WORLD
ECONOMIC
FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Trust, Security and Regulation
Dynamic Briefing

Generated 27 January 2022 for Exploring Leaders @ Digoshen

Trust, Security and Regulation

Last review on Sun 02 January 2022

About

This dynamic briefing draws on the collective intelligence of the Forum network to explore the key trends, interconnections and interdependencies between industry, regional and global issues. In the briefing, you will find a visual representation of this topic (Transformation Map – interactive version available online via intelligence.weforum.org), an overview and the key trends affecting it, along with summaries and links to the latest research and analysis on each of the trends. Briefings for countries also include the relevant data from the Forum's benchmarking indices. The content is continuously updated with the latest thinking of leaders and experts from across the Forum network, and with insights from Forum meetings, projects communities and activities.

WORLD ECONOMIC FORUM
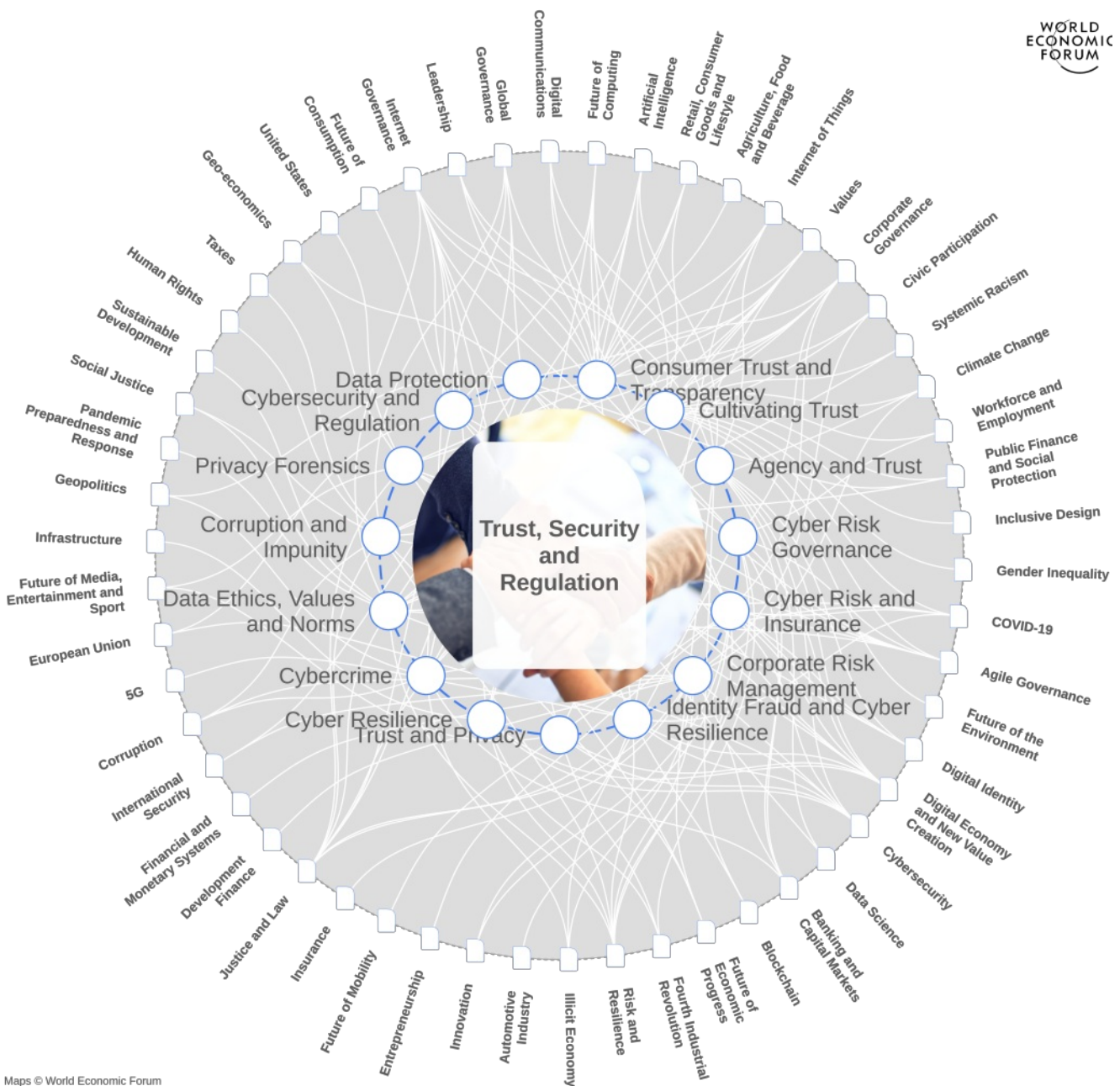
Maps © World Economic Forum
Licensed for professional use.

Trust, Security and Regulation Briefing, January 2022

Executive summary

Trust, Security and Regulation Intelligence Map - insights and perspectives curated by Digoshen via World Economic Forum Strategic insights and contextual intelligence.

1. Consumer Trust and Transparency

In countries where consumer spending is needed to fuel the global economy, trust in businesses is lagging.

2. Cultivating Trust

Responsible corporate governance can create a culture of mutual trust.

3. Agency and Trust

The ability to provide security and agency over personal data could become a competitive differentiator.

4. Agency and Trust

The ability to provide security and agency over personal data could become a competitive differentiator.

5. Cyber Risk Governance

The number of corporate boards with a dedicated cybersecurity committee is expected to increase sharply by 2025.

6. Cyber Risk and Insurance

Insurers are underwriting more related policies, as they themselves are increasingly exposed to attack.

7. Corporate Risk Management

For boards, the volatility of risk scenarios is only increasing.

8. Identity Fraud and Cyber Resilience

The increasing amount of personal data being collected and exploited creates security challenges.

9. Trust and Privacy

Trust in data-based applications is diminishing, as privacy concerns are not effectively addressed.

10. Cyber Resilience

Accelerating digitization prompts a need for integrated defense, prevention and response.

11. Cybercrime

The nature of ransomware attacks has shifted from annoyance to the disruption of key infrastructure.

12. Data Ethics, Values and Norms

Data can be deployed to solve global problems and achieve the SDGs, with the right oversight.

13. Corruption and Impunity

When illicit trade is allowed to flourish, it spawns a culture of impunity.

14. Privacy Forensics

New techniques offer an opportunity to address the asymmetry at the heart of the privacy problem.

15. Cybersecurity and Regulation

The EU has provided a model for the evolution of cybersecurity regulation.

16. Data Protection

Landmark regulation has not directly led to effective enforcement.

Consumer Trust and Transparency

In countries where consumer spending is needed to fuel the global economy, trust in businesses is lagging

Large emerging markets like India and China, where an expanding middle class is expected to buoy the global economy with growing consumer spending in the coming years, are home to notable lags in public trust among the "mass population" in businesses and government, according to the 2019 Edelman Trust Barometer - a survey of 33,000 respondents conducted in more than two dozen markets. According to the barometer, more than two-thirds of respondents agreed that they might be encouraged to buy products from a company with a good reputation - but unless they genuinely came to trust the company behind the product, they would stop buying it. As global consumers become more connected and empowered thanks to digital innovation, they will only place more scrutiny on businesses. For corporate leaders, this means having to strike the right balance between short-term gains and long-term value creation. According to the Edelman Trust Barometer, one means of winning external trust is by investing internally in employees; 78% of barometer respondents agreed with the idea that the way a company treats its employees is one of the best indicators of its level of trustworthiness.

People have fundamental concerns about the safety and quality of the goods they consume. In China, for example, worries about food and medicine safety have become significant (particularly among wealthier consumers) in recent years, according to a report published by the World Economic Forum in 2018. In addition, these affluent, urban-dwelling consumers in China have particular concerns related to the historical role of fake products in the country, according to the report. Another growing area of consumer concern is related to transparency in supply chains - whether it's tied to sustainable sourcing or ethical labour standards. In the apparel sector, efforts have been made by the Sustainable Apparel Coalition and Better Work, a collaboration between the UN's International Labour Organization and the International Finance Corporation, to improve working conditions and sustainability by, for example, introducing standards to measure social and environmental impact. Data privacy is also a serious consumer concern. A relatively small group of companies including Facebook and Amazon (or, in China, Alibaba and JD.com) control large amounts of consumer data - which will present trust issues, as new means of refining and selling that data emerge.

Related insight areas: Internet Governance, Global Governance, Digital Communications, Values, Leadership, Artificial Intelligence, Future of Computing, Agriculture, Food and Beverage, Corporate Governance, Internet of Things, Retail, Consumer Goods and Lifestyle

RAND Corporation
How Prices of Sugar-Rich Foods Contribute to the Diet-Related Disease Epidemic in Mexico
13 January 2022

New evidence on how price changes of nutritionally similar foods, such as those rich in sugar or fats, change obesity and diet-related diseases in the context of Mexico between 1996–2010. The association between prices of sugary foods and chronic disease is meaningful: estimating that in Mexico, price reductions of sugary foods explained roughly 15 percent of the rise in obesity and diabetes during the 15-year study period.

Frontiers
Disruptive Innovations for Well-Functioning Food Systems: The Data-Driven "Food and Nutrition Security Under Climate Evolution" Framework
03 January 2022

The current climate crisis poses new uncertainties, risks, and vulnerabilities, and is leading to losses for millions of people depending on fragile food systems. Food systems are, however, vastly different across landscapes and communities, and their capacities to respond to climate impacts evolves and changes through time. Humanitarian and development organizations are struggling to keep pace with these changes. Monitoring a large number of diverse food systems during an evolving climate crisis can be expensive and time-consuming. This paper introduces a monitoring approach that uses a combination of open-source earth observations along with national data sources to produce highly contextualized metrics for monitoring Food And Nutrition Security under Climate Evolution (FANSCE).
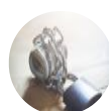
GreenBiz
HSBC, Walmart add science-based targets to supplier financing program
28 December 2021

HSBC, Walmart and CDP are teaming up to unlock more financing for Walmart suppliers. The suppliers must set validated science-based targets for emissions reductions and meet certain performance thresholds in ongoing ESG disclosures to reporting organization CDP. The supplier financing program is part of Walmart's Project Gigaton , the company's initiative to avoid 1 billion tons of greenhouse gas emissions from being released into the atmosphere by 2030. Decarbonizing this level of industry is vital for larger businesses to reach net zero and to significantly draw down carbon emissions — like many retailers, most of Walmart's emissions come from Scope 3 relationships, many of which are with smaller suppliers. By teaming up, Walmart and HSBC both stand to make headway on their net-zero goals through client and supplier engagement.

ETH Zürich
Watch out for fakes
17 December 2021

ETH alumna Leonie Flückiger is blazing a trail through the male-dominated world of tech start-ups with her company Adresta, which uses a blockchain-based certificate to authenticate luxury timepieces. She hopes to encourage other women to follow in her footsteps.

Center for Global Development
Small and Medium Enterprises Amidst the Pandemic and Reopening: Digital Edge and Transformation
10 December 2021

Using administrative universal firm registration data as well as primary offline and online surveys of small business owners in China, we examine (i) whether the digitization of business operations helps small and medium enterprises (SMEs) better cope with the pandemic shock, and (ii) if the pandemic has induced digital technology adoption.

