CLTC Center for Long-Term Cybersecurity
UC Berkeley

CNA

WORLD ECONOMIC FORUM

Cybersecurity Futures 2030
New Foundations

WHITE PAPER

DECEMBER 2023

Images: Getty Images

Contents

Foreword

Ann Cleaveland
Executive Director, CLTC,
UC Berkeley

Akshay Joshi
Head of Industry and Partnerships, Centre for Cybersecurity, World Economic Forum

Dawn Thomas
Co-Director, Institute for Public Research, CNA

The global cybersecurity landscape is constantly and rapidly changing. By 2030, it will once again be radically transformed. To better understand how technological, political, economic and environmental changes are impacting the future of cybersecurity for governments and organizations, the UC Berkeley Center for Long-Term Cybersecurity (CLTC), the World Economic Forum Centre for Cybersecurity and CNA's Institute for Public Research have collaborated on *Cybersecurity Futures 2030*, a foresight-focused research initiative that aims to inform cybersecurity strategic plans around the globe.

Our engagement in the Cybersecurity Futures 2030 initiative reflects a shared commitment to promote digital security as a strategic priority and understand how systemic cybersecurity challenges are experienced and addressed in different regions around the world.

Through a series of in-depth workshops held in six international locations, we explored various alternative digital futures considering how cybersecurity is set to transform over the next five to seven years. The report includes insights from the global workshops that are broadly applicable across countries and regions. The findings aim to help decision-makers in government, industry, academia and civil society seize opportunities and mitigate risks just over the horizon.

We extend our gratitude to those who contributed to this initiative, recognizing that only through collaborative efforts can we securely harness the promise and potential of technological progress. May the insights contained herein spur meaningful dialogue, inspire action and guide our collective journey toward a more secure and inclusive digital future.

Executive summary

Digital innovation is accelerating. Decision-makers need long-term strategic foresight to seize opportunities and mitigate risks.

This report presents findings from Cybersecurity Futures 2030, a global research initiative focused on exploring how digital security could evolve over the next five to seven years. The goal of this project is to help shape a future-focused research and policy agenda that is widely applicable across countries and sectors.

The findings are based on discussions held at a series of in-person workshops conducted throughout 2023 in Dubai (United Arab Emirates), Washington DC (USA), Kigali (Rwanda), New Delhi (India) and Singapore, as well as a virtual workshop with participants from multiple European countries and the United Kingdom. The workshops centred on discussion of four scenarios that portray diverse "cybersecurity futures" that are fictional (but plausible) depictions of the world roughly in the year 2030. UC Berkeley Center for Long-Term Cybersecurity (CLTC) independently designed the scenarios to explore trade-offs in goals and values that decision-makers will have to contend with in the near future.

Key findings

- Acceleration in technology and business model innovation (both licit and criminal) will underpin the new digital security landscape for 2030. Societies must fundamentally reorient their responses to perennial digital security challenges, including data privacy, talent development and sustainability.
- Shoring up trust will be a key goal of cybersecurity efforts over the next decade. The online spread of mis- and disinformation are now core cybersecurity concerns. Cybersecurity will become less about protecting the confidentiality and availability of information and more about protecting its integrity and provenance.
- Stable governments that follow through on long-term technology and cybersecurity strategies can become trusted "brands", gaining advantages in attracting talent, seizing leadership opportunities in multilateral standards-setting processes and countering disinformation campaigns.
- Public-private partnerships will be imperative to move the needle on combating sovereign and criminal cyberattacks and information operations but new incentive structures will be needed to achieve such partnerships.
- There is a window of opportunity for emerging and developing countries to implement "secure by design" principles that the first waves of digitalization have largely failed to embed. Decision-makers should monitor the pace of digitalization and the ability of populations to integrate new technologies safely and securely.
- Transformative investment in cybersecurity talent and training will be a priority objective. Countries' ability to project themselves as trusted global brands, attract global talent, retain homegrown talent and provide a productive environment to capitalize on that talent matters significantly. Promoting education and awareness of digital security will be critical.
- Decision-makers across regions are struggling to balance technology value-chain interdependencies and self-sufficiency. Even as national data regulations proliferate, trusted standards are needed that incentivize interoperability in cybersecurity and artificial intelligence (AI) security. In some regions, there is a sense of a global leadership void, a lack of trusted and expert regulatory bodies and insufficient capacity for enforcement of security and privacy laws and standards.
- The focus in the next three to five years will be on the practicalities of navigating a world in flux. This dynamic will vary across regions, will be influenced by their relationships with China and/or the US and will hold steady regardless of the strength or weakness of the US-China relationship over the next five years.

