



Future of the Connected World: Global Action and Recent Progress

INSIGHT REPORT
JUNE 2022

Contents

3	Foreword
4	Executive summary
6	Action 1: Increasing education
11	Action 2: Improving security
15	Action 3: Driving positive impact
19	Action 4: Combating inequity
23	Action 5: Strengthening collaboration
27	Contributors
29	Endnotes

This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Foreword



Nicolas Jeambon
Specialist, Urban Transformation
World Economic Forum



Anu Devi
Lead, Urban Transformation
World Economic Forum

In December 2020, the World Economic Forum released its inaugural report on the [State of the Connected World](#).¹ The report, developed in collaboration with the [Council on the Connected World](#) and PwC, underscores the critical role the internet of things (IoT) plays in our lives and the enormous potential that these technologies can unleash for the benefit of society. Yet, as we grow more dependent on these technologies, the risks associated with their misuse and

the need for strong governance also increase in parallel.

Building on this initial research and landscape analysis, the Council on the Connected World released a [Roadmap for Mobilizing Global Action](#) in April 2021 to help rally the international community and accelerate progress in five key priority areas: increasing education, improving security, driving positive impact, combating inequity and strengthening collaboration.²

The five actions are part of the building blocks for a more sustainable, prosperous and connected world.



- 1 Increasing education
- 2 Improving security
- 3 Driving positive impact
- 4 Combating inequity
- 5 Strengthening collaboration

This report provides a snapshot of new developments and initiatives taken by the international community since the release of the *State of the Connected World*. It highlights examples of notable efforts that address critical technology governance challenges and gaps across the globe.

Although this is not an exhaustive list, the report seeks to shine a light on how the landscape has changed over the past 18 months, including areas in which greater collective action will be needed to build a connected future that is more resilient, sustainable and inclusive.

³ Future of the Connected World: Global Action and Recent Progress

Executive summary

As internet-enabled devices and systems continue to evolve and their adoption accelerates, governance of the internet of things (IoT) and related technologies has struggled to keep pace. Over the past two years, improvements have been made in the public and private sectors in areas such as legislation and industry standards on IoT security and increased investment in digital infrastructure. However, significant work remains to be done.

IoT continues to face major risks related to security, privacy, sustainability, accessibility and interoperability, but investors' confidence in the economic value of these technologies remains strong. Although venture capital funding

in IoT declined to \$12 billion in 2020 compared to \$20 billion the previous year due to the COVID-19 pandemic, it has bounced back. As of the third quarter of 2021, venture capital funding had already increased to 87% of the 2019 level.³

While this growth in investment opens up new opportunities to expedite and scale IoT solutions in the public interest, it also increases the importance of accelerating governance efforts to mitigate the risks and reduce the possible harms to society, while maximizing the positive impacts.

Significant governance efforts between 2021 and 2022 include, but are not limited to, the following:

Key highlights

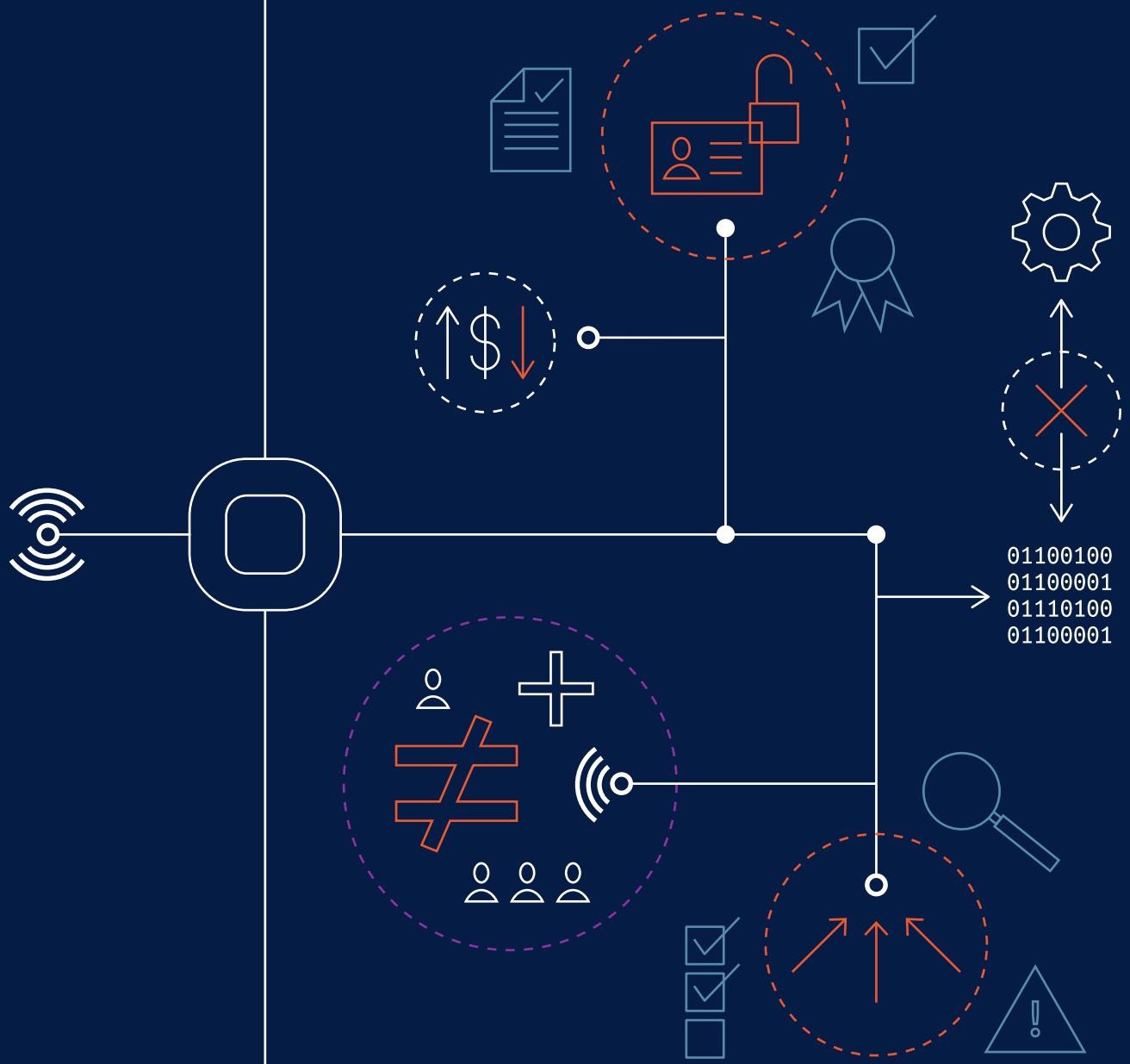
- Emerging global consensus on five minimum security provisions for consumer IoT devices
- Progress on improving interoperability standards for smart home devices
- Increased investment in sustainability and intensified commitment to climate goals by the public and private sectors, with connected technologies providing some solutions
- Increased investment in digital infrastructure for sustainability and resiliency goals
- Growth of a global network of centres working to improve technology governance across advanced and emerging economies
- Increased action to enable access to technology for small and medium-sized enterprises (SMEs)

Recent developments

2020	
Dec	World Economic Forum launches <i>State of the Connected World</i> report to track and address the most pressing governance gaps facing the development of IoT
2021	
Jan	Singapore's Cybersecurity Labelling Scheme is expanded to cover all types of consumer IoT devices
Feb	US Government issues a President's Executive Order, <i>Improving the Nation's Cybersecurity</i>
July	G20 Smart Cities Alliance releases policy benchmarks for ethical and responsible smart city development
Aug	G20 governments announce \$3.2 trillion in infrastructure investment as a stimulus between Feb 2020 and Aug 2021
Sep	EDISON Alliance announces it will accelerate digitally inclusive solutions for 1 billion people
Oct	Singapore and Finland agree to recognize each country's cybersecurity labels for consumer IoT devices
	The UK, US, Singapore, Australia and Turkey convene to share insights about policies and programmes that improve security of consumer IoT products
Nov	UNESCO and Huawei jointly launch the Technology-Enabled Open Schools for All project
	UK Government publishes Product Security and Telecommunications Infrastructure Bill
	New York City releases an IoT strategy progress report, outlining the steps the city has taken to reach its IoT goals and plans for larger efforts
	World Economic Forum releases research findings on the impact of COVID-19 on the adoption of technology among SMEs
	US signs Infrastructure Investment and Jobs Act, which includes \$2.75 billion for digital equity and inclusion work
2022	
Feb	uCIFI Alliance releases a unified data model to enable interoperability and interchangeability between smart city devices
	New Climate Institute releases Corporate Climate Responsibility Monitor 2022
	The National Institute for Standards and Technology publishes recommended criteria for cybersecurity labelling of consumer IoT products
	EU proposes new data act allowing users of connected devices to access and share the data generated by them
	Cybersecurity Tech Accord releases joint statement on an emerging consensus on baseline cybersecurity capabilities

1

Action 1: Increasing education





Increase public education and understanding of connected devices – including the responsibilities of technology makers, sellers, buyers and users – to empower individuals and organizations to make more informed decisions regarding design, adoption and use of these devices.