Cultivating Trust

Responsible corporate governance can create a culture of mutual trust

Trust is crucial for the long-term success of companies - especially at the board level. Genuine trust is underpinned by personal integrity, and by putting the interests of the organization (and of society) above those of individuals. Boards need to be able to trust that management will bring full transparency into the boardroom, and that will only happen thanks to shared integrity. There is a strong sense of pessimism about leadership in both the private and public sectors, and anxiety related to job security is high - due to a general lack of training and increasing automation, and not least due to the global pandemic. This threatens to fuel the growth of nationalist and protectionist movements. According to the Pew Research Center, as of 2019 only about one-third of adult Americans had a great deal or fair amount of confidence in elected officials to act in the public's best interests, and less than half said the same about business leaders (attitudes were far more positive when it came to the medical professionals now grappling with COVID-19). In addition to the general public, employees increasingly expect their employers to do the right thing and take action on issues related to inequality, the environment, and climate change.

As people lose faith in their political leaders, it appears that they have higher expectations for CEOs. According to the 2019 Edelman Trust Barometer, more than three-quarters of the general population, or 76%, want CEOs to take the lead on necessary social and economic change rather than waiting for governments to act. While organizations must comply with legislation and regulation on everything from taxes to consumer protection, competition, corruption, and environmental protection, they can also be positively influenced in terms of corporate governance and trust by industry self-regulation and voluntary practices - such as a code of conduct. Most cases of fraud and breach of trust among stakeholders can be traced to corporate governance failures, and so corporate leaders have the ultimate responsibility for creating an organizational culture that supports trust - and ensures that management and employees embody and act on the stated values and mission of their organization. Particular areas of increased social expectations that require the attention of boards of directors include diversity (including gender diversity), transparency, equal opportunity, and eliminating all forms of harassment.

Related insight areas: Values, Systemic Racism, Diversity and Inclusion, Leadership, Climate Change, Public Finance and Social Protection, Civic Participation, Agile Governance, Artificial Intelligence, Workforce and Employment, Retail, Consumer Goods and Lifestyle, Gender Inequality, Future of the Environment, COVID-19

London School of Economics and Political Science

Public support for a universal basic income is dependent on the way it is funded

25 January 2022

The concept of a universal basic income has received increased attention since the start of the Covid-19 pandemic. But what do the public think about the proposal? Drawing on a new study, Leire Rincón illustrates that a key factor affecting support for a universal basic income is the way it is funded, with more people … Continued.

London School of Economics and Political Science

Senate opposition means Democrats will struggle to pass voting rights bills.

10 January 2022

Democrats have begun 2022 with a renewed effort to pass voting rights legislation. And while President Joe Biden and senior Senate Democrats have been pushing for two key voting rights bills and changes to Senate rules to enable them to pass, they continue to be blocked by Republicans. Julie Norman discusses the context and content of the bills, the options […].

World Economic Forum

Stakeholder Capitalism | EP3 - Planet vs. Profit: Can Growth be Green?

06 January 2022

While the value of big tech companies has soared, what problems has that created? A lack of market competition and the impact that has on economies; data protection concerns; falling public trust. Is big tech too big, and what should be done? .

Harvard Business Review

How Brands Can Enter the Metaverse

03 January 2022

There are quite a few people who believe that the latest paradigm shift for the internet is already well underway: the metaverse, they say, is almost here.

Raconteur

Is it time to hire a head of remote work?

20 December 2021

Talent management is totally different from how it looked only two years ago, with some level of remote working becoming essential in many industries, rather than the nice-to-have option it was before.

Wharton School of the University of Pennsylvania - Knowledge@Wharton

Beyond Business: Humanizing ESG

13 December 2021

Smart firms are listening, learning, and changing longstanding practices that have caused decades of harm to people, according to participants in a recent "Beyond Business" panel discussion, hosted by Wharton Dean Erika James.

Chatham House

How can the investor community address the 'S' in ESG? – the role of social purpose values

24 November 2021

This webinar highlights the crucial relationship between an open civic space and a profitable business environment. 2020 was a tipping point for investors to think and act more responsibly, galvanized by catalysts like the killing of George Floyd and the pandemic. There is increasing investor support for social and environmental causes. Younger investors are placing increasing emphasis on values and social issues in their investment decisions. The 'S' in the Environment Social and Governance (ESG) agenda is clearly gaining traction, but how far does it extend to civil and political liberties i.e.

Agency and Trust

The ability to provide security and agency over personal data could become a competitive differentiator

The Fourth Industrial Revolution has been built on a foundation of data as a source of both innovation and governance. While giving people more agency over their data can potentially improve their relationships with the institutions they must rely on daily, the use of biometrics, facial recognition, and multi-factor authentication (verifying a user with multiple credentials) can help establish trust - something that has become increasingly scarce as cybercrime and the commercial exploitation of personal data increase. The same technology that can improves verification can deplete trust, however; artificial intelligence, for example, can be vulnerable to manipulation and the biases of its human programmers. People are generally demanding more agency over their data, and some technology companies and governments are exploring decentralized identity systems that could ultimately empower users; Microsoft, Accenture, and Mastercard have announced plans to invest in decentralized models, for example, and Malta's government developed a way for educational institutions to issue blockchain-based academic credentials that are owned by students, portable, and instantly verifiable. By the year 2022, about 150 million people will have blockchain-based identities, according to IDC, even though the technology is still at a relatively early stage of development.

Traditionally, governments or banks have played the role of "trust anchor" for financial transactions, though emerging digital identity models involve new actors. For example, the pharmacy startup Capsule, referred to as an "Uber for drugs," relies on doctors as a source of trust when filling e-prescriptions for delivery. Several related governance efforts exist, such as the Pan-Canadian Trust Framework and the European Union's implementation of an ethical AI strategy. However, the monopolization of technology platforms used for search and social media - and pervasive personal data gathering - complicate efforts to win digital trust. According to poll results published by the Pew Research Center in 2018, nearly half of American respondents did not trust the government to protect their personal data, and 51% did not trust social media companies to do so either. While internet users expect personalized experiences, they also expect security and agency over personal data - something that could become a competitive differentiator among companies and organizations. Stakeholders in every industry should promote the stewardship of identity practices that place the user at the centre of systems, create collaborative governance mechanisms, and take interactions between human and non-human identities into consideration.

Related insight areas: Internet of Things, The Digital Economy, Artificial Intelligence, Internet Governance, Economic Progress, Cybersecurity, Blockchain, Digital Communications, Digital Identity, Data Science, Banking and Capital Markets

Asian Development Bank (ADB)
Asian Impact 39: ADB Distinguished Speakers Program - Daron Acemoglu
25 January 2022

Is the world today afflicted with excessive automation? In this lecture, Professor Daron Acemoglu will discuss automation and its consequences, including the potential economic, political, and social costs of the current path of artificial intelligence (AI) and digital technologies. By displacing the developing countries' most valuable resource—labor—with capital and algorithms, the current trajectory of technology adoption may be inappropriate for the needs of the emerging world.
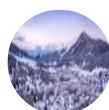
World Economic Forum
An attack on inequality misses its target
20 January 2022

In his book Davos Man , American journalist Peter Goodman investigates one of the defining global issues of our time: the steep and still rising economic inequality that characterizes global societies. With more interest in polemic than profound economic analysis, he misses a chance to make a more meaningful contribution. As a longtime participant to the World Economic Forum, Peter Goodman is well placed to weigh in on the causes of and solutions to economic inequality. In his new book, he shines more as reporter, relaying the testimonies of workers and small scale entrepreneurs anywhere from the american midwest to tuscan italy. He highlights the link that exists all around the world, between rising economic hardship and political anger.

World Economic Forum
3 ways digital technology can be a sustainability game-changer
19 January 2022

Our new survey underlines the huge impact digital technology is having on organisations' sustainability agendas. As well as its benefits, digital can also pose risks to sustainability. Here are 3 areas for companies to consider as they undergo their digital transformations and build their sustainability strategies. Digital strategy and sustainability are increasingly important and increasingly intertwined. In a recent survey of 400 executives from various industries and regions conducted by Bain & Company and the World Economic Forum, 40% of respondents said they believe digital technologies are already having a positive impact on their sustainability goals.

World Economic Forum
Special Address by António Guterres, Secretary-General, United Nations | Davos Agenda 2022
17 January 2022

Special Address by António Guterres, Secretary-General of the United Nations with Børge Brende, President of the World Economic Forum #DavosAgenda. Simultaneous interpretation in English, Arabic, French, Mandarin Chinese, Russian and Spanish. .

World Economic Forum
Technology Cooperation in the Fourth Industrial Revolution | Davos Agenda 2022
17 January 2022

The technologies of the Fourth Industrial Revolution have already led to transformative advances in numerous domains. How can technology stakeholders work together to balance innovation and responsibility to maximize the potential of emerging technologies for addressing global problems?.

MIT Sloan Management Review
Human Diversity Will Save Your Job From the Robot Takeover | Ayanna Howard
12 January 2022

Our expert columnists offer opinion and analysis on important issues facing modern businesses and managers. More in this series Robots have long been celebrated as ideally situated to take over society's most dirty, dull, and dangerous jobs, from robot vacuum cleaners (dirty) to manufacturing robots (dull) to military robots (dangerous). All those roles, of course, were at one point held by people, and people in those functions will continue to be replaced by robots. They won't be alone: jobs that classically don't fit into the "three d's" work category — dirty, dull, and dangerous — are also being eyed as opportunities for robot workers.

Brookings
Digital health tools for pandemic preparedness
28 December 2021

Steve Davis and Pardis Sabeti discuss the uptake of participatory digital health tools for pandemic preparedness and response. Davis and Sabeti moderated Room 3 focused on Sustainable Development Goal number 3—on good health and well-being—during the 2021 17 Rooms process.

Agency and Trust

The ability to provide security and agency over personal data could become a competitive differentiator

The Fourth Industrial Revolution has been built on a foundation of data as a source of both innovation and governance. While giving people more agency over their data can potentially improve their relationships with the institutions they must rely on daily, the use of biometrics, facial recognition, and multi-factor authentication (verifying a user with multiple credentials) can help establish trust - something that has become increasingly scarce as cybercrime and the commercial exploitation of personal data increase. The same technology that can improves verification can deplete trust, however; artificial intelligence, for example, can be vulnerable to manipulation and the biases of its human programmers. People are generally demanding more agency over their data, and some technology companies and governments are exploring decentralized identity systems that could ultimately empower users; Microsoft, Accenture, and Mastercard have announced plans to invest in decentralized models, for example, and Malta's government developed a way for educational institutions to issue blockchain-based academic credentials that are owned by students, portable, and instantly verifiable. By the year 2022, about 150 million people will have blockchain-based identities, according to IDC, even though the technology is still at a relatively early stage of development.

Traditionally, governments or banks have played the role of "trust anchor" for financial transactions, though emerging digital identity models involve new actors. For example, the pharmacy startup Capsule, referred to as an "Uber for drugs," relies on doctors as a source of trust when filling e-prescriptions for delivery. Several related governance efforts exist, such as the Pan-Canadian Trust Framework and the European Union's implementation of an ethical AI strategy. However, the monopolization of technology platforms used for search and social media - and pervasive personal data gathering - complicate efforts to win digital trust. According to poll results published by the Pew Research Center in 2018, nearly half of American respondents did not trust the government to protect their personal data, and 51% did not trust social media companies to do so either. While internet users expect personalized experiences, they also expect security and agency over personal data - something that could become a competitive differentiator among companies and organizations. Stakeholders in every industry should promote the stewardship of identity practices that place the user at the centre of systems, create collaborative governance mechanisms, and take interactions between human and non-human identities into consideration.

