a document file format to something as broad as the means by which people interact with one another, or the way that financial institutions transfer money. But providers that achieve that aim are ultimately under the legislative and regulatory umbrella of government. The more important a particular ubiquitous technology standard is to the functioning of society, the more geopolitical power a government can wield through its legislative and regulatory umbrella. Recent U.S. government sanctions placed on foreign politicians and businesspeople have demonstrated what this can look like in practical terms. [13]

CIOs must not confuse the strategic intent of governments with the tactics used to achieve those objectives. While specific initiatives may be short-lived or avoidable, the goals that these initiatives are tied to are long-term. Digital sovereignty has reached the same level of governmental concern as food security, energy supply, military capability and supply chain security.

The primary means that governments are addressing digital sovereignty is through their legislative and regulatory powers. Privacy laws such as the EU's GDPR, the California Consumer Privacy Act of 2018 or China's PIPL are high-profile examples. Furthermore, governments are increasingly turning to extraterritorial legislation. Companies that deal with the citizens of a jurisdiction are required to comply with its laws, regardless of where the company operates and, increasingly, regardless of where the jurisdiction's citizens reside.

Because governments' digital sovereignty efforts are largely in the legislative realm, CIOs are, themselves, not directly responsible for managing this dimension of digital geopolitics. It's the enterprise's legal counsel who bears the primary responsibility for staying abreast of the changing regulatory landscape. However, CIOs must be proactively engaged in ensuring that the IT organization's operating model and operating practices reflect current laws and regulations in place. CIOs should ensure that the appropriate direct reports of their teams have established lines of communication with legal counsel and that advice provided flows through the whole IT organization. The CIO's role is to be aware of the legal environment and be able to articulate to other executive leaders how the IT organization supports compliance across the enterprise.

Recommendation

- Task the head of enterprise architecture to establish a formalized communication channel with legal counsel to ensure that IT strategy and operating models are shaped in accordance with global digital regulation.

National Competition for Control Over the Governance of Cyberspace Will Reshape the Operations of Multinationals

What binds a nation, or a union of nations together, is a shared sense of identity, expressed through a common thread of values held by its citizens. Similarly, technology in general, and digital technology, specifically, are an expression of the values held by its designers.

We accept many facets of our modern digital infrastructure as inherently correct — for example, decentralized network design, technology as a tool for free expression and the positive long-term impact of creative destruction. But these facets are inherently American … they reflect the national values held by the people who built the early digital foundations.

However, those values are not shared globally. Some countries see any form of free market as antithetical to their own values. Free expression is not a universal right. Other countries value digital free markets, but not at the expense of other values. These could include cultural continuity or religious beliefs.

So, as digital technology weaves itself through all aspects of society, nations are seeking to ensure that their own technologies reflect and support their core values and their citizens' sense of nationhood. Increasingly, governments are concluding that this objective can't be achieved without a protected national digital infrastructure. It's what drove China's Great Firewall and is driving efforts like its proposal for a new internet transport protocol (New IP). It's what's behind initiatives like the EU's Gaia-X and is the basis for RuNet, Russia's sovereign internet.

Yet the economic laws of digital technology don't change. Scale and ubiquitous standards matter. Therefore, governments can't operate in a permanent state of protecting their digital sovereignty through reactive legislation and regulation. This is why there is a growing belief by governments that the route to true digital sovereignty comes through some form of protected national digital infrastructure that is projected outward, in direct competition with other digital national infrastructures. Whether this turns out to be true in a world where hyperscale providers are unlikely to disappear is yet to be seen.

The clearest example of national competition in cyberspace is China's Digital Silk Road (DSR) initiative. DSR investments being made around Asia/Pacific and Africa include not just infrastructure such as 5G cellular networks, data storage centers and global satellite navigation systems, but also fintech, edutech and e-commerce platforms and apps. [14]

The U.S. doesn't have a similar program, but it already exerts significant control over much of the world's digital technology infrastructure. This is generating another competitive dynamic — activities directed at undermining standards seen as under control by the U.S. One example would be Russia's efforts to establish a closed network between countries within the Brazil, Russia, India, China and South Africa (BRICS) partnership. The system would involve backup root DNS servers located in the BRICS countries, independent of those managed by the ICANN organization. [15]

The machinations by governments for control over cyberspace governance are beyond the influence of the CIO, much less any other executive leader. Yet these machinations will have profound impacts on the ability of a business to operate internationally, as well as corporate operations and structure.

The role of CIOs in this environment, as business and technology leaders, is to inspire, influence and advise other executive leaders. Digital geopolitics sits at the intersection between CIOs' desire to operate at the highest level of executive leadership and executive leadership's need for advice on how to respond to the highest level of digital disruption. CIOs should take this opportunity to expand their knowledge and expertise in digital geopolitics and find formal mechanisms to convey insights to the CEO, the board of directors and other senior leaders.

Recommendation

- Lead an annual cyberspace environmental update briefing for all executive leaders and board members, to help the organization navigate the impacts of cross-national competition for control over cyberspace governance.

Acronym Key and Glossary Terms

DSR	Digital Silk Road
ICANN	Internet Corporation for Assigned Names and Numbers

Evidence

[1] Gartner Market Databook, 4Q21 Update.