Helena Leurent
Director-General of Consumers International

Member of the Council on the Connected World, Chair for Action 1

The need for action

Distrust of internet-connected technologies is a growing crisis: 75% of consumers in six major economies do not trust organizations to manage their data through IoT devices.⁴ Instead, consumers want greater control over their personal data (83%).⁵

The consumer IoT segment is fast-growing and its market size is predicted to rise from \$44 billion in 2020 to \$154 billion by 2028.⁶ Devices such as smart wearables and electronics are a web of interconnected technologies, so understanding them without access to high-quality education, skills and tools can be difficult.⁷

As these devices increasingly enter people's lives, distrust in technology is likely to intensify and become highly complex, especially without adequate governance and leadership. In fact, since the onset of COVID-19, many Americans (85%) believe that

at least one tech company is spying on them.⁸

The demand for transparency and the need for advanced education in the use of technology are clear – and are two important drivers of trust. Business school students believe they lack the skills to survive in the digital age and expect more from their institutions and leaders;⁹ and according to the 2022 Edelman Trust Barometer, access to “clear, consistent, fact-based information is critical to breaking the cycle of distrust”. In addition, executives are expected to restore societal stability through trust – 74% of respondents from 28 countries expect CEOs to inform conversations and shape policy debates on technology and automation.¹⁰

The adoption of IoT for the betterment of society requires the building of long-lasting public trust and ensuring that IoT devices are trustworthy to begin with.

It is critical to demonstrate responsible leadership by taking action to improve education, transparency and other governance matters. Despite some progress on increasing public awareness, the growing amount of data, misinformation and conflicting messages about IoT may generate more issues than it does good. Practices that provide high-quality, legible and reliable information directly to consumers can be a game changer for increasing trust and informing decisions.

Recent progress

1 Modest progression on transparency through labelling for consumer devices

The public sector is taking steps to improve the transparency of consumer IoT products through labelling and signage, paving the way for informed purchasing decisions. Examples include:

- In Singapore, the implementation of the Cybersecurity Labelling Scheme (CLS), a four-tier voluntary programme with a self-declaration and conformity component, has demonstrated value in the form of increased sales and enquiries.¹¹ Companies such as Google, Nokia, Home Automation Solutions and Kyla have adopted CLS for home appliances, switches and other connected products.¹²
- The cybersecurity label issued by the Finnish Transportation and Communication Agency (Traficom) is used by Cozify, Polar and others for smart home and fitness devices.¹³ Finland and Singapore also mutually recognize elements of their programmes so that manufacturers have a single application process for label usage in both countries – as demonstrated by Signify with its smart lighting solution.¹⁴
- In the United States, the National Institute for Standards and Technology published recommended criteria for cybersecurity labelling of consumer IoT devices and software in February 2022 following the Biden administration's executive order, Improving the Nation's Cybersecurity.¹⁵
- Researchers at Carnegie Mellon University have designed a privacy

and security label generator for smart devices after an extensive review of standards and guidelines, and interviews with experts and consumers.¹⁶

While these efforts represent progress, meetings convened by the World Economic Forum with senior leaders from government agencies, consumer groups and the private sector also underscored the significant challenges facing the ecosystem. In particular, stronger alignment of public and private efforts is needed to reduce fragmentation of policies and programmes and increased incentives will be critical to help businesses with adoption in jurisdictions and markets.

Through the World Economic Forum's Future of the Connected World initiative, a multistakeholder coalition has been formed with the aim of increasing the trustworthiness of consumer IoT devices for all consumers and within the value chain. The coalition has recommended critical steps that labelling programmes need to consider to minimize future risks, including:

- Consolidate labels to reduce fragmentation globally
- Develop dynamic labels with real-time information to avoid obsolescence
- Establish a common test-and-approval system for checking labelling claims
- Determine the effectiveness of labelling policies and programmes
- Address consumer labelling fatigue

2 Usage of digital tools and data to engage and inform the public

At a local level, cities are taking action to build trust in public-facing technologies by improving transparency. This can create a path to build and maintain public trust in institutions, while harnessing public technologies' potential to address civic challenges. Examples include:

- The Angers-Loire metropolitan region in France, the town of Innisfil in Canada and in the United States both the City of Boston and the District of Columbia have joined a cohort to pilot Digital Trust for Places and Routines –

an open-source visual communication standard for connected technologies in public spaces.¹⁷

- Since the launch of What Works Cities, which helps local governments improve residents' lives using data and evidence,¹⁸ the number of cities engaging with residents and communicating on specific goals has more than tripled (from 19% to 70%), as has the number of cities using platforms and processes to release information to residents (from 18% to 67%).¹⁹

3 Increased dialogue to align public- and private-sector efforts

Government agencies, the private sector, civil society groups and other stakeholders are increasingly meeting to share insights and make progress on transparency and education around technology governance to inform consumers and other stakeholders. For instance:

- For the first time, six government agencies from the United Kingdom, the United States, Singapore, Australia, Turkey and Finland convened with other stakeholders through the Connected World to exchange learnings about their policies (with and without a labelling component) on improving the security of consumer-facing connected products. Continuous engagement is viewed as a step forward in protecting consumers and supporting businesses.
- UNESCO and Huawei jointly launched the Technology-Enabled Open Schools for All project in 2021 to build technology-enabled crisis-

resilient school systems in Africa. They will design, pilot and scale the project in Ghana, Ethiopia and Egypt over three years to connect school- and home-based learning, putting in place measures to withstand global crises and ensure continuity and quality of learning for all.²⁰

- In an effort to build the manufacturing leaders of tomorrow, Purdue Polytechnic Institute has partnered with Rockwell Automation, Honeywell, Microsoft and others to create an Industrial IoT Lab to enable hands-on learning and foster innovation.²¹

Building trustworthy connected devices requires more than shaping and accelerating transparency and educational efforts to inform key stakeholders. Factors such as accountability and agency are also perceived as key drivers of trust, which must be integrated into strategies for designing, manufacturing and selling IoT products.²²

By the numbers

83%

of consumers want greater control over their data

74%

of the public say they expect CEOs to shape policies on technology and automation

6

government agencies recently convened to share insights and learning for good practice