Takeaways for decision-makers

- Organizations will need to ensure they have a stable and secure supply chain of resources, including technology components, raw materials and skilled, affordable workers.
- Effective digital policies and regulations should demonstrate clear and stable priorities of companies, governments and other organizations.
- Resilience, humour and optimism about the future – and the opportunities that await those willing and able to seize them – are critical in the run-up to 2030.
- Having a digitally literate public and customer base that is media savvy and inoculated against mis-, dis- and mal-information (MDM) will be a source of strength for organizations that wish to succeed in an era of degrading trust.
- Leaders should actively look for ways to ensure that emerging technologies help the general population, for example by stabilizing national economies, addressing high costs of living, providing food security and advancing renewable energy.
- The public and private sectors should invest in education (e.g. media literacy and cybersecurity hygiene) for the general population to decrease the attack surface and in-job training to upskill a digital workforce.
- Leaders will need to strategically and tactically use regulation to guard against the downsides of AI products as they rise in prominence and must take meaningful measures to combat MDM before it further degrades trust and unity.
- Countries should form and strengthen trusted research institutions, particularly in less-developed economies, to support governments in addressing the most challenging social and technical cybersecurity problems of 2030.

The next phase of this project will include working with decision-makers to generate additional priorities and thinking more broadly about how findings from this report could reshape organizations' futures. Grappling with these kinds of questions should be a defining focus in 2024 for C-suites, boards and government agencies internationally.

Introduction

Cybersecurity Futures 2030 is a foresight-focused research initiative that aims to inform cybersecurity strategic planning around the globe.

“ This broader look at cybersecurity can best be understood as defending against harm and promoting opportunity anywhere technology touches society.

A wide range of issues have changed the cybersecurity agenda over the past five years – from digital transformation during a global pandemic to the commercialization of large language models and from the largest military conflicts of the cyber age to an international ransomware scourge. As Ken McCallum, the Director-General of the British Security Service, recently remarked: “If you are working at the cutting edge of technology today, you may not be interested in geopolitics, but geopolitics is certainly interested in you.”[1] The next five years will bring another set of unprecedented cybersecurity challenges and opportunities. Those with strategic foresight will be better situated to tilt the digital world in a direction that is more secure.

To look over the horizon, the UC Berkeley Center for Long-Term Cybersecurity (CLTC), with the support of the World Economic Forum’s Centre for Cybersecurity (C4C) and CNA’s Institute for Public Research, launched Cybersecurity Futures 2030, a global initiative that explores how digital security could evolve over the next five to seven years. The aim is to help shape a future-focused research and policy agenda that is widely applicable across countries and sectors. This broader look at cybersecurity can best be understood as defending against harm and promoting opportunity anywhere technology touches society.

Between January and April 2023, the CLTC independently developed a set of four scenarios that portray possible “cybersecurity futures” looking forward to roughly 2030. The scenarios were designed to examine some of the trade-offs in goals and values that decision-makers will have to contend with in the near future. The scenarios focus on what is relevant and plausible, while also challenging implicit beliefs and today’s conventional wisdom. Rather than predict the future, they are specifically designed to elicit meaningfully different global perspectives.

Between May and September 2023, the initiative took these scenarios to five international locations that will have different influences and perspectives on the digital security landscape of the next decade: Dubai (United Arab Emirates), Washington DC (USA), Kigali (Rwanda), New Delhi (India) and Singapore. In addition, there were virtual workshops with participants from multiple European countries and the United Kingdom. A workshop in each location had a mix of participants from government, business, civil society, academia and other domains. Similar workshop processes were run to extract reactions and insights that would be comparable. These comparisons are the most important immediate product of the workshops.

Of course, these comparisons come with caveats, the most important of which is the use of aggregate geographical categories as placeholders. A single workshop in New Delhi (despite broad representation from experts in academia, industry, government and civil society) cannot represent the comprehensive perspective of citizens in the world’s most populous country. Nor can a workshop in Kigali speak for the whole African continent. The geographic labels are best thought of as imperfect proxies that shed light on commonalities and differences across many regions that will impact the future of the global digital security landscape, but there was no capacity to convene workshops in all parts of the world. Another caveat is recency bias; the workshop participants are people and people read future scenarios in the context of what is most important and urgent in their minds at that moment. In this context, it is likely unsurprising that workshop participants mentioned artificial intelligence (AI) more than other emerging technologies by a factor of 10. Finally, scenarios themselves have blind spots, even as they stretch imaginations to the edge of plausibility. The workshop process was designed to minimize these kinds of biases but it is impossible to fully eliminate them.

The workshops helped expose how attitudes and perspectives are developing and diverging across geographies. The insights reported below are likely to reframe the decision-making environment and will help decision-makers in government, industry and civil society reduce frictions, seize opportunities for cooperation and better prepare for the future.

1 Findings and insights from the workshops

A series of international workshops revealed critical challenges, uncertainties and opportunities for governments and organizations in a rapidly evolving cybersecurity landscape.