Related insight areas: Internet of Things, The Digital Economy, Artificial Intelligence, Internet Governance, Economic Progress, Cybersecurity, Blockchain, Digital Communications, Digital Identity, Data Science, Banking and Capital Markets

Frontiers

Editorial: Intelligence and Safety for
Humanoid Robots: Design, Control,
and Applications

20 December 2021

Humanoid robots attract growing research interests from
different communities, both as tools for artificial intelligence
research and neurocognitive interaction assessment and as
enabling technology with high societal impacts as personal
robots for health, education, and entertainment. These
robots, modelled on the basis of the embodiment of neural
systems in software and hardware devices, are characterized
by a high number of degrees of freedom, complex end
effectors and locomotion mechanisms on the hardware side.

Cyber Risk Governance

The number of corporate boards with a dedicated cybersecurity committee is expected to increase sharply by 2025

Governance relies on risk-based decision making as a fundamental means to both drive the efficient use of resources, and to improve confidence in an organization's ability to achieve strategic objectives. All organizations rely on their employees' ability to navigate a world of growing uncertainty, and to dodge threats to their ability to achieve its collective goals. Unfortunately, complex organizations can easily be overwhelmed; each risk demands a distinct analysis and potential investment of additional resources, to respond in ways that adequately reduce exposure. A good governance structure will provide a framework that enables the right managers to make the right decisions, which will help prioritize and allocate resources as needed. All risks don't necessarily require analytic rigour or subsequent investment - immediate hazards like icy sidewalks or commonplace cyber incidents like phishing emails can be addressed at lower management levels. That is not the case for strategic risks like global pandemics or advanced, persistent cyber threats that have the potential to disrupt or damage an organization indefinitely. A structure that effectively prioritizes and adjudicates risks to the right organizational level is required.

Responsibility for risks is typically apportioned in accordance with an organization's willingness to accept them, also called "risk appetite." A risk-appetite statement can be used to direct employees and clarify who has the necessary level of authority to decide how to respond to any given situation. The National Institute of Standards and Technology Special Publication 800-37 addresses the divvying up of risk with a three-tier structure including the organization, the mission, and the system. Meanwhile the ISO 27000 series of standards provides recommendations for the use of policy and organizational structure to reduce risk, and the COSO framework connects governance to culture by highlighting the importance of board oversight, culture requirements, core values, and human resource development. Vigorous, board-level engagement in risk governance is essential for success. Thankfully, boards are increasingly recognizing the importance of cyber risk governance; a study published by Ernst and Young in 2020 found that 81% of board members categorize cybersecurity as "highly relevant," and Gartner researchers predict that 40% of all boards will have a dedicated cybersecurity committee by the year 2025 (currently, just 10% of boards have one).

Related insight areas: Banking and Capital Markets, Fourth Industrial Revolution, Internet Governance, The Digital Economy, Workforce and Employment, Corporate Governance, Agile Governance, Leadership, Risk and Resilience, Illicit Economy
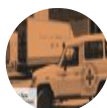
The New Humanitarian
Comment: Red Cross data hack
24 January 2022

The fallout is just beginning after what data privacy researchers say could be the biggest-ever breach of humanitarian data. The New Humanitarian spoke to Zara Rahman, acting executive director of The Engine Room, a tech and data non-profit, to find out why this huge hack at the International Committee of the Red Cross (ICRC) on 19 January shouldn't come as a surprise, and what the aid sector needs to do to protect itself — and vulnerable people. For Rahman, "it's in many ways the worst-case scenario we've been warning about for years now", but what should perhaps concern us more, she warns, is that it happened at the ICRC, a place considered to have one of the best digital protection practices in the sector. Watch this short video for her full comment on the hack. The ICRC said the cyber-attack compromised the data of more than 515,000 of the world's most vulnerable – including people uprooted by conflict and disasters.

World Economic Forum
Global Risks Report 2022 Press Conference
11 January 2022

At the virtual press conference on the Global Risks Report 2022, speakers share key findings and insights from the report.

German Institute for International and Security Affairs
Attribution: A Major Challenge for EU Cyber Sanctions
16 December 2021

An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW The attribution of cyberattacks is a sovereign act by the EU Member States. However, these all have different technical and intelligence capabilities. This leads to a lack of coherence in European cyber diplomacy, for example when imposing cyber sanctions. Analysis of policy responses to the WannaCry, NotPetya, Cloud Hopper, OPCW, and Bundestag hack cyber incidents reveals the following problems: Attribution takes a long time and relies on intelligence from NATO partners; the technical realities and the legal facts for classifying and prosecuting cyberattacks do not always match; the weighting of the criteria for establishing what constitutes a crime is unclear.

Stockholm International Peace Research Institute
Hacking nuclear deterrence: Cyber threats to nuclear systems
15 December 2021

Official and non-official attention towards cyber threats to nuclear command, control and communications (NC3) has been growing. In 2019, European, Russian and United States officials called for dialogue to address cyber threats to NC3, while think tanks in China, Sweden and the USA have identified a range of cyber-related NC3 scenarios, including false detection of a nuclear attack, disruption of communications in a crisis, supply chain threats to nuclear systems and cyber intrusions leading to unauthorized use of nuclear weapons. This complex range of threats derives from factors such as NC3's mixture of legacy and modern components, which complicates integration and identification of vulnerabilities, as well as its support of both conventional and nuclear operations, contributing to entanglement and crisis escalation.

Harvard Kennedy School - Belfer Center for Science and International Affairs
Student Fellows Share Goals and Special Moments
08 December 2021

More than 30 Harvard Kennedy School (HKS) students were selected by the Belfer Center for the coveted 2021-2022 Belfer Young Leader Student Fellowships. We asked the student fellows who will graduate in the spring of 2022 to share with us their professional interests and goals for the future as well as their most memorable experiences at HKS, tips for others, or something not well known about themselves. Meet some of our impressive upcoming grads!.

Project Syndicate
Corruption's War on the Law
23 November 2021

From Nigeria to Italy, the forces of corruption are fighting back against those who would root them out, and from bombs and bullets to writs and motions, they will use any weapon they can to improve their chances. Not content to intimidate or even murder their opponents, now they are targeting the rule of law itself.

Cyber Risk and Insurance

Insurers are underwriting more related policies, as they themselves are increasingly exposed to attack

Cyber risk has become a pressing issue both for the insurance sector specifically and for an increasingly digital world generally. According to the World Economic Forum's Global Risks Report for 2019, cyber-attacks ranked among the top 10 risks in terms of both likelihood and impact; the report pointed to massive data breaches during the prior year, the revealing of new hardware weaknesses, and research suggesting the potential use of artificial intelligence to engineer ever-more-potent cyber-attacks. Most respondents in a related survey expected cyber-attacks involving the theft of money and data, as well as disruption of operations, to increase. Insurers are underwriting a growing amount of this risk through cybersecurity insurance policies. According to a report released in 2019, the cybersecurity insurance market was expected to increase annually by nearly 25% until 2024, when it is expected to reach $20.7 billion. Due to its reliance on a proliferation of personal data, healthcare is emerging as the leading target market for cybersecurity insurance; as much as 80% of the data generated by the healthcare industry is estimated to be stored in the cloud.

The healthcare sector's vulnerability to threat has been exacerbated by the broad adoption of telehealth and telemedicine tools - which have only become increasingly necessary during the COVID-19 pandemic. The amplified size and complexity of cyber risks, coupled with a general lack of related historical data, make their pricing challenging for insurers. On the other hand, insurers themselves are increasingly exposed to cyber-attacks - not least as they deploy advanced insurtech tools based on artificial intelligence, big data, and cloud computing. For example, automobile insurers including TD Insurance are offering premium discounts based on information about policyholders' driving habits that is collected in real-time using mobile apps. Insurers must properly manage and maintain such continuously expanding volumes of data, while protecting them from fraud and theft. AI-powered customer service and claims adjustments, implemented for the greater convenience of policyholders, have also led to vulnerabilities that can be exploited by hackers. Ultimately, insurers' transition to cloud computing for quantitative processes, and greater cyber dependency, have increased the risk of outages for entire platforms and networks in ways that can cause losses and disrupt operations.

Related insight areas: Mobility, COVID-19, Risk and Resilience, Entrepreneurship, Innovation, Automotive Industry, Cybersecurity, Corporate Governance, Digital Communications, Digital Identity, The Digital Economy, Future of Computing

Harvard Business School Working Knowledge
7 Trends to Watch in 2022
19 January 2022

As 2022 gets underway we asked our faculty to highlight some trends worth watching in the coming year. Ariel Stern: A new future for digital health care While 2020 and 2021 were years of rapid innovation and deployment of new health care technologies and delivery modalities, 2022 will be a big year for learning about what works in digital health. Recently, we have witnessed developments that would have been difficult to imagine just a few years ago. In Germany, the past 15 months have seen the rollout of "prescription apps" and the introduction of a system of nationwide health insurance coverage for digital health applications, the first of its kind worldwide.

Wharton School of the University of Pennsylvania - Knowledge@Wharton
Will 2022 Be a Banner Year for Real Estate?
18 January 2022

Home prices and construction are set for a banner year in 2022, riding on the back of historically low interest rates and strong demand for work-from-home space, according to Susan M. Wachter , Wharton professor of real estate and finance. That could change, however, if prospective home buyers resist higher interest rates and rising home prices beyond a point, she said. The outlook is less rosy for the commercial space markets, with the prevailing low occupancy rates for office and retail space. Especially hurt in pandemic times will be big cities like New York City and San Francisco that depend substantially on their downtown retail economies, she predicted. Wachter shared her insights on the outlook for 2022 in a recent interview on Wharton Business Daily on SiriusXM .

Wharton School of the University of Pennsylvania - Knowledge@Wharton
What's Ahead for the U.S. Economy in 2022
11 January 2022

The Federal Reserve must get "more aggressive" in 2022 by increasing interest rates and tapering down asset purchases in order to tame inflation, according to Wharton finance professor Jeremy Siegel . "The Fed is way behind the curve … and should have started raising interest rates by now," he said on the Wharton Business Daily show on SiriusXM as he forecast market and economic trends for 2022. (Listen to the full podcast above.) Siegel predicted the Dow and the S&P 500 will continue to climb in the year ahead, albeit at a slower pace than in 2021. The stock markets will face some headwinds when the Fed raises rates, but "stocks are real assets, and you want to hold real assets when there is inflation," he said.

Asian Development Bank
Digital Technologies for Government-Supported Health Insurance Systems in Asia and the Pacific
22 December 2021

DIGITAL TECHNOLOGIES SAMPLE OF A TWO-DECK FOR GOVERNMENTPUBLICATION TITLE SUPPORTED HEALTH PUBLICATION SUBTITLE INSURANCE SYSTEMS IN ASIA AND THE PACIFIC JUNE 2021 DECEMBER 2021 ASIAN DEVELOPMENT BANK DIGITAL TECHNOLOGIES FOR GOVERNMENTSUPPORTED HEALTH INSURANCE SYSTEMS IN ASIA AND THE PACIFIC DECEMBER 2021 ASIAN DEVELOPMENT BANK Creative Commons Attribution 3.0 IGO license (CC BY 3.0 IGO) © 2021 Asian Development Bank 6 ADB Avenue, Mandaluyong City, 1550 Metro Manila, Philippines Tel +63 2 8632 4444; Fax +63 2 8636 2444 www.adb.org Some rights reserved. Published in 2021.