3

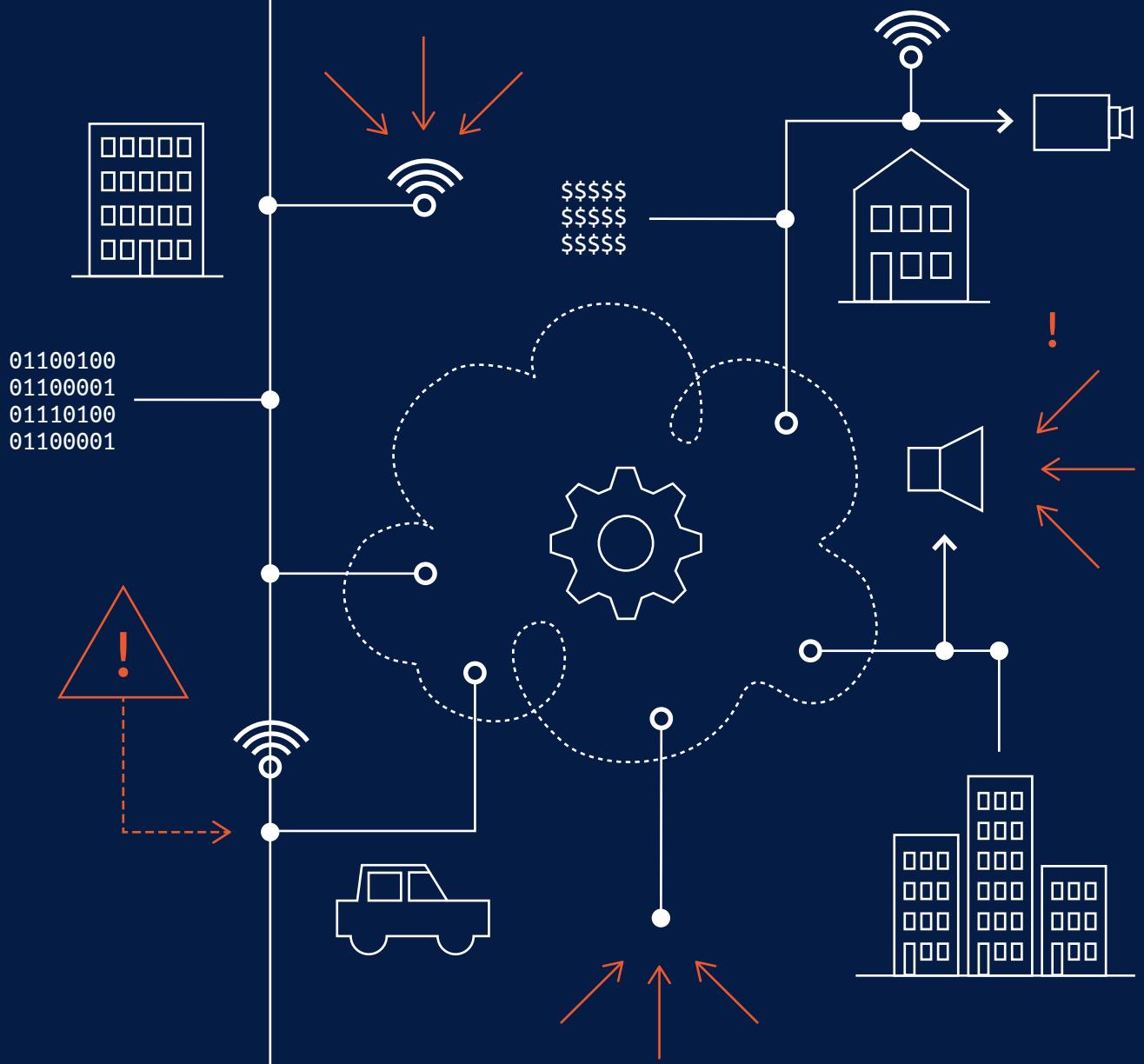
countries took steps to increase the transparency of consumer IoT devices through labelling

If you want to nominate an initiative to help advance this work or have an idea for a new solution, please email iot@weforum.org



2

Action 2: Improving security





Ease and incentivize adoption of cybersecurity best practices to ensure a common duty of care among connected device manufacturers, system integrators, service providers, purchasers and users.



Madeline Carr

Professor of Global Politics and Cybersecurity at University College London

Member of the Council on the Connected World, Chair for **Action 2**

The need for action

In 2022, cyber risk escalated to new levels. The COVID-19 pandemic, the war in Ukraine and the increasing complexity of the IoT landscape have accelerated cyberthreats, outpacing societies' ability to prevent them and respond effectively.²³

According to Accenture, there were on average 270 attacks per company in 2021 – an increase of 31% from the previous year.²⁴ This increase is more pronounced among connected devices, where cyberattacks on IoT devices more than doubled year-on-year during the first half of 2021.²⁵

Such attacks can have a drastic effect on individuals and businesses. The financial

impact of ransomware alone is substantial for organizations, with the average recovery cost for mid-sized companies more than doubling in a year, from \$761,106 in 2020 to \$1.85 million in 2021. Even after making ransom payments, only 8% of businesses regain all of their data and 29% get back no more than half.²⁶

To add to the distress, more than half (54%) of IT professionals at these organizations believe that such attacks are too advanced for their team to handle.²⁷ When it comes to healthcare, cyberattacks can have a detrimental effect on people's lives, particularly for patients who are dependent on internet-connected medical devices such as pacemakers.²⁸

“As society and the economy become more dependent on digital technology, it is imperative that governments and the private sector align and share responsibility to make these systems resilient to cyber risk by design.”

Recent progress

Increasing regulatory action to secure connected devices

Governments around the world are developing new policies and programmes to improve the cybersecurity of connected products. Notable examples include the following:

- In the United States, the IoT Cybersecurity Improvement Act of 2020 requires federal agencies to strengthen the security of IoT devices they own and control,²⁹ while the Cybersecurity & Infrastructure Security Agency (CISA) playbooks released in 2021 provide the Federal Civilian Executive Branch (FCEB) with a standard set of procedures to lead the response to cybersecurity incidents and vulnerabilities and safeguard the nation's critical assets.³⁰
- The Parliament of the United Kingdom is considering mandating security requirements for consumer IoT devices sold in the country through the Product Security and Telecommunications Infrastructure Bill after several research and consultation processes.³¹ This bill will introduce the top three guidelines

of the UK Code of Practice, including a ban on default passwords, products to have a vulnerability disclosure policy and transparency about the time period of security updates for products.³²

- Australia, Finland, Turkey and Singapore have also made strides in advancing their efforts to secure connected devices. For instance, the Australian government published its Code of Practice on securing IoT for consumers in 2020 and is discussing potential legislation for baseline cybersecurity.³³

While these efforts represent progress, meetings convened by the World Economic Forum with senior leaders from government agencies, consumer groups and the private sector also underscored the significant challenges facing the ecosystem. In particular, stronger alignment of public and private efforts is needed to reduce fragmentation of policies and programmes and increased incentives will be critical to help businesses with adoption in jurisdictions and markets.

Growing collaboration on cybersecurity through alliances

Alliances are playing an increasingly important role in improving and scaling cybersecurity best practices in industries. For instance:

- The G20 Global Smart Cities Alliance released a policy benchmark report underlining the progress of "28 pioneer cities" in adopting their cyber accountability policies. About half of the cities (13/28) met the basic requirements for senior accountability, while just over half (15/28) stated that they reviewed their cybersecurity governance frameworks regularly.³⁴
- The United Nations Internet Governance Forum held discussions on supply chain security with a focus on connected cars in which the integration of software and hardware intensifies the safety risks. Both

multistakeholder collaboration and multidisciplinary approaches are recognized as necessary instruments to reduce risk and understand the financial dimensions and social impact of supply-chain vulnerabilities.³⁵

- Other examples of alliances include the Connectivity Standards Alliance, the Global Cyber Alliance, the ioXt Alliance and the Cyber Threat Alliance. Numerous companies are joining these efforts, reflecting the growing movement among businesses to address cybersecurity, remain competitive and protect their customers.

These alliances can act as platforms to strengthen collaboration between the public and private sectors to make progress in securing internet-connected products for the betterment of society.

Emerging consensus on minimum security provisions

A global consensus is forming on IoT security provision, most notably for consumer-facing connected devices.

- Copper Horse mapped the recommendations, standards and compliance schemes of think tanks, industry associations, standard bodies and others with the European Standards cybersecurity baseline requirements for consumer IoT to make sense of global IoT recommendations and standards³⁶
- World-leading hackers focusing on responsible security practices for smart homes, industrial IoT and medical devices convened with consumer advocates, academia and industry groups in 2021 to explain the vulnerability of these devices. Together they created a statement of support for

five security provisions for consumer IoT devices representing more than 400 organizations globally.³⁷

- This statement has also been endorsed by 113 organizations. It seeks to increase awareness, and calls on manufacturers and vendors to adopt five security provisions immediately and take steps to ensure that consumers are aware of security information. The five security provisions are also found in more than 100 standards, specifications and guidelines in different regions.³⁸

While the global consensus on baseline IoT security is a critical step towards defragmenting the cybersecurity landscape, the uptake of these capabilities by manufacturers, vendors and others is still required.

By the numbers

31%

increase in cyberattacks per company from 2020 to 2021

\$1.85

million average recovery cost for mid-sized companies to recover from cyberattacks

2x

as many IoT device attacks in the first six months of 2022 compared to 2021

113

organizations signed a statement of support calling on manufacturers and others to adopt five baseline consumer IoT security provisions

If you want to nominate an initiative to help advance this work or have an idea for a new solution, please email iot@weforum.org.

3

Action 3: Driving positive impact





Increase awareness of the positive and negative impacts of connected devices on the well-being of individuals, organizations and society to incentivize adoption that benefits the world.