This report details three overarching observations and three proposed elements of the new landscape in 2030 that emerged from the workshops.

Each deserves focused attention in strategic planning and future decision-making.

1.1 Overarching observations

> Cybersecurity will become less about protecting the confidentiality and availability of information and more about protecting its integrity and provenance.

1 **Digital security is being reframed as the ability of societies to match the speed of trust with the speed of innovation.** In each workshop, participants voiced fears that the speed of technological and criminal innovation has surpassed humanity's ability to ensure the trustworthiness of digital products and information, which has profound consequences for the legitimacy of national and international institutions. Shoring up trust emerged as a key goal of cybersecurity efforts over the next decade. At a strategic level, stable governments that follow through on long-term technology and cybersecurity strategies can become trusted "brands", gaining advantages in attracting talent, seizing leadership opportunities in multilateral standard-setting processes and countering disinformation campaigns. This outlook was most pronounced in Singapore, India and the United Arab Emirates. At a more operational level, participants also discussed regulators' role in monitoring multinational companies closely with effective accountability measures. This sentiment was most pronounced in Africa and the EU. In the US, there was much more tension about who is "in charge" of trust – the government or the private sector. Agreement that public-private partnerships are imperative to move the needle on combating sovereign and criminal cyberattacks and information operations was accompanied by an equal sense of disillusionment about the feasibility of such partnerships given current incentive structures. Participants voiced nearly universal agreement that the online spread of mis-, dis- and mal-information (MDM) are now core cybersecurity concerns. Cybersecurity will become less about protecting the confidentiality and availability of information and more about protecting its integrity and provenance.

2 **The pace and scale of digitalization will drive changes to the global security landscape as much as (or more than) the specific capabilities of emerging technologies.** Workshop participants focused on AI and automation more than other technologies by a factor of 10, though the current and potential capabilities of quantum computing, the internet of things (IoT) and advances in space also emerged as priorities. In the context of uncertainties and vulnerabilities, participants cautioned about future cleavages that could emerge with quantum technologies and identified the development and deployment of quantum-safe cryptography as a priority. Preparing technically and by creating norms and boundaries could have sweeping positive impacts for governments, businesses and societies. Space – given the integration of advanced technologies in space-based systems – came up as another environment where emerging technology could cause future cleavages and as a domain ripe for countries to innovate and advance. Yet the biggest threat to the digital security landscape is still more human than technical. The security consequences of rapid digital transformation had particular relevance in emerging and developing countries with large populations. Cybersecurity challenges and opportunities of the next decade will be proportionate to the pace and scale at which countries digitalize. As participants in India pointed out, larger populations correspond to a larger target for attacks, ranging from disinformation

campaigns to fraud and extortion – familiar attacks that will only become more complex as criminals gain easier and cheaper access to more sophisticated technologies. The upside is that there is a window of opportunity for emerging and developing countries to implement "secure by design" principles that the first waves of digitalization in more developed countries have largely failed to embed. To anticipate and address the cybersecurity challenges of the next decade, decision-makers should monitor the pace of digitalization – and the ability of populations to integrate new technologies safely and securely – as closely as they do the security specifications of the technology itself.

3 **Debates about internet fragmentation versus a "free and open" internet are morphing into more practical conversations about trade-offs between digital sovereignty and interoperability.** Decision-makers across regions are struggling to create the right balance between technology value-chain interdependencies and self-sufficiency. For example, even as national data regulations proliferate, including across the continent of Africa, participants voiced more uniform and urgent calls for trusted standards that incentivize interoperability in cybersecurity and AI security. In Singapore, there was more confidence that the government can de-risk its dependencies by exerting influence through regulation, standards and partnerships to ensure that technologies used in the country meet high cybersecurity standards. In other regions, there is a profound sense of a global leadership void, a lack of trusted and expert regulatory bodies and insufficient capacity for the enforcement of security and privacy laws and standards. To meet this need, multi-aligned countries may be best positioned to facilitate multilateral efforts and most able to advance common norms and standards that benefit collective cybersecurity, while simultaneously investing to limit their technology and supply chain dependencies. This pragmatic sense of opportunity was heard most strongly in Singapore, the United Arab Emirates and India. The focus in the next three to five years will be on the practicalities of navigating a world in flux.

This dynamic seems to gain traction as countries become increasingly aware of the consequences of technological colonialism that regions have experienced to varying degrees depending on their relationships with China and/or the US, and holds steady regardless of the strength or weakness of the US-China relationship over the next five years. Europeans worried about a false sense of security and asked the question: "If the region is reliant on external large technology companies to manage our data and develop AI, how can we know which technology products are safe to use?" Chinese tools permeate India and Rwanda (and Africa more broadly), and Chinese technology companies continue to be seen as potential partners for advancing digital infrastructure in these regions. There is also considerable concern about China's ability and willingness to protect partner technology, potential loss of privacy and the end of low-cost, high-quality technology products if the US and China cooperate instead of competing. Participants anticipate that global alliances are set to reshuffle in the coming years, with opportunities for countries to create new poles in a more multipolar world.