MIT Sloan Management Review
How Marketers Can Address Data Challenges to Drive Growth
08 December 2021

Connecting With Customers in the Age of Acceleration The pandemic forced companies to speed digital transformation and adapt to a virtual world. Customers are now rewarding those that offer the best experiences and engage authentically. To succeed in the next era, businesses and marketers must meet new expectations and build new strategies and skills. Imagine that you have just been promoted to manager at a large food company and will be in charge of a popular candy brand primarily sold in grocery stores.

Harvard Business School Working Knowledge
The Popular Stock Metric That Can Lead Investors Astray
06 December 2021

What if a bedrock method that investors have relied on for decades to find cheap-but-promising stocks to buy low and sell high no longer works well? The book-to-market ratio has been used since at least the Great Depression to identify undervalued stocks. It has become so detached from a modern economy driven by research and intellectual property that it no longer accurately signals so-called value stocks, suggests new research from charles c.y. Wang, Harvard Business School's Glenn and Mary Jane Creamer Associate Professor of Business Administration. Investors use book-to-market ratios to spot potentially underpriced stocks, and major stock indexes and institutional investors lean on the metric as well.

Corporate Risk Management

For boards, the volatility of risk scenarios is only increasing

Every organization is confronted with some type of risk - operational, financial, technological, environmental, regulatory - which can have devastating consequences. Effective corporate governance requires continuous and systematic management of all types of risk, both current and anticipated. First, risks must be prioritized, and here the board of directors can play a key role by deciding in what priority they should be addressed, what is to be deemed simply unacceptable, and how they should be addressed from a structural perspective. For example, evidence gathered from the 2007 global financial meltdown indicates that banks with boards that had identified a need to establish a separate risk management committee managed the crisis better than those with integrated committees. The benefits of this type of separation have become only more evident as fiduciary duties have come to include oversight of a broad range of matters, including compliance with international accounting rules and stability measures that require banks to set aside capital in case of potential losses. Implementing a robust risk management system requires the integration of different parts of an organization, including the board's risk committee, internal auditing, finance, legal, and operations.

Increasingly complex and rapidly changing economic, environmental, social, and technological conditions have multiplied potential risk scenarios. Worsening climate change, geopolitical tensions, trade wars, and social upheaval like the protests that spread in Hong Kong in 2019 require corporate governance that is proactive when it comes to identifying risks and addressing them. Determining an appropriate board structure and approach to risk management will depend upon both a company's industry and stage of its life cycle; risk exposure is very different for financial institutions than it is for petrochemical firms. Even within the financial sector, different approaches are required - from insurers exposed to extreme weather events related to climate change, to retail banks making loans to small businesses during volatile periods. Organizations are dealing with complexity and litigiousness like never before, forcing their boards to assess current and past organizational exposure. Still, there are some strategic advantages to taking risks; after all, achieving sustained growth requires some degree of risk-taking. Incorporating risk management into corporate strategy is therefore crucial.

Related insight areas: Illicit Economy, Cybersecurity, International Security, Financial and Monetary Systems, Development Finance, Climate Change, Corruption, Risk and Resilience, Civic Participation, Insurance, Justice and Law, Banking and Capital Markets

Australian Institute of International Affairs
The World's Oldest Democracy Debates How It Functions
19 January 2022

President Biden's speech to Atlanta last week saw a renewed focus on protecting the "heart and soul" of American democracy – voting rights. What does this strategy reveal about Biden's plans for 2022?.

Wharton School of the University of Pennsylvania - Knowledge@Wharton
How Risk-shifting by Underperforming Funds Distorts Stock Prices
18 January 2022

As fund managers of laggard mutual funds try to catch up with their peers, they tend to pursue high-risk stocks that may give higher than average returns. In the process, they push the prices of those risky stocks disproportionately higher than what the returns may justify, according to a new research paper by experts at wharton and elsewhere. The research explored the relationship between risk-shifting by underperforming mutual funds and "risk anomalies" such as subpar risk-adjusted performance of stocks with high market betas, or high volatility.

Project Syndicate
Capital Is Not a Strategy
06 January 2022

After years of central banks keeping interest rates low and pumping liquidity into financial markets, asset valuations are at historic highs. While entrepreneurs and venture-capital founders tell themselves that "capital is a strategy," bubble finance is no substitute for a business plan that can achieve positive cash flow.

University of St. Gallen
Do CEOs really stay in the job for too long?
20 December 2021

20 December 2021 . How long should CEOs remain in office? Do some of them stay on for too long? This is an ongoing debate among academics and practitioners, often triggered by headlines about long-serving CEOs who perform badly and destroy company value. A recent example is Société Générale's Frédéric Oudéa, who is currently the longest-serving CEO of a major European bank despite having overseen a 75% drop in the company's share price during his 13-year reign, giving it the lowest price-to-book ratio of any European bank.

VoxEU
Socially responsible investors amplify the positive externalities of regulatory enforcement
08 December 2021

Whether socially responsible investors have any impact on the environmental, social, and governance policies of portfolio firms has become a much-debated issue. This column shows that firms reduce emissions at their local plants following enforcement actions by the US Environmental Protection Agency against nearby plants of firms operating in the same market, and that the emissions reduction is twice as large if a nearby 'socially responsible' mutual fund owns shares of the parent firm of the peer plants. The threat of exit by these funds appears to have real consequences for how the local plants respond to the enforcement action.

Project Syndicate
Building a One-Earth Balance Sheet
30 November 2021

While all politics is local, it is shaped by a fast-changing global landscape. Only a one-Earth balance sheet – a bottom-up reset of how we measure global wealth – can ensure that countries work toward a better future for all.
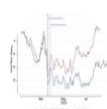
VoxEU
Bank leverage constraints and bond market illiquidity during the COVID-19 crisis
27 November 2021

The onset of COVID-19 led to heightened uncertainty and a 'dash-for-cash', particularly in the mutual fund sector which faced fire sale pressure. Typically, banks trading securities absorb such pressure and support market liquidity, but regulation may limit their ability to do so. This column analyses the role of bank leverage constraints as an amplifier of bond market illiquidity. It concludes that leverage ratio regulation can have negative side effects by increasing bond market illiquidity in times of economic distress, suggesting that the optimal leverage ratio is procyclical.

Identity Fraud and Cyber Resilience

The increasing amount of personal data being collected and exploited creates security challenges

The growing use of digital identities online - in combination with the massive amount of personal data increasingly being collected by governments, businesses, and everything from wearable devices to household appliances - creates significant vulnerabilities. According to the Identity Theft Resource Center, more than 300 million people had their identities compromised between January and September of 2020 alone, and high-profile breaches have included the 533 million Facebook users who had their phone numbers and personal data leaked online in 2021. COVID-19 has accelerated the need for secure digital identity systems, and most organizations are concerned about the security risk involved in increased remote work during the pandemic. Cultivating trust in digital identity relies not only on ensuring privacy but also that data is being issued, shared, and verified in trusted ways through certified authorities. Other approaches for better securing identities and building resilience and trust include keeping data collection to a minimum, alongside disclosure and informed consent. Bolstering digital literacy and helping people better understand the need for password-free, multi-factor authentication can also help.

Security is essential for trusted digital interaction and must be directly embedded in the design of digital identity systems - especially amid the growing use of biometrics. The World Wide Web Consortium, the US National Institute of Standards and Technology, and the Financial Action Taskforce have defined standards for digital identity security, and the app "itsme" uses elements such as multifactor authentication criteria including biometrics, a mobile phone number, and a SIM card linked to the user - along with a personal code. For the Internet of Things, the European Telecommunications Standards Institute has endorsed security-by-design principles - like ensuring devices are not pre-set with passwords, providing a point of contact for issues, and opting into timely software updates. Completely infallible security is impossible, and security is more of a process than a state of being. Stakeholders in all sectors and industries should take proactive design and policy steps to protect digital identities and personal data in order to regain user trust, provide regulatory, certification and control mechanisms, address data breaches, harmonize standards, and encourage digital skills training.

Related insight areas: Cybersecurity, The Digital Economy, European Union, COVID-19, Blockchain, Risk and Resilience, Justice and Law, 5G, Internet of Things, Future of Computing, Innovation, Internet Governance

VoxEU
Pulse as a biometric measure of wellbeing
11 January 2022

Pulse rates have been overlooked as a potentially valuable way of capturing individuals' wellbeing. The value of pulse rate as a wellbeing metric is that, unlike subjective wellbeing metrics, it is recorded on an objective cardinal scale. This column uses empirical analyses of the English and Scottish Health Surveys and the 1958 National Child Development Study to show pulse is highly correlated with subjective wellbeing, that pulse equations look very similar to those for subjective wellbeing, and that pulse is predictive of subjective wellbeing and labour market outcomes later in life.

Social Europe
Online surveillance thrives when fear takes over
05 January 2022

European law-enforcement agencies have been pushing to end encryption and survey everyone's online communications. LuckyStep/shutterstock.com In 2020, the European Commission put forward temporary legislation on 'chat control'. This sought to legalise the scanning of everyone's private online communications —every message, email or chat. Successor to a long line of attacks from governments on the encryption of online communications, it raised concerns among privacy activists with its potential to spark a new such 'cryptowar' .

Asian Development Bank
Harnessing Digitalization for Sustainable Economic Development: Insights for Asia
24 December 2021

Harnessing Digitalization for Sustainable Economic Development: Insights for Asia describes digitalization's role in raising the productive capacities of economies. It examines how digital transformation can enhance trade, financial inclusion, and firm competitiveness, as well as how greater digital infrastructure investment, internet connectivity, and financial and digital education in the region can maximize digitalization's economic benefits. It also explains the importance of striking the right balance between the regulation and supervision of financial technology to enable innovation and safeguarding financial stability and consumer protection. Part I of the book seeks to build an understanding of digitalization's effects on macroeconomic performance, including through trade channels and financial inclusion.
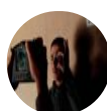
Project Syndicate
The Danger of Digitalizing Aid
20 December 2021

The humanitarian aid sector faces growing pressure to innovate and adopt digital technologies, reflecting the urgent need to make such assistance more effective. But the world's most vulnerable communities must not be forced to make themselves visible to governments that may not have their best interests at heart.

Social Europe
Towards transparency by design in the EU
20 December 2021

Citizens must have access to information to engage with the democratic life of the union, the European ombusman argues. A meeting of the Council of the EU—positions adopted by member-states are not accessible Twenty years ago the European Union ushered in a far-reaching and progressive piece of legislation, soon known as the 'transparency law'. While not perfect, it became a cornerstone of efforts to make EU institutions more accountable by giving concrete expression to the right of public access to their documents. Over the years, this right was enshrined in the treaties while European case law further defined its scope.

CyberPeace Institute
Four Calls to World Leaders for 2022
17 December 2021

The impact of cyberattacks on people's lives is increasing. It's time for more action from governments, whose role it is to provide security for their citizens. Here are four calls […] The post Four Calls to World Leaders for 2022 appeared first on CyberPeace Institute .

ITU
Measuring digital development: Facts and figures 2021
16 December 2021

ITU's Measuring digital development: Facts and figures 2021 offers a snapshot of the most important ICT indicators, including estimates for the current year. Latest figures show that an estimated 4.9 billion people are using the Internet in 2021, or roughly 63 per cent of the world's population. This is an increase of almost 17 per cent since 2019, with almost 800 million people estimated to have come online during that period. The statistics reveal a connectivity 'grand canyon' separating the digitally empowered from the digitally excluded, with 96 per cent of the 2.9 billion still offline living in the developing world. Location plays a big part: our figures reveal that the share of Internet users in urban areas is twice as high as in rural areas.