[2] Hi-Tech Market Set to Reach USD 16 Trillion by 2030, Business Wire.

[3] "In sum, for places like these across the nation's interior, venture capital is unlikely to work as the sole type of financing mechanism to drive technology innovation and entrepreneurship. Given that, innovation-oriented policymakers looking to foster the growth of resilient and tech-driven economies in the Heartland will need to look beyond venture capital and explore a diversity of financing mechanisms to support technology companies in their regions." Beyond VC: Financing Technology Entrepreneurship in the Rest of America, Brookings Institute blog post.

[4] "Pilot Industries Research, Development and Upgrade Programme, which will provide NT$10bn (US$334m) in subsidies over seven years to attract international technology companies to invest in research-and-development (R&D) activity on the island … The subsidies are available to eligible foreign companies that collaborate with aspiring local firms in R&D activity related to three core technologies: emerging semiconductors, 5G and artificial intelligence. The plan offers 50% government support for those R&D costs, and aims to further cement Taiwan's status as a high-technology innovation hub." Government Aims to Attract Foreign Technology Companies, Economist Intelligence Unit.

[5] EU Startup Fund Overwhelmed by High Demand, Politico.

[6] Legal Restrictions on Cryptography, section on U.S. regulatory efforts and history, O'Reilly.

[7] Beijing Shuns Ericsson, Nokia as the West Curbs Huawei, The Wall Street Journal.

[8] BIS Adds Seven Chinese Parties Involved in Supercomputing to the Entity List, Baker McKenzie blog post.

[9] "Quantum Information Processing (QIP) could contribute to future combat systems through Network Quantum Enabled Capability (NQEC). There are challenges and issues which must be considered and resolved before the technology is available so that adoption will be as rapid as possible." A. Middleton and S. Till, Quantum Information Processing Landscape 2020: Prospects for U.K. Defence and Security, U.K. Defence Science and Technology Laboratory, Page 38.

[10] UK Government to Invest £153 Million in Quantum Research Projects, Finextra.

[11] "Government procurement programs are a key determinant of HPC hardware providers' outlooks. This is especially true when companies have little chance to sell into foreign markets. Today, the United States and China are keeping their market closed to foreign vendors … Two initiatives in Europe are ongoing: a plan to build European supercomputers, including exascale HPC, known as the EuroHPC Joint Undertaking (JU), and a plan to develop a European microprocessor for extreme-scale computing, known as European Processor Initiative or EPI … The funding will be used toward a dual goal: to deploy top-of-the-range supercomputing infrastructure across Europe to match users' needs, and to develop a research and innovation ecosystem for HPC technologies in Europe." A. Pannier, Strategic Calculation: High-Performance Computing and Quantum Computing in Europe's Quest for Technological Power, Études de l'Ifri.

[12] Shaping Europe's Digital Future: Op-Ed by Ursula von der Leyen, President of the European Commission, European Commission.

[13] "Financial sanctions focus on the flow of funds and other forms of value to and from a target country, corporation, individual, or other entity. These sanctions can have wide impact because they can not only freeze financial assets and prohibit or limit financial transactions, but they also impede trade by making it difficult to pay for the export or import of goods and services … their enforcement, which occurs through a unique combination of (a) actions and self-reporting by U.S. and other international financial institutions and (b) supervision by U.S. regulatory authorities. " B. E. Carter and R. Farha, Overview and Operation of U.S. Financial Sanctions, Including the Example of Iran, Georgetown University Law Center.

[14] China's Digital Silk Road and the Global Digital Order, The Diplomat.

[15] Digital Sovereignty in the Age of Connectivity: RuNet 2020, SecAlliance blog post.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

The 2022 CIO and Technology Executive Agenda: Master Business Composability to Succeed in Uncertain Times

Roadmap to Renewal: The 2022 Board of Directors Survey

Predicts 2022: Privacy Risk Expands

[12] Shaping Europe's Digital Future: Op-Ed by Ursula von der Leyen, President of the European Commission, European Commission.

[13] "Financial sanctions focus on the flow of funds and other forms of value to and from a target country, corporation, individual, or other entity. These sanctions can have wide impact because they can not only freeze financial assets and prohibit or limit financial transactions, but they also impede trade by making it difficult to pay for the export or import of goods and services … their enforcement, which occurs through a unique combination of (a) actions and self-reporting by U.S. and other international financial institutions and (b) supervision by U.S. regulatory authorities." B. E. Carter and R. Farha, Overview and Operation of U.S. Financial Sanctions, Including the Example of Iran, Georgetown University Law Center.

[14] China's Digital Silk Road and the Global Digital Order, The Diplomat.

[15] Digital Sovereignty in the Age of Connectivity: RuNet 2020, SecAlliance blog post.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

The 2022 CIO and Technology Executive Agenda: Master Business Composability to Succeed in Uncertain Times

Roadmap to Renewal: The 2022 Board of Directors Survey

Predicts 2022: Privacy Risk Expands

Connect With Us

Get actionable, objective insight to deliver on your most critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Stay connected to the latest insights

Attend a Gartner webinar

View Webinars

Gartner®