Anton Kotov
Chief Strategy Officer and
Chief Digital Officer, ABB
Electrification

Member of the Council on the Connected World, Co-Chair for Action 3

The need for action

Global investment in sustainability increased by 15% over two years, reaching \$35.3 trillion in 2020 across five major markets – the United States, Canada, Japan, Australasia and Europe.³⁹ Despite this growth, CO₂ emissions remain high⁴⁰ and leaders at COP26 urged greater action.⁴¹ Following 13 days of negotiation, 197 countries committed to the Glasgow Climate Pact to accelerate action on climate mitigation, adaption, finance and collaboration.⁴²

Connected technologies will play an important role in mitigating climate change and other environmental issues. New artificial intelligence and IoT technologies are predicted to generate energy savings equivalent to 58% of the ICT industry's

total power usage.⁴³ Despite their potential, 35% of IoT projects failed during the trial phase in 2021, compared to 30% in 2020. This is due to high scaling costs, the lack of necessary technology and a clear strategy, unclear business value and other reasons.⁴⁴

The positive and negative impacts of IoT on the well-being of society also extend beyond sustainability. People's ability to afford and access digital technologies is equally important. Studies have shown that in sub-Saharan Africa – where 53% of the population still do not use mobile internet in spite of living in an area with broadband coverage⁴⁵ – access to 3G/4G for a year can cut extreme poverty (people living on less than \$1.90 a day) by 4.3%.⁴⁶

⌚ Connected technologies have provided enormous benefit to society. Yet sadly these innovations and related opportunities have not been accessible to all. Again and again, we have also failed to anticipate the myriad of social, economic and environmental problems that these groundbreaking technologies can unleash. We must not repeat the mistakes of the past – this requires new ways of thinking and a new approach of designing for radical inclusion.



Victor Santiago Pineda
President, Pineda Foundation/
World Enabled, and Chairman
of the Board, Cities for All

Member of the Council on the Connected World, Co-Chair for Action 3

Recent progress

1 Increasing commitment to achieve climate goals

The private sector is increasing its focus on understanding the complexity of environmental, social and governance (ESG) issues to determine action areas with a strong emphasis on sustainability. These include:

- As many as 394 companies appointed chief sustainability officers (CSOs) in 2020–2021, a major increase compared to the 414 appointed over the previous eight years. A significant 50% of CSOs, however, hold limited influence due to having minimum access to corporate boards and overlapping roles with corporate social responsibility and health.⁴⁷
- Some 70 companies have started implementing stakeholder capitalism ESG metrics in their reporting since 2021.⁴⁸ The ESG pillar, on protecting the planet from degradation, lists the core metrics and disclosures for climate change, solid waste, resource availability, air and water pollution, nature loss and other themes. The metrics on climate change ask businesses to disclose information on

greenhouse gas (GHG) emissions from downstream and upstream activities.⁴⁹

- The Race to Zero is a coalition representing 5,235 businesses, 1,049 cities and 67 regions aiming to achieve net-zero emissions by 2050. This alliance unites 120 countries in the fight against climate change, covering about 25% of global CO₂ emissions.⁵⁰
- According to the Corporate Climate Responsibility Monitor 2022, which assessed the climate strategy of 25 global companies, only Maersk, Vodafone and Deutsche Telekom have committed to decarbonize more than 90% of their value chain emissions by the companies' target dates. Although no company achieved the high integrity rating score, Maersk scored reasonable integrity, while Apple, Sony and Vodafone had moderate integrity.⁵¹

The number of corporate climate pledges is increasing rapidly, but climate leadership and strategies will need to be more rigorous to limit global warming to 1.5° and achieve a 45% reduction in global emissions by 2030.

2 Adopting beneficial technologies to mitigate environmental challenges

IoT and related technologies have demonstrated their value in mitigating environmental challenges despite ongoing complexity and governance difficulties. Some use cases have also validated technologies' ability to generate cost savings or new economic benefits. For instance:

- Brainbox implemented a cloud-based artificial intelligence solution in a 34-storey mixed-use 1960s building in Montreal, which enabled real-time optimization of the heating, ventilation and air-conditioning system. The technology permitted the existing infrastructure to become predictive and self-adaptive, and demonstrated energy savings of 33% – about \$30,000 in savings over two months.⁵²

– Schneider Electric retrofitted its 50-year-old factory in Le Vaudreuil, France, with industrial IoT sensors, unlocking data to minimize CO₂ emissions by 25%, reducing material waste by 17% and optimizing energy management by 25%.⁵³

- Western Digital integrated IoT sensors with digital twin modelling and an analytics-powered plant management system at its factory in Penang, Malaysia, achieving a reduction in energy use of 41%, in water consumption of 45% and in material waste of 16%. The site is certified by the Malaysia Green Building Index due to this coordinated effort.⁵⁴

- New York City released an IoT strategy progress report, outlining the steps the city has taken to reach its IoT goals and its plans for larger efforts. Since March 2021, the city has successfully completed a data collection programme, including projects that gather sensor data in flood-prone neighbourhoods to monitor for stormwater and tidal flooding occurrences.⁵⁵

These use cases reflect a growing number of tried-and-tested solutions that have clear societal and financial returns. While these solutions demonstrate their potential to manage several environmental issues, their long-term success is dependent on the adoption of the circular economy and right-to-repair models to ensure smart devices – whether consumer or industrial IoT – do not contribute to growing e-waste, pollution and other sustainability concerns.

3 Scaling initiatives for a more affordable and accessible city

Stakeholders in the public and private sectors are uniting to develop model initiatives to increase the accessibility and affordability of internet and digital technologies. Some examples include:

- Government bodies from Bahrain, Bangladesh and Indonesia, and executives from businesses such as Ericsson, MTN Group, Verizon and Qualcomm have committed to the EDISON Alliance to bring digital solutions to unserved and underserved population. They aim to provide affordable and accessible digital solutions in health, finance and education to 1 billion people globally by 2025.⁵⁶
- In collaboration with Microsoft and the World Economic Forum, G3ict will partner with a cohort of six cities to adopt the G20 Global Smart Cities Alliance model policy, using

the procurement process to support more accessible digital city services for all. This will allow cities to leverage both technologies and the purchasing process to help people with disabilities through digital accessibility.⁵⁷

- Several cities (including Amsterdam, Pittsburgh and Mexico City) have deployed an online platform that enables visitors to explore streets, mark the quality of accessibility and provide feedback on improvements. Such information can help users plan their journey and assist policy-makers with improving accessibility.⁵⁸

These initiatives provide guidance for local governments and the private sector on ways to navigate the adoption, deployment and operation of technologies that deliver positive impact for the public while also laying the groundwork to scale.