Trust and Privacy

Trust in data-based applications is diminishing, as privacy concerns are not effectively addressed

Global dialogue around the governing and safeguarding of personal data is polarized. The often conflicting objectives of governments, businesses and private citizens result in a complicated and often emotional discourse – which hinders informed decision-making.

Personal data is increasingly seen as a pervasive, 21st-century asset class, like a stock or bond. That comes as business models are being built around unprecedented opportunities to create value through the flow of such data. According to the 2014 World Economic Forum report Personal Data: The Emergence of a New Asset Class, trust between individuals, governments and companies is necessary in order to fully unlock its potential.

Yet there is a crisis of trust, as stakeholders struggle to agree upon a personal data framework that is reliable and fair. Existing legal frameworks will prove inadequate, due to the speed of change and uncertainty about appropriate rights and responsibilities. The establishment of effective new frameworks must involve a truly democratic approach, if the public's trust in data governance is to be restored.

Related insight areas: Fourth Industrial Revolution, The Digital Economy, Cybersecurity, Internet Governance, Future of Media, Entertainment and Sport, Values

London School of Economics and Political Science

Investment in technology is not enough to guarantee e-participation in politics

24 January 2022

There have been a number of efforts to promote 'e-participation' in politics to give citizens a better voice in policymaking. Yet the success of these initiatives has varied substantially across the world. Pragati Rawat and John C. Morris argue that investment in technology alone is not enough for citizens to embrace these new avenues for … Continued.

Greater Manchester Combined Authority

CASE STUDY: Helping Wythenshawe residents develop their digital skills

17 January 2022

Wythenshawe Community Housing Group's Digital Inclusion Officer runs free training support sessions at several locations around Wythenshawe. These sessions include drop-in computer classes, basic digital skills training and sessions supporting residents to complete benefits forms, Universal Credit and Visa applications online. Stories and experience of some beneficiaries are presented.
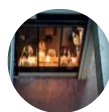
World Economic Forum

4 ways to promote workforce equality in the new digital economy

13 January 2022

The COVID-19 pandemic and the rise of automation have increased the significance of the new digital economy, impacting both the supply of and demand for jobs globally. Governments, businesses and higher education institutions must co-operate to build more equality into the workforce as it adapts to suit the new digital economy. Many organisations are partnering on technology-based solutions and moving from ideas to action to train and upskill employees in this new era. The combined forces of automation and the pandemic have profoundly reshaped the labour market, displacing millions of workers, disrupting local economies, and worsening social inequities worldwide. Today's workplace requires modern skills and workers are looking for well-paying careers with mobility and remote work potential.

World Economic Forum

Stakeholder Capitalism | EP4 - Tech for Good: Promise & Peril | World Economic Forum

08 January 2022

While the value of big tech companies has soared, what problems has that created? A lack of market competition and the impact that has on economies; data protection concerns; falling public trust. Is big tech too big, and what should be done? Guests: Zia Qureshi, fellow at the Brookings Institute; Marietje Schaake, International Policy Director at the Cyber Policy Center of Stanford University.

The Conversation

Six Big Digital Trends to Watch in 2022

01 January 2022

According to recent McKinsey research, 2021 was a year of transformation: people, corporations and society began to look ahead to influencing their futures rather than just surviving the present. It was the year that premature hopes for herd immunity, an end to pandemic lockdowns, and a return to normality were dashed at least for now. Aside from the great social media resignation, during which burnt-out gen z workers quit their jobs on tiktok and instagram, the rise of non fungible tokens (nfts), and the introduction of the metaverse, the world's space-going billionaires were as wealthy and productive in business and technology as ever. While it's hard to make accurate predictions in the unpredictable environment we've been experiencing over the last two years, the year ahead will bring many surprises.

RAND Corporation

Cognitive Behavioral Intervention for Trauma in Schools (CBITS) for American Indian Youth

22 December 2021

The Cognitive Behavioral Intervention for Trauma in Schools (CBITS) program helps students exposed to traumatic events who are experiencing emotional or behavioral problems. This tool is an adaptation of the CBITS program for American Indian youth.

Cyber Resilience

Accelerating digitization prompts a need for integrated defense, prevention and response

Cyber resilience, or shielding critical systems from hackers or internal failures, is an increasingly important strategic goal in a world of fast, cheap technologies that deliver both unprecedented benefits and risks.

A common denominator for any proper resilience approach is a deep understanding of the risks associated with particular business models. This means that companies must go beyond traditional information-technology planning and make risk evaluation a regular part of their strategy – particularly as they integrate emerging technologies such as artificial intelligence or quantum computing.

Because of the global scope of modern, private sector IT networks, their digital security is a public good. The public sector has its own responsibility to ensure that its institutions also incorporate digital resilience. That's because the risk of the misappropriation of digital public infrastructure, like smart electrical grids or communications devices embedded in roads, will only increase over time. Governments and private actors must work together, to develop new ways to sufficiently protect their digital domains.

Related insight areas: Future of Computing, Fourth Industrial Revolution, Cybersecurity, Internet Governance, The Digital Economy, Infrastructure, Artificial Intelligence, Risk and Resilience

VoxEU
Consumption inequality in the digital age
21 January 2022

When considering the effect of digitalisation on inequality, researchers usually focus on income inequality. This column compares the consumption baskets of US households to study the effect of digitalisation on consumption inequality. High-income households have a higher share of ITC-intensive products in their consumption, and thus benefit more from price declines in these goods due to digitalisation. The price channel accounts for 22.5% of the increase in consumption inequality between 1960 and 2017.

VoxEU
Opening the black box of hospital mergers
16 January 2022

Despite the current wave of US hospital mergers, it is unclear how they change behaviour and performance. This column 'opens the black box' of hospital practices by analysing a mega-merger between two for-profit chains. Benchmarking the merger's actual effects against the acquirer's stated aims, its shows that while the merger achieved some goals – harmonising electronic medical records and sending managers to target hospitals – it produced few gains in overall performance. Further research is needed into the impact of mergers on the healthcare industry specifically and the economy more broadly.

Asian Development Bank (ADB)
DigitalxADB: Building Innovation Ecosystems in Developing Asia and the Pacific
12 January 2022

Venture-stage investor Linh Thai hosts a panel discussion exploring why startup ecosystems are so valuable for sustainable development, and what the Asian Development Bank is doing – and can do – to support their growth. ADB produced this talk show as part of its DigitalxADB 2021– an event series aimed at raising awareness and build broad consensus within ADB to continue focusing on the digital opportunities that lie ahead in a world reshaped by COVID-19.

World Economic Forum
Preparing for the 'New' Future of Work | Sustainable Development Summit 2021
02 January 2022

The live session is available for eligible participants on TopLink; the first part will be webcast to all shortly after the session ends. Industry-led and country collaboration could reduce reskilling costs and times by 30%, enabling nearly half of the disrupted workforce to be reskilled by employers, with a positive cost-benefit balance. Speakers: Sally Bundock, Gog Soon Joo, Dan Rosensweig, Mona Mourshed, Jeff Maggioncalda, Gabriel Dalporto, Robert E. Moritz, Andrew Baird.

The Conversation
Diversity in the workplace must be matched with an atmosphere of genuine inclusion
23 December 2021

The idea that greater diversity in the workplace is good for business seems to be gaining ground. In a recent major step in December 2021, BT announced plans for 25% of its workforce to be from "non-white backgrounds" by the end of the decade. Yet taking steps to increase the representation of minority ethnic groups (and women) in areas of employment from which they have been historically excluded is not without its committed critics. Objections are raised by those who believe such moves violate the logic of meritocracy – that roles should be won regardless of ethnicity or sex. Meanwhile, supporters of active pro-diversity policies and affirmative action see such steps as a way of remedying decades of unfairness.

The Tokenist
2021 Has Been The Year Of ETFs, With 445 Debuting
21 December 2021

445 Exchange Traded Funds made their debuts in 2021, making it a record year for the $7 trillion industry. The post 2021 Has Been The Year Of ETFs, With 445 Debuting appeared first on The Tokenist .

World Economic Forum
How to overcome mistrust of data
15 December 2021

The data ecosystem is vast and complex even for seasoned professionals, but more so for average individuals who act as users. The majority of consumers are starting to believe that companies benefit more from their data than they do. Without trust, individuals are less likely to share data. This is why it's crucial to rethink consent management. The data ecosystem is vast and complex.

Cybercrime

The nature of ransomware attacks has shifted from annoyance to the disruption of key infrastructure

The annual cost of cybercrime will likely increase by 15% every year until it hits $10.5 trillion in 2025, according to one estimate. An increasingly connected world brings with it unprecedented cyber challenges, potentially impacting just about every type of digital operation, undermining financial stability and security, and robbing us of our privacy. News stories about data breaches, ransomware, and malware attacks are a seemingly daily occurrence, and the criminal compromise of the digital devices and networks we now depend upon severely diminishes their reliability - and the trust we place in them. Everyone and every organization is a potential cybercrime victim; as people and businesses demand greater efficiency and productivity through internet-connected devices, what is collected for analysis can be targeted by cyber criminals - for leverage, to inflict damage, or to steal money (indeed, just as Willie Sutton once robbed banks because "that's where the money is," the digital world now fills that role). In the wake of COVID-19, many people have only increased their online presence for remote work purposes or entertainment, creating even bigger targets for criminal activity.

As a growing universe of connected Internet of Things devices has increased the number of available digital targets for would-be attackers, it has also amplified the ability to inflict harm more broadly and deeply. Gartner has estimated that there are now some two billion IoT devices in operation, and high-profile examples of damage inflicted through these targets include the Mirai botnet - which compromised more than 600,000 of them, including cameras, routers, and network storage devices (it then leveraged its control of the devices to launch distributed denial-of-service attacks on a variety of organizations). Researchers at Verizon have found that nearly a third of all malware now being discovered is ransomware; the nature of attacks has meanwhile shifted from pervasive annoyance to the significant disruption of key infrastructure. This was underscored by the Colonial Pipeline and JBS Foods ransomware incidents in 2021 - both organizations capitulated to attackers and paid out millions of dollars (though much of what Colonial Pipeline paid was later recovered). Cybercrime is clearly not going away anytime soon, and people and businesses should prepare for how to best deal with it.

Related insight areas: Justice and Law, COVID-19, Illicit Economy, Global Governance, Values, Internet of Things, Banking and Capital Markets, Internet Governance, Retail, Consumer Goods and Lifestyle, Corruption, Geopolitics

Trust, Security and Regulation Briefing, January 2022

World Economic Forum
What you need to know about cybersecurity in 2022
18 January 2022

The COVID-19 pandemic has expedited the use of digital tools in business and the home. These advances in digitalization have led to increasingly frequent, costly and damaging cyber incidents. The World Economic Forum's Global Cybersecurity Outlook 2022 presents critical findings from 120 global cyber leaders on how to shift from cybersecurity to cyber resilience. Digitalization has increased during the COVID-19 pandemic. The global use of services such as video conferencing has grown tenfold .

CoinDesk
Kosovo Moves to Ban Crypto Mining in Face of Energy Crisis
04 January 2022

Artane Rizvanolli, the eastern European country's economy minister, acted on the advice of the Technical Committee for Emergency Measures in Energy Supply on Dec. 31 as part of a set of relief measures. The government declared a state of emergency in December lasting for 60 days, allowing it to allocate more money for energy imports and introduce power cuts, according to a report by the Gazeta Express. .

Harvard Kennedy School - Belfer Center for Science and International Affairs
How Corporate Intelligence Teams Help Businesses Manage Risk
04 January 2022

The word "intelligence" is loaded: While some confuse it with corporate espionage, today nearly every major company has an intelligence function or is building one. Prior to Covid-19, many corporate intelligence teams largely focused on security, but the pandemic has demonstrated the broader value of intelligence. In a world of contradictory and misleading information, smart business leaders use intelligence to see around corners, mitigate risk, provide insight, and shape their decision-making. Paul Kolbe and Maria Robson Morrow offer an overview of corporate intelligence functions and provide advice on how to structure these internal teams.

Scientific American
Hacking the Ransomware Problem
03 January 2022

During a ransomware hack, attackers infiltrate a target's computer system and encrypt its data. They then demand a payment before they will release the decryption key to free the system. This type of extortion has existed for decades, but in the 2010s it exploded in popularity, with online gangs holding local governments, infrastructure and even hospitals hostage. Ransomware is a collective problem —and solving it will require collaborative action from companies, the U.S. government and international partners. In 2020 the Federal Bureau of Investigation received more than 2,400 reports of ransomware attacks, which cost victims at least $29 million, not counting lost time and other resources.

Harvard Kennedy School - Belfer Center for Science and International Affairs
Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity
01 December 2021

Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity is a practical leadership guidebook outlining a new strategy for improving organizational cybersecurity and mitigating cyber risk.

Harvard Business School Working Knowledge
5 Principles for Scaling Change from IBM's High School Innovation
18 November 2021

P-TECH has bolstered graduation rates for students of color while creating a new tech hiring pipeline. Rosabeth Moss Kanter and program architect Stanley Litow discuss the social impact lessons for other organizations.

Project Syndicate
A Strategic Compass for Europe
12 November 2021

The European Union is at risk of "strategic shrinkage," owing to geopolitical, economic, and ideological pressures from all sides. Safeguarding European citizens, interests, and values will require new thinking about the EU's security and defense responsibilities and the capacities it needs to fulfill them.

Data Ethics, Values and Norms

Data can be deployed to solve global problems and achieve the SDGs, with the right oversight

The development and deployment of any emerging technology keys on social values, preferences, and ethical norms. It is important for organizations to understand these factors in a local context before formulating how they will govern data and artificial intelligence; in addition to whether local values and norms are adequately reflected, they should seriously consider the interplay between technology and individual rights, and how to put safeguards in place that incentivize responsible and human-centric development. Ensuring the trustworthiness of an organization's data practices is essential, often for practical reasons; for example, Facebook was sued in the US in 2019, after the Department of Housing and Urban Development alleged the company was violating a prohibition on housing discrimination because its machine learning algorithms functioned like an advertiser that excludes users based on race, ethnicity or religion. Certain foundational elements should be considered at the start of commercial projects: privacy, accountability, safety and security, transparency and explainability, fairness and non-discrimination, human control of technology, professional responsibility, and the promotion of human values. Understanding these in the relevant context is necessary for responsible data use.

By using data responsibly, businesses, non-profits, and governments can better address many of the unprecedented social and environmental challenges we now face - not least current and future pandemics, and environmental disasters aggravated by the worsening impacts of climate change. For example, artificial intelligence can play a significant role in achieving the UN Sustainable Development Goals - one study published in 2020 found that AI can enable the accomplishment of 134 targets across all 17 global goals if its development is supported by the necessary regulatory oversight (though it may also inhibit 59 targets). Some of the levers at hand that can help facilitate the use of data for good include global digital trade, the facilitation of equitable access to data flows, and responsible data collection. Technical elements such as data portability and interoperability are also important. The need to mitigate risks calls for putting firm safeguards in place related to cybersecurity, encryption, risk management, accountability, and overall data protection. Some uses of data and machine learning present particular sets of risks, like privacy breaches and phishing attacks.

Related insight areas: Internet Governance, Risk and Resilience, Artificial Intelligence, Sustainable Development, Social Justice, Pandemic Preparedness and Response, Cybersecurity, COVID-19, Values, Climate Change, Corporate Governance, Agile Governance, Systemic Racism, Justice and Law

World Economic Forum

Special Address by Xi Jinping, President of the People's Republic of China | Davos Agenda 2022

17 January 2022

Special Address by Xi Jinping, President of the People's Republic of China with Klaus Schwab at the World Economic Forum's Davos Agenda 2022. .

World Economic Forum

We're failing at the ethics of AI. Here's how we make real impact

14 January 2022

The global COVID-19 crisis has acted as a world-wide accelerator for the rollout of artificial intelligence (AI) initiatives. The ethics and governance of AI systems are unclear. We need to advance in three main issues to make a real impact. The global COVID-19 crisis has acted as a world-wide accelerator for the rollout of AI initiatives. Technologies that would've taken place over five years have taken place over six months .

Harvard Business School Working Knowledge

Can Entrepreneurs and Governments Team Up to Solve Big Problems?

11 January 2022

Shield AI's quadcopter, with no pilot and no flight plan, could clear a building and outpace human warfighters by almost five minutes. It was evidence that autonomous robots could help protect civilian and service member lives. But was it also evidence that Shield AI—a startup barely two years past founding—could ask their newest potential customer, the US government, for a $50 to $60 million contract for a system of coordinated, exploring robots? Or would it scare them away? Harvard Business School professor Mitch Weiss and Brandon Tseng, Shield AI's COO and co-founder, discuss these and other challenges entrepreneurs face when working with the public sector, and how investing in new ideas can enable entrepreneurs and governments to join forces and solve big problems in the case, "Shield AI.".

Sustainable Development Solutions Network

2022 Predictions For The Evolution of Data Use

30 December 2021

At this time of the year, there is no shortage of predictions of what lies ahead. Typing "year ahead 2022" into your web browser alone yields 885 million results - more than one for every ten people on the planet. And for big data enthusiasts, limiting the search terms to "year ahead," "big data," and "2022" returns 300,000+ articles covering data trends, top tech predictions, and what we can expect from big data analytics. The results are spottier, however, when we search for what's in store for national data ecosystems and the implications for sustainable development. Yet, efficient national data ecosystems and better use of data are critical to helping organizations from the public sector, private sector, and civil society achieve better outcomes, particularly in sustainable development.

Wired

The James Webb Space Telescope Finally Prepares for Launch

23 December 2021

+++lead-in-text In the mid-1990s, a team of scientists proposed developing a next-generation infrared space probe. Nearly three decades later, after overcoming engineering, logistical, and political challenges, the ambitious spacecraft envisioned as [Hubble's successor] (https://www.wired.com/story/nasa-tries-to-save-hubble-again/) will finally blast off. Dubbed the James Webb Space Telescope, or JWST, in honor of a former NASA administrator, it comes packed with the biggest mirror ever to fly in space, a huge sunshield, and a suite of cutting-edge instruments that will enable it to find new life-friendly planets, reveal the births and deaths of stars, and probe the early years of the universe.

London School of Economics and Political Science

2021 In Review: The Culture of Academic Publishing

22 December 2021

Responding to the necessities of the COVID-19 pandemic and the accelerating application of the open paradigm to more and more aspects of research, academic publishing and the cultures that support it continue to be in flux in 2021. This review brings together posts focused on the way in which the publication of research has developed … Continued.

Corruption and Impunity

When illicit trade is allowed to flourish, it spawns a culture of impunity

Organized crime and illicit economies are increasingly prominent sources of political corruption, as criminal networks pour money into parties and forge alliances with officials and their intermediaries. Transnational organized crime generates an estimated $870 billion in annual revenue, and about one third of organized crime groups surveyed by the United Nations have political influence at the local level, according to a report published in 2016 by the Global Initiative against Transnational Organized Crime. Transactional corruption of law enforcement and public officials diverts resources from the state, and increasingly, in countries with poor institutions, the receipt of a bribe is perceived as a right of office - while payment of a bribe is seen as a cost of doing business. This has generated distrust in politicians, distorted markets, undermined public infrastructure, and disengaged citizens. During the 2014 regional elections in Peru, for example, the Ministry of the Interior announced that 124 candidates had links to drug traffickers - yet, 14% of those candidates were ultimately elected, according to the Global Initiative against Transnational Organized Crime's 2016 report.

Crime and corruption are further facilitated by the decline of stigma associated with illegal acts; illicit activity is regularly used to gain political power, or to buy legitimacy with the public. A lack of law enforcement, penalties, or any deterring government presence at all runs the risk of increasing complicity over time. In Afghanistan, for example, the lack of a state presence is thought to be the most important contributing factor to the rampant opium production in the southwestern provinces of Helmand, Kandahar, Nimruz, and Farah, according to the Global Initiative against Transnational Organized Crime's report. In many areas of Afghanistan, the Taliban has taken advantage of the lack of state security to become the security provider itself, and its drug-related income - from both smuggling and protecting fields from police scrutiny - has been estimated to be as much as $155 million annually, according to the report. The high-level business and government officials who enable criminal behaviour through neglect or complicity are exacting heavy cost on the rest of us; the annual cost of corruption in the form of bribery and theft amounts to about $3.6 trillion, according to a UN estimate published in 2018.

Related insight areas: Corruption, Justice and Law, Corporate Governance, Agile Governance, Civic Participation, Taxes, Human Rights, Global Governance, Social Justice, Risk and Resilience, Public Finance and Social Protection, Economic Progress

Trust, Security and Regulation Briefing, January 2022

World Economic Forum
Stakeholder Capitalism - EP.5 | Stakeholder Capitalism at Work | World Economic Forum
13 January 2022

In this concluding episode we ask how can the idea of 'stakeholder capitalism' work in the real world. Joining hosts Peter Vanham and Natalie Pearce are: Emily Bayley, project lead of the World Economic Forum's ESG Initiative Jonas Prising, CEO of Manpower Group Geraldine Matchett, CFO and co-CEO of Royal DSM .

London School of Economics and Political Science
What causes regime change in African autocracies?
13 January 2022

Drawing on these insights, our paper seeks to explain political change in African competitive autocracies using the notion of 'regime cycles'. This framework, which produced rich insights into the failed democratisation processes of the post-communist states during the 1990s, applies a logic of collective action to analyse elite behaviour, identifying four stages within a regime cycle. Each stage of the cycle is determined by the nature of contestation between the incumbent and senior elites. The balance of power between these actors varies in each stage, according to the level of fragmentation of authority within and across those groups. The four stages, which do not necessarily follow a chronological order, include accommodation, consolidation, factionalisation and crisis.

Social Europe
Tax justice—a crucial tool to advance human rights
10 December 2021

Magdalena Sepúlveda is executive director of the Global Initiative for Economic, Social and Cultural Rights and a member of the Independent Commission on International Corporate Tax Reform (ICRICT). From 2008 to 2014 she was United Nations rapporteur on extreme poverty and human rights.

Chatham House
Diagnosing social behavioural dynamics of corruption
08 December 2021

Diagnosing social behavioural dynamics of corruption Other resource dora.popova 8 December 2021 This interactive toolkit identifies the types of social expectations which sustain selected corrupt practices and provides behaviourally-informed recommendations for changing them. When tackling a problem as complex as corruption, it is important to understand why and how people behave in different situations where corruption occurs. In contexts where it is easier to engage in corruption than avoid it, identifying the social expectations and informal rules which sustain corrupt practices can advance corruption prevention and deepen collective action.