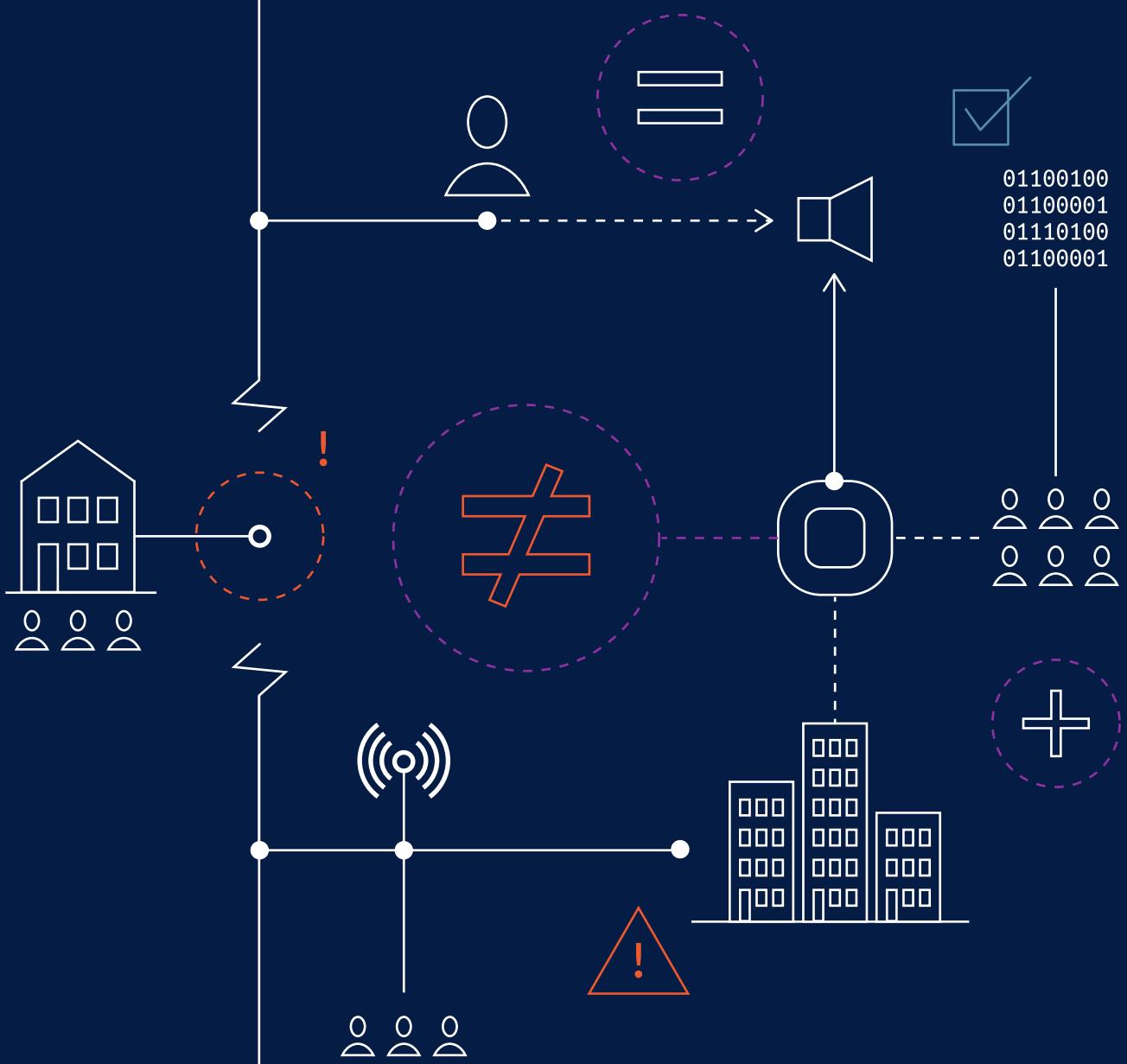
By the numbers



If you want to nominate an initiative to help advance this work or have an idea for a new solution, please email iot@weforum.org

4

Action 4: Combating inequity





Accelerate adoption of connected devices and systems among small and/or under-resourced communities and organizations through the introduction of new funding models, incentives and capacity-building mechanisms.



Shahid Ahmed
Group Executive Vice-President, New Ventures and Innovation, Nippon Telegraph and Telephone Corporation (NTT)

Member of the Council on the Connected World, Chair for Action 4

The need for action

The COVID-19 pandemic exposed inequity of access to underlying technologies that directly affected under-resourced communities and SMEs.⁵⁹ Between February 2020 and April 2021, 70–80% of SMEs in 32 countries lost between 30% and 50% of their revenue.⁶⁰

The pandemic has also intensified the need for technologies that enable access to the internet. More than half of the world's population (4.32 billion) used mobile devices during the pandemic to get online.⁶¹ Advances in internet accessibility are a significant step in connecting people and obtaining information; however, inequitable access to technologies persists: 37% of the world's population (3 billion people) have never used the internet,⁶² while the digital divide continues to be a challenge.⁶³

As the world emerges from the COVID-19 crisis, governments are announcing stimulus programmes, allowing for a core shift in how infrastructure is enabled by digital and other technologies. Between February 2020 and August 2021, G20 governments announced \$3.2 trillion (4.6% of G20 GDP) investment in infrastructure as a stimulus. Of this investment, 17% will go to digitalization, with one of the goals being to provide reliable internet access to unserved and under-served communities.

While investments provide much-needed resources and support for under-resourced communities and organizations, better leadership and more action are needed globally to make sure equitable access to technologies continues.

⌚ As the world emerges from the COVID-19 crisis, governments are welcoming opportunities to democratize digital technologies in a way that provides under-resourced communities and SMEs with greater access to enabling technologies.

Recent progress

1 New investment and resources to strengthen digital infrastructure

Global investments in digital infrastructure offer a once-in-a-generation opportunity to shape long-term growth, for both traditional network infrastructure and intelligent systems built on connected sensors and analytics.⁶⁴ For example:

- The \$1.2 trillion Infrastructure Investment and Jobs Act in the United States includes \$2.75 billion for digital equity and inclusion. It will provide much-needed investment at the state and local level, giving stakeholders the funds to plan digital equity work, improve connectivity and give people the skills to use technology.⁶⁵
- The European Union has announced similar commitments with its NextGenerationEU package worth €2.018 trillion to rebuild Europe post-COVID-19. At least 20% of the Recovery and Resilience

Facility, a key instrument of the package, will be available for digital transformation, including supporting public investments and reform projects such as faster internet, education and training.⁶⁶

- The G20 Global Smart Cities Alliance's Dig Once policy aims to provide a thorough foundation to drive and accelerate digital infrastructure. The Alliance convened a series of workshops with 17 cities and the private sector to investigate challenges and gaps, as well as how to future-proof connectivity.⁶⁷

Allocating investment to improve digital infrastructure offers a partial solution – policy-makers must further define the problem by addressing poverty, and geographic and social isolation to combat inequity.

2 Accelerating technology adoption for SMEs

SMEs represent more than 90% of all companies globally and are the primary drivers of social mobility, creating seven out of 10 jobs.⁶⁸ Their ability to access the advances of the Fourth Industrial Revolution to remain competitive in the long run is imperative for economic stability. For instance:

- The World Economic Forum, in partnership with the Ministry of Economy of Brazil and the Brazilian State of São Paulo, developed a policy protocol to lower barriers and foster the adoption of digital technologies and industrial IoT among SMEs. The initiative was successfully piloted in partnership with federal government schemes, supporting almost 2,000 SMEs, and is now being scaled in several Fourth Industrial Revolution centres around the world, including South Africa, Turkey and Kazakhstan.⁶⁹
- Findings from the Organisation for Economic Co-operation and

Development (OECD) have shown that “loans to SMEs hit new heights during the pandemic, as small firms face renewed pressures during the recovery”.⁷⁰ In addition, the OECD’s Digital for SMEs Global Initiative (D4SME) provides SMEs with knowledge-sharing and findings to help them with digitalization in response to COVID-19. The effort will strengthen understandings of how governments and SMEs are preparing for the post-pandemic environment and enable policy-makers to build more resilient and sustainable business models.⁷¹

SMEs have diverse needs, and policy-makers hold the power to help overcome a range of challenges, including raising awareness of emerging technology, providing expert and financial support, building trusted partnerships and encouraging collaborative environments in which SMEs can learn from one another.⁷²

By the numbers

\$3.2

trillion investment in infrastructure as stimulus by G20 governments (between February 2020 and August 2021)

17%

of stimulus by G20 governments allocated to digitalization

30–50%

decrease in revenue for SMEs across 32 countries (between February 2020 and April 2021)

2,000

SMEs in six countries participating in a global pilot to ease adoption of digital technology and bolster productivity

17

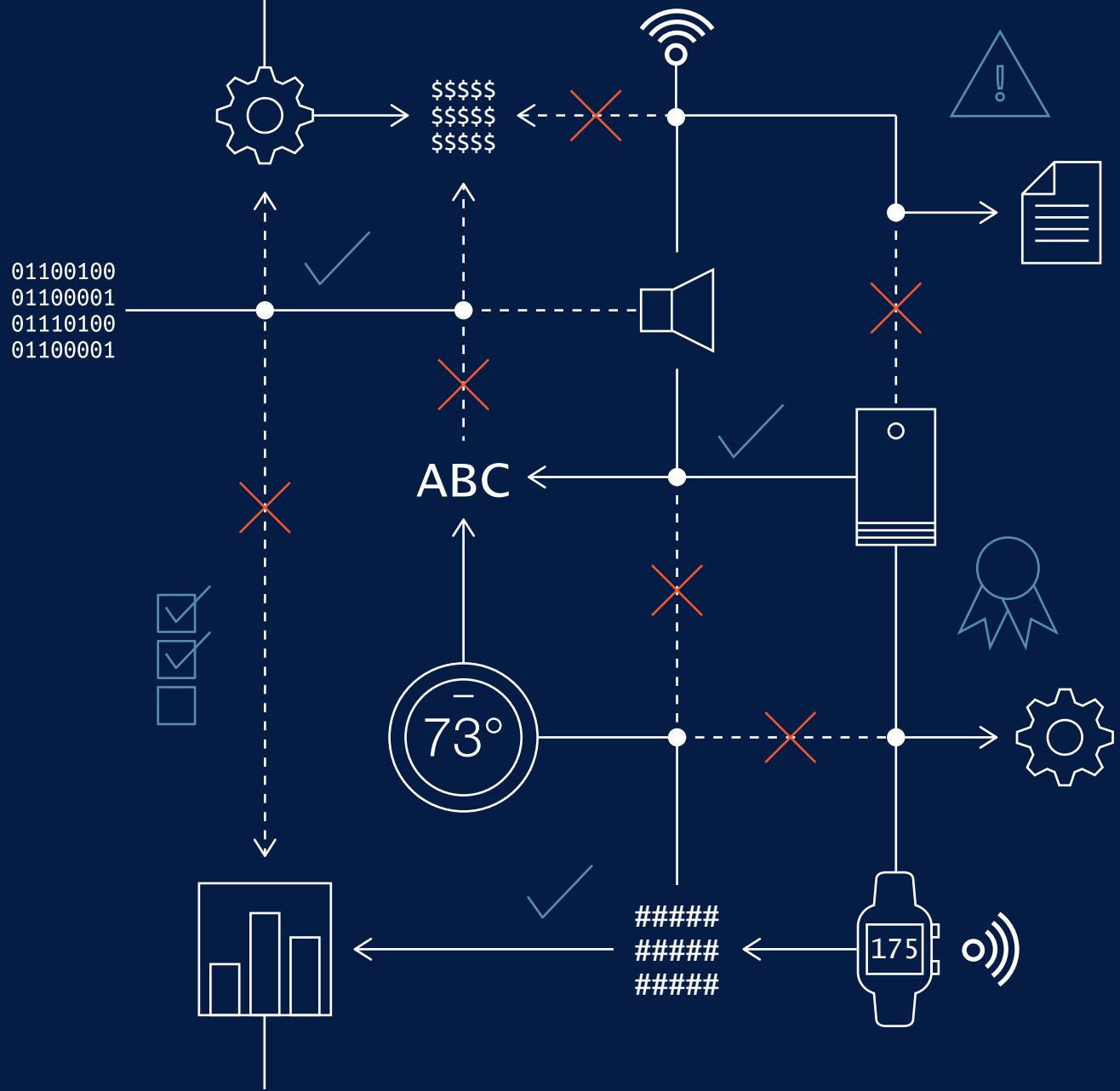
cities taking part in G20 Global Smart Cities Alliance's Dig Once policy

If you want to nominate an initiative to help advance this work or have an idea for a new solution, please email iot@weforum.org



5

Action 5: Strengthening collaboration





Strengthen collaboration and sharing of information and data across the IoT ecosystem to combat fragmentation of governance efforts, accelerate value creation and scale best practices across geographies and industries.



Tobin Richardson

President and Chief Executive Officer, Connectivity Standards Alliance

Member of the Council on the Connected World, Chair for Action 5

The need for action

Connected technologies require a collaborative ecosystem and interoperable systems throughout the value chain to achieve their full potential. According to McKinsey, the value of IoT could range from \$4–11 trillion per year by 2025 and interoperability could unlock 40–60% of this value.⁷³ Interoperability could deliver the necessary processes and tools to enable multiple technologies to share and exchange information and interact effectively.

The IoT landscape is, however, dominated by highly fragmented, proprietary and supplier-specific systems and the lack of standards for communication and data exchange between devices can inhibit growth. For instance, in factories, 70% of manufacturers are unable to scale IoT projects beyond pilots due to problems with

costs, cybersecurity and interoperability.⁷⁴ Beyond the benefits of greater efficiency and ease of use through interoperability, models and policies that make IoT data available can open up opportunities for the public and private sectors as well as for consumers. Open-data ecosystems have the potential to unlock new value in terms of innovative, data-based products and services. However, in 2021 only 14% of organizations were engaged in collaborative models for extensive data sharing. Over the next two to three years, one in four organizations will invest more than \$50 million in data ecosystems.⁷⁵

As more disruptive technologies enter the marketplace, strengthening collaboration to find a unified approach and increasing access to data across sectors and industries is needed for progress.

⌚ As more disruptive technologies enter the marketplace, strengthening collaboration to find a unified approach and increasing access to data across sectors and industries is needed for progress.

Recent progress

1

Growing pockets of consensus on IoT interoperability standards

For connected systems to communicate, interoperability is essential between hardware and software as well as beyond to other vendors within and across ecosystems. For this reason, interoperability and open standards have become essential criteria for the adoption of IoT solutions:

- The interoperability connectivity protocol, Matter, is building momentum in the smart home space. More than 200 companies including Apple, Google, Samsung and Amazon collaborated with the Connectivity Standards Alliance to form a standard to enable smart home devices to communicate with each other locally without the need for cloud services:

more than 50 companies with 130 compatible products are taking part in testing ahead of the first roll-out.⁷⁶

- The uCIFI Alliance released a unified data model to enable interoperability and interchangeability between smart city devices. Through this model, internet-connected objects will be able to communicate with any open and proprietary IoT network.⁷⁷

Models like these can accelerate the adoption of IoT and related technologies by overcoming some of the biggest challenges. However, existing and new interoperability standards must also be consolidated through collaboration to minimize further silos and confusion.

2

Forming policies to enable the exchange and transfer of data

Several policies are being developed to increase the availability of data, including:

- In February 2022, the European Commission published the EU Data Act to establish a single market for data exchange within the EU for all sectors. Businesses, public bodies, researchers and others can use the available data for innovation and remain competitive. The act will enable customers to switch between different cloud data-processing services, protect against illicit data transfer and safeguard SMEs from contractual abuse.⁷⁸

- The G20 Global Smart Cities Alliance released the policy benchmark for ethical and responsible smart city development in July 2021, covering five foundational policies, including one on open data. Of the 34 pioneer cities sharing details about their open data policy, 26 have already implemented a programme and 20 have a written policy, while 27 have a central data team.⁷⁹

These policies unite IoT ecosystems and spur innovation by stimulating competition and balancing market power between various players, such as data generators, aggregators, processors and users.

By the numbers

40–60%

of the economic value of IoT can be unlocked by interoperability

70%

of manufacturers are unable to scale IoT projects beyond pilots

50

companies are testing the interoperability protocol Matter for smart home devices

26+

cities are working to adopt the G20 Global Smart Cities Alliance model open data policy to bolster public- and private-sector collaboration

If you want to nominate an initiative to help advance this work or have an idea for a new solution, please email iot@weforum.org



Contributors

This paper benefited from the input, guidance and review of experts and stakeholders on the World Economic Forum's Council on the Connected World.

Council members

Shahid Ahmed

Group Executive Vice-President, New Ventures and Innovation, Nippon Telegraph and Telephone, US

José Alonso

Chief Executive Officer, World Wide Web Foundation, Spain

Anousheh Ansari

Chief Executive Officer, XPrize Foundation, US

Alicia Asin

Chief Executive Officer, Libelium, Spain

Madeline Carr

Professor of Global Politics and Cybersecurity, University College London, UK

Harsh Chitale

Chief Executive Officer, Digital Solutions Division, Signify, Netherlands

Cristina Colom

Director, Digital Future Society, Mobile World Capital, Spain

Jackline Conca

Undersecretary of Innovation and Digital Transformation, Ministry of Economy of Brazil, Brazil

Sridhar Gadhi

Founder and Executive Chairman, Quantela, India

Che Haiping

Chief Digital Transformation Officer, Huawei Technologies, China

Ken Hu

Deputy Chairman, Huawei Technologies, China

Farnam Jahanian

President, Carnegie Mellon University, US

Chris Johnson

Head, Global Enterprise Business, Nokia, UK

Gilbert Kamieniecky

Head, Private Equity Technology, Investcorp, UK

Mohamed Kande

Vice-Chair and Leader, US and Global Advisory, PwC, US

Vimal Kapur

President and Chief Executive Officer, Honeywell Performance Materials and Technologies, US

Anton Kotov

Chief Strategy Officer and Chief Digital Officer, ABB Electrification, ABB, Switzerland

Helena Leurent

Director-General, Consumers International, Switzerland

Fanyu Lin

Chief Executive Officer, Fluxus, US

Jeff Lorbeck

Senior Vice-President, Qualcomm, US

Jacqueline Lu

President and Co-Founder, Helpful Places, US

Keisuke Naito

Vice-President; Chief Ecosystem Officer, Eisai, Japan

Stella Ndabeni-Abrahams

Minister Small Business Development, Government of South Africa, Republic of South Africa