European University Institute
Understanding the future of European Union counter-smuggling policy : the renewed EU action plan against migrant smuggling (2021-2025)
29 November 2021

Political contention surrounding 'irregular migration' in recent years has instigated national and multilateral government authorities to develop new transnational approaches to counter-smuggling policy. Contemporary migration movements result from disparate catalysts, extending far beyond direct personal persecution, thereby rendering existing asylum policies ill-equipped to accommodate modern mixed migration movements. This article argues that European Union (EU) approaches to counter-smuggling policy prioritise preventing spontaneous arrivals and restricting individuals' access to humanitarian protection systems.

Social Europe
Matteo Salvini's League and the price of unbridled populism
24 November 2021

Valerio Alfonso Bruno is a political analyst and senior fellow at the Centre for Analysis of the Radical Right (CARR), also involved with the ASERI at the Università Cattolica of Milan and the Observatoire de la Finance (Geneva). Vittorio Emanuele Parsi is an international relations professor and director of the Advanced School in Economics and International Relations (ASERI) at the Università Cattolica of Milan, author of Vulnerable: How the Pandemic Will Change the World and a columnist for Il Messaggero.

Privacy Forensics

New techniques offer an opportunity to address the asymmetry at the heart of the privacy problem

The fundamental asymmetry between users and platform owners when it comes to privacy has been a central theme for internet governance. The current state of play allows for little governance, per se; platform owners largely remain unchallenged, since governance institutions can only request information about abuse from the platform owners themselves. Core to this asymmetry is that governance institutions (whether national or supranational) frequently suffer from a lack of substantial independent evidence of non-compliant or even illegal behaviour. And the asymmetry is not only exploited by multinational actors, but also by smaller, local players who are able to harm people or companies without leaving an accessible trail of forensic evidence. Privacy and security are not the only areas where this disparity is present - algorithmic discrimination also requires urgent redress. Some researchers have highlighted Google AdSense's discrimination as it delivers targeted advertising, for example. Safiya Umoja Noble, an American academic and author, has compiled cases of such algorithmic discrimination through interviews and open-source information, highlighting instances where the "value-laden choices of algorithms" promote "oppressive and discriminatory" outputs.

Companies with a global presence are often able to evade and mitigate oversight. For these companies to be identified, investigated, and monitored, the collection of independent evidence is necessary. This is likely to require independent monitoring by organizations with the necessary tools to monitor platform behaviour, surveillance, and abuse in real time - and in a way that yields forensic evidence for use in litigation and scientific measurement. As independent researchers have observed, particularly in the US and Germany, the arrival of the European Union's General Data Protection Regulation (GDPR) and the California Privacy Act (CCPA) have resulted in a growing number of cases that make effective use of digital forensic evidence in data protection lawsuits - a trend only likely to increase as companies are forced to adopt "Digital Forensic Readiness." By consistently monitoring companies that mine user data, and by providing regulators with accurate reports on the state of online tracking, it is possible to apply a scalable means of redress. Ultimately, privacy forensics promises to address the lingering asymmetry between platforms and users.

Related insight areas: Future of Media, Entertainment and Sport, Economic Progress, Corporate Governance, United States, Geo-economics, Digital Identity, Values, Justice and Law, The Digital Economy, Agile Governance

Observer Research Foundation
The near future of international law in cyberspace: Contentions and realities
15 January 2022

This piece is part of the series, Technology and Governance: Competing Interests Both global leaders and international legal experts agree to the position that existing international law applies to cyber operations. Additionally, case law and advisory opinions derived from the International Court of Justice have proved useful as precedents determining the future debates on the matter. However, not every single detail of how international law and its specific bodies apply to cyber operations is figured out today. As michael schmitt, the director of the tallinn manual project has put it in a feature article , "the devil is in the details".
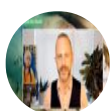
World Economic Forum
Deepfakes, cryptocurriences and misinformation: 2022's cybercrime predictions
31 December 2021

While cybercriminals continue to leverage the impact of the COVID-19 pandemic, they will also find new opportunities to attack such as deepfakes, cryptocurrency and mobile wallets.

World Economic Forum
Shaping a Responsible Data Ecosystem | Sustainable Development Summit 2021
29 December 2021

Every day the world generates 25 quintillion (and growing) data points, which could help shape post-pandemic societies for progress, people and the planet. What actions can organizations take at an individual and collective level to enhance data for development? Speakers: Gideon Lichfield, JoAnn Stonier, Quentin Palfrey, Erin Egan, Alain Bejjani .

Project Syndicate
Fixing Global Trade Finance
21 December 2021

The smaller the business, the more difficult it is to navigate the complexity, fragmentation, and opacity of today's trade-finance system. But more digital interconnection would greatly benefit micro, small, and medium-size enterprises and hence the global economy, too.

Electronic Frontier Foundation
Virtual Worlds, Real People: Human Rights in the Metaverse
10 December 2021

Access Now and the Electronic Frontier Foundation (EFF) are calling upon governments and companies to address human rights in the context of virtual and augmented reality (VR and AR) and ensure that these rights are respected and enforced.

UN Sustainable Development Goals
Internet Governance Forum promotes inclusive digital future for all
07 December 2021

The Internet Governance Forum (IGF) brings together more than 7,000 innovators, big tech executives, young people, ministers and parliamentarians to spur efforts to build an open, secure and free digital future for all. In his video message to the opening session on Tuesday, UN Secretary-General António Guterres spoke of how the COVID-19 pandemic has underlined the forum's theme of 'Internet United.

London School of Economics and Political Science
Cutting Edge Issues in Development – COVID-19, Corporatisation and Closing Space: The Triple Threat to Civil Society in India
01 December 2021

On Friday 26 November, Ingrid Srinath gave an online lecture on 'COVID-19, Corporatisation and Closing Space: The Triple Threat to Civil Society in India' as part of the Cutting Edge Issues in Development Lecture Series for 2021/22 . Ingrid Srinath is the Founder Director of the Centre for Social Impact and Philanthropy (CSIP) at Ashoka University. LSE ID's Professor David Lewis was an invited discussant for the lecture. Read what MSc students Ananya Radhakrishnan, Krithika Rao, Muskaan Arora and Bhuvan Majmudar took away from the lecture below. You can watch the lecture back on YouTube or listen to the podcast .

Cybersecurity and Regulation

The EU has provided a model for the evolution of cybersecurity regulation

Government authorities generally require organizations entrusted with data, regardless of industry or sector, to abide by rules intended to protect sensitive, high-value information and other cyber assets. The regulatory environment is fluid, however; it varies in terms of requirements, potential penalties, and execution. The definition of compliance also differs, depending on jurisdiction. The United Nations Conference on Trade and Development divides cybersecurity regulations into four basic categories: data protection/privacy laws, e-transaction laws, cybercrime laws, and consumer protection laws. Regulations aligned with these categories reflect global cybersecurity priorities: 82% of countries have laws governing electronic transactions, 80% formally identify and prosecute cybercrime, 66% address data privacy with specific laws, and 56% have codified online consumer protection. The European Union has served as an enviable model in terms of the evolution of cybersecurity regulation. In comparison with the US, for example, the EU's regulatory environment is generally built upon similar principles related to information-security measures. However, the EU faces additional challenges as it must try to accommodate a more diverse set of cultural, social, and strategic values across the bloc's 27 member countries.

The EU has sought to address cyber risk with policies including the Directive on Security of Network and Information Systems (the NIS directive), the Cybersecurity Act, and the General Data Protection Regulation (GDPR). While the NIS directive obliges member states to develop frameworks for cybersecurity practice, the Cybersecurity Act complements it with a certification framework. The GDPR marks the strongest step taken yet by any developed country to issue requirements for protecting consumer and user information from exploitation. In addition, the EU has established the European Union Agency for Cybersecurity (ENISA) to implement policies and assist member states during incidents. Other countries and regions have made similar attempts to codify rules and cybersecurity best practices, which continue to evolve amid a shifting technology environment. The vanguard of regulators continue to seek to implement ever-stronger reporting requirements, enhanced detection capabilities, data security and disposal rules, and cyber-crime prevention. This trend will persist as long as governments acknowledge the real potential for negative cyber outcomes. Some incidents, like data breaches, may never be meaningfully prevented - even as regulations continue to evolve.

Related insight areas: Global Governance, Future of Consumption, Justice and Law, European Union, Corporate Governance, Internet Governance, Future of Computing, Data Science, The Digital Economy, Agile Governance

World Economic Forum

How to make organizations cyber resilient in the digital frontier

05 January 2022

Cyber crimes are set to cost governments and organizations $10 trillion by 2025. As new cyber threats emerge, boards of directors must develop cyber risk plans to ensure their organizations have greater cyber resilience. Cyber risk strategies should align to financial analysis using clear and understandable language. In their 2020 Board of Directors Survey, Gartner, Inc. found that directors see cybersecurity as the second-greatest threat to their businesses, right after regulatory compliance risks. Cyber crime already cost the world at least $6 trillion in 2021 and could lead to over $10 trillion worth of annual damages by 2025 .

The Diplomat

Cyber Threats and Nuclear Weapons: Assessing Risks

20 December 2021

Trans-Pacific View author Mercy Kuo regularly engages subject-matter experts, policy practitioners, and strategic thinkers across the globe for their diverse insights into U.S. Asia policy. .

Raconteur

How to manage and mitigate cyber risk in an evolving threat landscape

16 December 2021

The pandemic necessitated greater collaboration to achieve fleet of foot within the National Healthcare System. The change prompted numerous digital solutions to be developed with trusted ecosystem partners, but more work now needs to be done to empower patients.

RAND Corporation

Wing-Level Mission Assurance for a Cyber-Contested Environment

09 December 2021

The authors offer ways to help wings assure their missions despite cyber attacks, focusing on how wings can maintain situational awareness, defend their systems, and respond to and recover from attacks to survive and operate when under cyber attack.

SpringerOpen

Detection of illicit cryptomining using network metadata

04 December 2021

Illicit cryptocurrency mining has become one of the prevalent methods for monetization of computer security incidents. In this attack, victims' computing resources are abused to mine cryptocurrency for the benefit of attackers. The most popular illicitly mined digital coin is Monero as it provides strong anonymity and is efficiently mined on CPUs.Illicit mining crucially relies on communication between compromised systems and remote mining pools using the de facto standard protocol Stratum. While prior research primarily focused on endpoint-based detection of in-browser mining, in this paper, we address network-based detection of cryptomining malware in general. We propose XMR-Ray, a machine learning detector using novel features based on reconstructing the Stratum protocol from raw NetFlow records.

The Conversation

Most common passwords of 2021: here's what to do if yours makes the list

18 November 2021

If you use "123456", "password" or "qwerty" as a password, you're probably aware that you're leaving yourself vulnerable to hackers. You're also not alone – these are three of the top ten most common passwords around the world, according to a new report. In partnership with independent researchers, password management service NordPass complied millions of passwords into a dataset to determine the 200 most commonly used passwords around the world in 2021. They analysed the data and presented results across 50 countries, looking at how popular various choices were in different parts of the world. They also looked at password trends by gender.

European Centre For International Political Economy

Cybersecurity and Gray-Zone Attacks - How to Protect Societies against New Threats? With Elisabeth Braw

12 November 2021

This summer alone, there were cyberattacks in the West bringing down pipelines, healthcare systems, payment processors and others – sometimes leading to a complete standstill in the production. How can societies defend against these cyberattacks?.