Peter Nicoletti

Chief Information Security Officer, Field, Check Point Software Technologies, US

Julie Owono

Executive Director, Internet Sans Frontières, France

Maria Paz Canales

Executive Director, Derechos Digitales, Chile

Nadège Petit
Chief Innovation Officer, Schneider Electric, France

Victor Santiago Pineda
President, Pineda Foundation/World Enabled and Chairman of the Board, Cities for All, US

Tobin Richardson
President and Chief Executive Officer, Connectivity Standards Alliance, US

Aarthi Subramania
Group Chief Digital Officer, Tata Sons, India

Åsa Tamsons
Senior Vice-President; Head, Business Area Technologies and New Businesses, Telefonaktiebolaget LM Ericsson, Sweden

Michele Turner
Senior Director, Google Smart Home Ecosystem, Google, US

Kristel Van Der Elst
Chief Executive Officer, The Global Foresight Group, Canada

Beau Woods
Cyber Safety Innovation Fellow, Atlantic Council, US

World Economic Forum

Lead authors

Anu Devi
Lead, Urban Transformation, World Economic Forum

Nicolas Jeambon
Specialist, Urban Transformation, World Economic Forum

Contributors

Metadel Mengestu
Coordinator, Urban Transformation, World Economic Forum

Jeff Merritt
Head of Urban Transformation; Member of the Executive Committee, World Economic Forum

Endnotes

1. World Economic Forum, “State of the Connected World: 2020 Edition”, December 2020: https://www3.weforum.org/docs/WEF_The_State_of_the_Connected_World_2020.pdf.
2. World Economic Forum, “Future of the Connected World: A Roadmap For Mobilizing Global Action”, April 2021: https://www3.weforum.org/docs/WEF_Future_of_the_Connected_World_global_action_2021.pdf.
3. McKinsey, “The Internet of Things: Catching Up to an Accelerating Opportunity”, November 2021: <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf>.
4. Consumers International and the Internet Society, “The Trust Opportunity: Exploring Consumers Attitudes’ to the Internet of Things”, 1 May 2019: <https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/>.
5. PwC, “Four Steps to Gaining Consumer Trust in Your Tech”, 19 February 2020: <https://www.pwc.com/us/en/tech-effect/cybersecurity/trusted-tech.html>.
6. Verified Market Research, “Global Consumer IoT Market Size by Type, by Application, by Geographic Scope and Forecast”, July 2021: <https://www.verifiedmarketresearch.com/product/consumer-iot-market/>.
7. Brook, Charlotte, “Business School Students Fear Digital Skills Gap”, Business Because, 6 May 2022: <https://www.businessbecause.com/news/in-the-news/8186/business-school-digital-skills>.
8. Ilumba, Angelo, “Most Americans Think Big Tech Is Spying on Them”, WhistleOut, 24 September 2020: <https://www.whistleout.com/CellPhones/Guides/americans-think-companies-are-spying>.
9. Brook, Charlotte, “Business School Students Fear Digital Skills Gap”, Business Because, 6 May 2022: <https://www.businessbecause.com/news/in-the-news/8186/business-school-digital-skills>.
10. Edelman, “Global Report: Edelman Trust Barometer, 2022”: <https://www.edelman.com/trust/2022-trust-barometer>.
11. CSA Singapore, “Cybersecurity Labelling Scheme: About”, 2022: <https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cla>.
12. CSA Singapore, “Cybersecurity Labelling Scheme: Product List”, 2022: <https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/product-list>.
13. Traficom, “Cybersecurity Label”, 2022: <https://tietoturvamerkki.fi/en/>.
14. Traficom, “Information Security Requirements for Smart Devices: Are Companies Ready?”, 26 May 2021: <https://www.traficom.fi/en/news/information-security-requirements-smart-devices-are-companies-ready>.
15. National Institute for Standards and Technology, “Executive Order 14028, Improving the Nation’s Cybersecurity. Cybersecurity Labeling for Consumers: Internet of Things (IoT), Devices and Software, 2022”: <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/cybersecurity-labeling-consumers-internet-things>.
16. Carnegie Mellon University, “IoT Security and Privacy Label: Label Generator (Beta)”: <https://iotsecurityprivacy.org/generate/>.
17. Helpful Places, “Fall 2021 DTPR Cohort”: <https://dtprcohort.helpfulplaces.com>.
18. What Works Cities, “About”: <https://whatworkscities.bloomberg.org/about>.
19. Deloitte Monitor Institute, “Closing the Data Gap: How Cities Are Delivering Better Results for Residents”, 2021: <https://results4america.org/tools/closing-the-data-gap-how-cities-are-delivering-better-results-for-residents/>.
20. United Nations Educational, Scientific and Cultural Organization (UNESCO), “Technology Enables Open Schools for All”, 2021: <https://en.unesco.org/themes/ict-education/teoss>.
21. Selko, Adrienne, “Purdue University Is Training the Manufacturing Leaders of Tomorrow”, Industry Week, 25 March 2021: <https://www.industryweek.com/talent/article/21159291/purdue-university-is-training-the-manufacturing-leaders-of-tomorrow>.
22. Devi, Anu, Fanyu Lin and Karen Lightman, “3 Ways to Get Consumers to Trust internet Connected Devices”, World Economic Forum Agenda, 10 December 2021: <https://www.weforum.org/agenda/2021/12/3-ways-to-get-consumers-to-trust-internet-connected-devices/>.
23. World Economic Forum, “The Global Risks Report 2022: 17th Edition”, 2022: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.
24. Accenture, “The State of Cybersecurity Resilience 2021: How Aligning Security and the Business Creates Cyber Resilience”, 3 November 2021: https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf#zoom=40.
25. PYMNTS.com, “Kaspersky Detects 1.5B IoT Cyberattacks This Year”, 3 September 2021: <https://www.pymnts.com/news/security-and-risk/2021/kaspersky-detects-iot-cyberattacks-double-last-year/>.

26. Sophos, "Ransomware Recovery Cost Reaches Nearly \$2 Million, More Than Doubling in a Year", Sophos Survey Shows (press release), 27 April 2021: <https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year>.
27. Ibid.
28. Canadian Centre for Cybersecurity, "Cyber Security for Connected Medical Devices (ITSAP.00.132)", November 2021: <https://cyber.gc.ca/en/guidance/cyber-security-connected-medical-devices-itsap00132>.
29. Congress.Gov, "H.R.1688: IoT Cybersecurity Improvement Act of 2020", 116th Congress, Public Law No: 116-207 (12/04/2020): <https://www.congress.gov/bill/116th-congress/house-bill/1668>.
30. Cybersecurity and Infrastructure Security Agenda, "Cybersecurity Incident and Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems", November 2021: https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.
31. UK Parliament, "Product Security and Telecommunications Infrastructure Bill", Government Bill, 19 May 2022: <https://bills.parliament.uk/bills/3069>.
32. Parliament of the United Kingdom, House of Commons, "Research Briefing: Product Security and Telecommunications Infrastructure Bill", 20 May 2022: <https://researchbriefings.files.parliament.uk/documents/CBP-9430/CBP-9430.pdf>.
33. Itnews, "Gov Pledges to Mandate IoT Cyber Security Standards", 13 May 2022: <https://www.itnews.com.au/news/gov-pledges-to-mandate-iot-cyber-security-standards-579961>.
34. World Economic Forum, "Governing Smart Cities: Policy Benchmark for Ethical and Responsible Smart City Development", July 2021: https://www3.weforum.org/docs/WEF_Governing_Smart_Cities_2021.pdf.
35. Internet Governance Forum, "IGF 2021 WS #228 Supply Chain Governance and Security for IoT Resilience", Session on Inclusive IG Ecosystems and Digital Cooperation, 2021: <https://www.intgovforum.org/multilingual/content/igf-2021-ws-228-supply-chain-governance-and-security-for-iot-resilience>.
36. Copper Horse, "Mapping Security and Privacy in the Internet of Things: Making Sense of Global IoT Recommendations and Standards and Mapping them to ETSI EN 303 645, 2021": <https://iotsecuritymapping.com>.
37. Tech Accord, "Joint Statement of Support on Consumer IoT Device Security", 15 February 2022: <https://cybertechaccord.org/industry-hackers-and-consumers-for-a-global-baseline-for-consumer-iot-security/>.
38. Ibid.
39. Global Sustainable Investment Alliance, "Global Sustainable Investment Review 2020": <http://www.gsi-alliance.org/wp-content/uploads/2021/08/GSIR-20201.pdf>.
40. International Energy Agency, "Global Energy Review 2021: CO2 Emissions", March 2022: <https://www.iea.org/reports/global-energy-review-co2-emissions-in-2021-2>.
41. United Nations Climate Change Conference UK 2021, "COP26 Outcomes", 2021: <https://ukcop26.org/the-conference/cop26-outcomes/>.
42. United Nations Climate Change Conference UK 2021, "Delivering the Glasgow Climate Pact", 2021: <https://ukcop26.org>.
43. 6G World, "Sustainability in New and Emerging Technologies", 2021: <https://www.6gworld.com/sustainability-in-new-and-emerging-technologies/>.
44. Microsoft, "IoT Signals", 3rd edition, 2021: <https://azure.microsoft.com/en-gb/resources/iot-signals/>.
45. Delaporte, Anne, "The State of Mobile Internet Connectivity in sub-Saharan Africa: Why Addressing the Barriers to Mobile Internet Use Matters Now More Than Ever", GSMA Mobile for Development, 27 October 2021: <https://www.gsma.com/mobilefordevelopment/blog/the-state-of-mobile-internet-connectivity-in-sub-saharan-africa/>.
46. World Bank Group, "The Welfare Effects of Mobile Broadband Internet: Evidence from Nigeria", Policy Research Working Paper 9230, 2020: <https://elibrary.worldbank.org/doi/pdf/10.1596/1813-9450-9230>.
47. PwC Strategy&, "Empowered Chief Sustainability Officers: The Key to Remaining Credible and Competitive", 2021: <https://www.strategyand.pwc.com/de/en/unique-solutions/sustainable-impact-made-real/empowered-chief-sustainability-officers.html>.
48. World Economic Forum, "Stakeholder Capitalism: Over 70 Companies Implement ESG Reporting Metrics", Agenda, 24 May 2022: <https://www.weforum.org/impact/stakeholder-capitalism-50-companies-adopt-esg-reporting-metrics/>.
49. World Economic Forum, "Measuring Stakeholder Capitalism: Towards Common Metrics and Consistent Reporting of Sustainable Value Creation", September 2020: https://www3.weforum.org/docs/WEF_IBC_Measuring_Stakeholder_Capitalism_Report_2020.pdf.
50. United Nations Climate Change, "Race to Zero Campaign", 2022: <https://unfccc.int/climate-action/race-to-zero-campaign>.

51. New Climate Institute, "Corporate Climate Responsibility Monitor 2022: Assessing the Transparency and Integrity of Companies' Emission Reduction and Net-Zero Targets", 2022: <https://newclimate.org/2022/02/07/corporate-climate-responsibility-monitor-2022/>.
52. World Economic Forum, "Driving Digitalization: Value Creation for Commercial Real Estate", 2021: https://www3.weforum.org/docs/WEF_Driving_Digitalization_Real_Estate_2021.pdf.
53. World Economic Forum, "The Global Lighthouse Network Playbook for Responsible Industry Transformation", March 2022: https://www3.weforum.org/docs/WEF_The_Global_Lighthouse_Network_Playbook_for_Responsible_Industry_Transformation_2022.pdf.
54. World Economic Forum, "The Global Lighthouse Network Playbook for Responsible Industry Transformation", 2022: https://www3.weforum.org/docs/WEF_The_Global_Lighthouse_Network_Playbook_for_Responsible_Industry_Transformation_2022.pdf.
55. New York City Mayor's Office of the Chief Technology Officer, "2021 Impact Report", 2021: https://www1.nyc.gov/assets/cto/downloads/annual-reports/2021_impact_report.pdf.
56. MTN, "EDISON Alliance Members Commit to 1 Billion Lives Challenge": <https://www.mtn.com/edison-alliance-members-commit-to-1-billion-lives-challenge/>.
57. G3ict, "G3ict, World Economic Forum, and Microsoft Launch New Inclusive Cities Project" (news release), 25 October 2021: <https://g3ict.org/news-releases/g3ict-world-economic-forum-and-microsoft-launch-new-inclusive-cities-project>.
58. Silicon Canals, "Amsterdam and Accessibility: Here's How AI Startups Are Helping the City" (news release), 19 April 2022: <https://siliconcanals.com/news/startups/amsterdam-ai-startups-accessibility/>.
59. Broadband Commission for Sustainable Development, "The State of Broadband: People-Centred Approaches for Universal Broadband", September 2021: https://www.itu.int/dms_pub/itu-s/obp/pol/S-POL-BROADBAND.23-2021-PDF-E.pdf.
60. McKinsey, "Beyond Financials: Helping Small and Medium-size Enterprises Thrive", 2022: <https://www.mckinsey.com/industries/public-and-social-sector/our-insights/beyond-financials-helping-small-and-medium-size-enterprises-thrive>.
61. Statista, "Mobile Internet Usage Worldwide: Statistics and Facts", 22 February 2022: <https://www.statista.com/topics/779/mobile-internet/>.
62. Agence France-Presse, "More than a Third of World's Population Have Never Used Internet, Says UN", The Guardian, 30 November 2021: <https://www.theguardian.com/technology/2021/nov/30/more-than-a-third-of-worlds-population-has-never-used-the-internet-says-un>.
63. Global Infrastructure Hub, "Transformative Outcomes through Infrastructure: Overview", 2021: <https://transformativeinfratracker.github.io/overview/>.
64. Information Technology and Innovation Foundation, "'Building Back Better' Requires Building in Digital", 10 May 2021: <https://itif.org/publications/2021/05/10/building-back-better-requires-building-digital>.
65. Quaintance, Zack, "Infrastructure Bill Promises Historic Boost for Digital Equity, Government Technology", 16 November 2021: <https://www.govtech.com/network/infrastructure-bill-promises-historic-boost-for-digital-equity>.
66. European Commission, Directorate-General for Budget, "The EU's 2021–2027 Long-term Budget and NextGenerationEU: Facts and Figures", 2021: <https://op.europa.eu/en/publication-detail/-/publication/d3e77637-a963-11eb-9585-01aa75ed71a1/language-en>.
67. G20 Global Smart Cities Alliance, "Model Policy: Dig Once", 2020: <https://globalsmarcitiesalliance.org/?p=806>.
68. The World Bank, "Small and Medium Enterprises (SMEs) Finance: Improving SMEs Access to Finance and Finding Innovative Solutions to Unlock Resources of Capital": <https://www.worldbank.org/en/topic/smefinance>.
69. World Economic Forum, "Small and Medium Size Enterprises Futures Network": <https://www.weforum.org/projects/sme-futures>.
70. Organisation for Economic Co-operation and Development (OECD), "New OECD Report Shows Loans to SMEs Hit New Heights During the Pandemic, as Small Firms Face Renewed Pressures During the Recovery", 29 March 2022: <https://www.oecd.org/newsroom/new-oecd-report-shows-loans-to-smes-hit-new-heights-during-the-pandemic-as-small-firms-face-renewed-pressures-during-the-recovery.htm>.
71. OECD, "OECD Digital for SMEs Global Initiative", 2022: <https://www.oecd.org/digital/sme/>.
72. World Economic Forum, "Accelerating the Impact of Industrial IoT in Small and Medium-Sized Enterprises: A Protocol for Action", January 2020: https://www3.weforum.org/docs/WEF_Accelerating_the_Impact_of_IoT.pdf.
73. Manyika, James (ed.), "Unlocking the Potential of the Internet of Things", McKinsey Digital, 1 June 2015: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>.
74. McKinsey, "The Internet of Things: Catching Up to an Accelerating Opportunity", November 2021: <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf>.

75. Capgemini Research Institute, "Data Sharing Masters: How Smart Organizations Use Data Ecosystems to Gain Unbeatable Competitive Edge", 2021: <https://www.capgemini.com/insights/research-library/data-sharing-masters/>.
76. Wroclawski, Daniel, "Matter, Explained: What the New Standard Could Mean for Your Smart Home", Consumer Reports, 7 January 2022: <https://www.consumerreports.org/smart-home/matter-smart-home-standard-faq-a9475777045/>.
77. uCIFI, "uCIFI Data Model": <https://ucifi.org/ucifi-data-model/>.
78. European Commission, "Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy" (press release), 23 February 2022: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.
79. World Economic Forum, "Governing Smart Cities: Policy Benchmarks for Ethical and Responsible Smart City Development", July 2021: https://www3.weforum.org/docs/WEF_Governing_Smart_Cities_2021.pdf.



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

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.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org