Data Protection

Landmark regulation has not directly led to effective enforcement

Data protection has never been more widely discussed. Europe's landmark General Data Protection Regulation (GDPR) was implemented in 2018, and the California Consumer Privacy Act (CCPA) in the US raised the discourse (and the stakes) even further in 2020. As data protection legislation has evolved, it has in many jurisdictions been as much a product of market regulation as of human rights law; data protection law has therefore arguably been a mechanism for redistributing the economic value of personal data. Google and Facebook have recently, in their view, been burdened by this development - as organizations that deeply financially benefit from user data. In legal cases in Europe, such as Maximilian Schrems v. Facebook Ireland Limited, and Google Spain v. AEPD and Mario Costeja González, both organizations have been accused of a lack of transparency. Meanwhile a lack of accountability mechanisms, and frustration with the outsourcing of enforcement to the platform owners themselves, has increased regulatory pressure. So far, evidence suggests the GDPR has increased regulatory burden for smaller companies greatly, while Facebook and Google have yet to see their business suffer as a result.

As the European Union continues to emerge as a regulatory force in data protection, it has renewed a focus on human rights - and on judgements suggesting that commercial entities are responsible for consumer protections including a fundamental right to privacy. However, this renewed focus also risks censorship, due to a lack of directives that take into account the technical particularities of internet services - and the potential impact of applying EU regional law to global infrastructure. Censorship has not been a priority of recent data-protection judgements, however; instead, due to an ambition to counter the dominance of both US authorities and US companies, and to a disparity in regulations, commercial and regulatory power imbalances still pose very real threats to the protection of user data, and to the protection of data subject rights. Intriguing business models have emerged around offering accessibility to enforce rights via data subject access requests (DSARs) - which could possibly lead to a higher quality of data protection standards and "privacy by design" architectures in industries looking to avoid the compliance costs associated with fulfilling such requests.

Related insight areas: Agile Governance, Justice and Law, Values, The Digital Economy, Geo-economics, Global Governance, Geopolitics, Digital Identity, International Security, Public Finance and Social Protection

Trust, Security and Regulation Briefing, January 2022

Australian Institute of International Affairs

## Book Review: Public Intellectual: The Life of a Citizen Pilgrim

16 January 2022

Public Intellectual seeks to reveal how Richard Falk became prominent in America and internationally as a public intellectual and citizen pilgrim. It's written in plain, if not brusque English, devoid of the usual international relations jargon, while filled with trenchant observations and acerbic wit.

The Guardian

Kazakhstan internet shutdown deals blow to global bitcoin mining operation

06 January 2022

Bitcoin took a hit on Thursday after the internet in Kazakhstan was shut down amid intensifying violence.
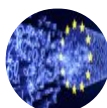
Social Europe

Regulate, but build too: for a European digital sphere

22 December 2021

Alek Tarkowski is the strategy director at Open Future. He has a PhD in sociology from the Polish Academy of Science. In 2010 he established Centrum Cyfrowe to promote openness and internet users' rights in Poland, leading it for ten years. Previously, he was a strategic adviser to the prime minister of Poland. Paul Keller is the policy director at Open Future. A political scientist, he served for ten years as co-director of Kennisland, an Amsterdam-based think-tank. He is a research fellow at the Institute for Information Law of the University of Amsterdam. From 2013 to 2018 he was on the board of Creative Commons.

In Depth News

Internet Governance Forum Calls for Stronger Digital Rights

12 December 2021

Ensuring the protection of human rights and social and economic inclusion in the digital age was front and centre at the five-day discussions.

Australian Institute of International Affairs

Germany Has Declared a Feminist Foreign Policy… So What Happens Next?

09 December 2021

Germany's new coalition agreement explicitly mentions a feminist foreign policy approach.

Center for Global Development

How Can Multilateral Organizations Strengthen Global Data Governance Practices? Roundtable Summary

06 December 2021

This brief is based on a roundtable hosted by CGD as part of the Governing Data for Development project, which explores how governments can use data to support innovation, development, and inclusive growth while protecting citizens and communities against harm. The views expressed here are those of the participants and do not necessarily represent the views of CGD staff. For other briefs in the series, as well as more on the project, visit cgdev.org/governing-data .
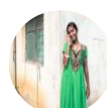
Brookings

Unlocking young women's economic potential through digital mentoring in India

30 November 2021

Imagine a room full of university students in India: young men and women sitting shoulder to shoulder in equal numbers. Fast forward 10 years: 8 out of those 10 men are likely to be active in the work force compared to only 3 out of 10 of the women. This example illustrates one of the….

References

1. Consumer Trust and Transparency

- How Prices of Sugar-Rich Foods Contribute to the Diet-Related Disease Epidemic in Mexico, RAND Corporation, www.rand.org
- Disruptive Innovations for Well-Functioning Food Systems: The Data-Driven "Food and Nutrition Security Under Climate Evolution" Framework, Frontiers, www.frontiersin.org
- HSBC, Walmart add science-based targets to supplier financing program, GreenBiz, www.greenbiz.com
- Watch out for fakes, ETH Zürich, ethz.ch
- Small and Medium Enterprises Amidst the Pandemic and Reopening: Digital Edge and Transformation, Center for Global Development, www.cgdev.org

2. Cultivating Trust

- Public support for a universal basic income is dependent on the way it is funded, London School of Economics and Political Science, blogs.lse.ac.uk
- Senate opposition means Democrats will struggle to pass voting rights bills., London School of Economics and Political Science, blogs.lse.ac.uk
- Stakeholder Capitalism | EP3 - Planet vs. Profit: Can Growth be Green?, World Economic Forum, www.youtube.com
- How Brands Can Enter the Metaverse, Harvard Business Review, hbr.org
- Is it time to hire a head of remote work?, Raconteur, www.raconteur.net
- Beyond Business: Humanizing ESG, Wharton School of the University of Pennsylvania - Knowledge@Wharton, knowledge.wharton.upenn.edu
- How can the investor community address the 'S' in ESG? – the role of social purpose values, Chatham House, www.youtube.com

3. Agency and Trust

- Asian Impact 39: ADB Distinguished Speakers Program - Daron Acemoglu, Asian Development Bank (ADB), www.youtube.com
- An attack on inequality misses its target, World Economic Forum, www.weforum.org
- 3 ways digital technology can be a sustainability game-changer, World Economic Forum, www.weforum.org
- Special Address by António Guterres, Secretary-General, United Nations | Davos Agenda 2022, World Economic Forum, www.youtube.com
- Technology Cooperation in the Fourth Industrial Revolution | Davos Agenda 2022, World Economic Forum, www.youtube.com
- Human Diversity Will Save Your Job From the Robot Takeover | Ayanna Howard, MIT Sloan Management Review, sloanreview.mit.edu
- Digital health tools for pandemic preparedness, Brookings, www.brookings.edu

4. Agency and Trust

- Editorial: Intelligence and Safety for Humanoid Robots: Design, Control, and Applications, Frontiers, www.frontiersin.org

5. Cyber Risk Governance

- Comment: Red Cross data hack, The New Humanitarian, www.thenewhumanitarian.org
- Global Risks Report 2022 Press Conference, World Economic Forum, www.youtube.com
- Attribution: A Major Challenge for EU Cyber Sanctions, German Institute for International and Security Affairs, www.swp-berlin.org
- Hacking nuclear deterrence: Cyber threats to nuclear systems, Stockholm International Peace Research Institute, www.youtube.com

6. Cyber Risk and Insurance

- 7 Trends to Watch in 2022, Harvard Business School Working Knowledge, hbswk.hbs.edu
- Will 2022 Be a Banner Year for Real Estate?, Wharton School of the University of Pennsylvania - Knowledge@Wharton, knowledge.wharton.upenn.edu
- What's Ahead for the U.S. Economy in 2022, Wharton School of the University of Pennsylvania - Knowledge@Wharton, knowledge.wharton.upenn.edu
- Digital Technologies for Government-Supported Health Insurance Systems in Asia and the Pacific, Asian Development Bank, www.adb.org
- How Marketers Can Address Data Challenges to Drive Growth, MIT Sloan Management Review, sloanreview.mit.edu
- The Popular Stock Metric That Can Lead Investors Astray, Harvard Business School Working Knowledge, hbswk.hbs.edu

7. Corporate Risk Management

- The World's Oldest Democracy Debates How It Functions, Australian Institute of International Affairs, www.internationalaffairs.org.au
- How Risk-shifting by Underperforming Funds Distorts Stock Prices, Wharton School of the University of Pennsylvania - Knowledge@Wharton, knowledge.wharton.upenn.edu
- Capital Is Not a Strategy, Project Syndicate, www.project-syndicate.org
- Do CEOs really stay in the job for too long?, University of St. Gallen, www.unisg.ch
- Socially responsible investors amplify the positive externalities of regulatory enforcement, VoxEU, voxeu.org
- Building a One-Earth Balance Sheet, Project Syndicate, www.project-syndicate.org
- Bank leverage constraints and bond market illiquidity during the COVID-19 crisis, VoxEU, voxeu.org

8. Identity Fraud and Cyber Resilience

- Pulse as a biometric measure of wellbeing, VoxEU, voxeu.org
- Online surveillance thrives when fear takes over, Social Europe, socialeurope.eu
- Harnessing Digitalization for Sustainable Economic Development: Insights for Asia, Asian Development Bank, www.adb.org
- The Danger of Digitalizing Aid, Project Syndicate, www.project-syndicate.org
- Towards transparency by design in the EU, Social Europe, socialeurope.eu
- Four Calls to World Leaders for 2022, CyberPeace Institute, cyberpeaceinstitute.org
- Measuring digital development: Facts and figures 2021, ITU, www.itu.int:443

Acknowledgements

Trust, Security and Regulation Briefing, January 2022

Continue the experience online

Explore the collective intelligence of the World Economic Forum

In today's world, individuals and organizations can find it difficult to keep up with the latest trends or to make sense of the countless transformations taking place around them.

How can you decipher the potential impact of rapidly unfolding changes when you're flooded with information—some of it misleading or unreliable? How do you continuously adapt your vision and strategy within a fast-evolving global context?

Leaders require new tools to make better strategic decisions in an increasingly complex and uncertain environment. The World Economic Forum developed Strategic Intelligence to help you understand the global forces at play and make more informed decisions.

Connect to Strategic Intelligence

Visit Strategic Intelligence on the web or download the Strategic IQ app on your mobile device to learn more.
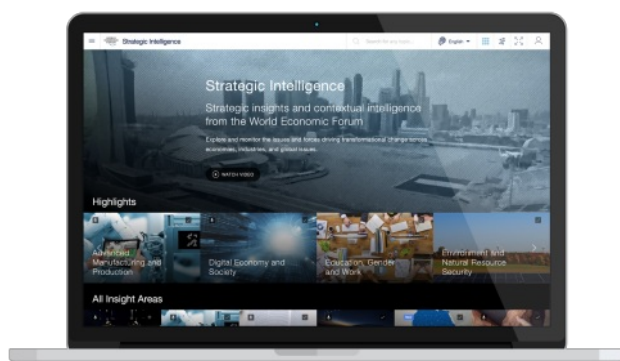
intelligence.weforum.org
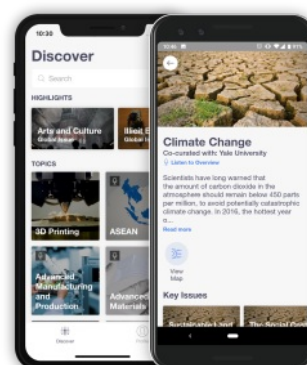
wef.ch/si

Trust, Security and Regulation Briefing, January 2022

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.