1.2 The new digital security landscape for 2030

> "The objective in 2030 will be for countries, communities and individuals to negotiate a fair return on investment in controlled and responsible use of their data.

Acceleration in technology and business model innovation (both licit and criminal) will underpin the new digital security landscape for 2030. The workshops uncovered a universal sense that this acceleration is not likely to be incremental. The new landscape will require societies to fundamentally reorient their responses to perennial digital security challenges, three of which are changing in particularly important ways: data privacy, talent development and sustainability.

– "Make sure you are getting something in return for your personal data," was a refrain heard around the world. In the workshop discussions, almost no one believed that it is still plausible or desirable to fully restrict flows of personal data. Rather, the sentiment is that "the cat is out of the bag" and that the objective in the decade to 2030 will be for countries, communities and individuals to negotiate a fair return on investment (ROI) in controlled and responsible use of their data. What does this mean for the future of digital security and privacy? European participants saw a tightrope walk between leading the world in digital regulation and enforcement on one side and the financial and economic returns that data-powered innovation could generate on the other. In Rwanda, concerns emerged about AI models that are moving ahead without African data. African representation in training data is critical in order for AI products to be safe and trustworthy to deploy in an African context but technology producers and African data owners must be equal participants in the transaction. In the US, firms making investments in data protection and

“ Transformative investment in cybersecurity talent and training emerged as a priority objective across scenarios and geographies.

use will need to contend with emerging societal movements advocating for more self-owned or self-managed data. There is also potential for platform firms and their users to become new allies in disincentivizing large-scale data scraping by third parties. But the “Make sure our data is out there – and used securely in ways that benefit communities” sentiment is a pronounced change in attitude towards personal data than heard in the past.

– Transformative investment in cybersecurity talent and training emerged robustly as a priority objective across geographies. To a far greater degree than seen in the past, participants in all workshop locations recognized the importance of human capital for managing technology and cybersecurity, regardless of technological advances. Several intersecting dynamics were universally cited:

  a. *The intensifying competition for global talent.* The bar for cybersecurity talent is getting higher. Participants noted that as automation and AI fulfill many entry-level technical jobs, there will be increasing need and opportunities for people trained in supervisory and policy roles for cybersecurity and AI security. In addition, the demand for people who can design, build and deploy secure machine learning and AI products is skyrocketing. The ability of countries to project themselves as trusted global brands, attract global talent, retain homegrown talent and provide a productive environment to capitalize on that talent matters significantly. Participants expressed acute awareness of the risk of a zero-sum game dynamic – whereby countries compete over the same limited pool of talent – if countries don’t simultaneously invest in the development and retention of local talent, with particular consequences for less developed countries. Instead of “brain drain”, decision-makers will need to consider ideas like “brain circulation” (by which foreign-born technologists transfer technical and institutional know-how between distant regional economies) in the next decade.[2]

  b. *The urgency for broad cyber literacy training to combat disinformation and garden-variety cybercrime.* Education and awareness of digital security will be critical. Participants saw profound upside for companies, governments and NGOs that successfully create updated campaigns and curricula to educate the public on digital security issues and best practices. This is especially true for new technology users in less developed countries.

  c. *Local and regional education and skilling programmes to reshore supply chains and enable economic development.* The need to develop and retain talent in hardware security and industrial control systems emerged as a shared global challenge. In contrast, concerns about the future of the job market and AI-driven displacement of the workforce were expressed as different pressures in different regions. In Rwanda, participants saw an upside opportunity to create an indigenous technology economy and workforce, with Africa’s youth demographic representing an enormous untapped talent pool if jobs can be created. Participants warned, however, that, “We [Africa] will struggle to keep up” economically and with technology development if access to technical training and education does not improve. In the US and Europe, participants expressed a sense of urgency about keeping an edge in a technology race with China and emphasized the mobilization that will be required to upskill a labour force equipped to design, build and deploy advanced technology across many sectors.

– Sustainability, climate change and digital security goals are becoming more entangled. Participants expressed a shared awareness that technology advancements are causing major increases in energy demand, with no sign of slowing. At the same time, construction of new, distributed green energy infrastructure, such as electric vehicle charging and smart grid networks, is set to expand the IoT, a notorious source of cyber insecurity in danger of being overlooked as hype about AI captures headlines and imaginations. Participants expressed optimism about the potential of new technologies, particularly AI tools, to help with climate and energy solutions but stressed that digital infrastructure will need to be built and upgraded with climate and energy resilience measures in mind to keep the lights on and realize this promise.

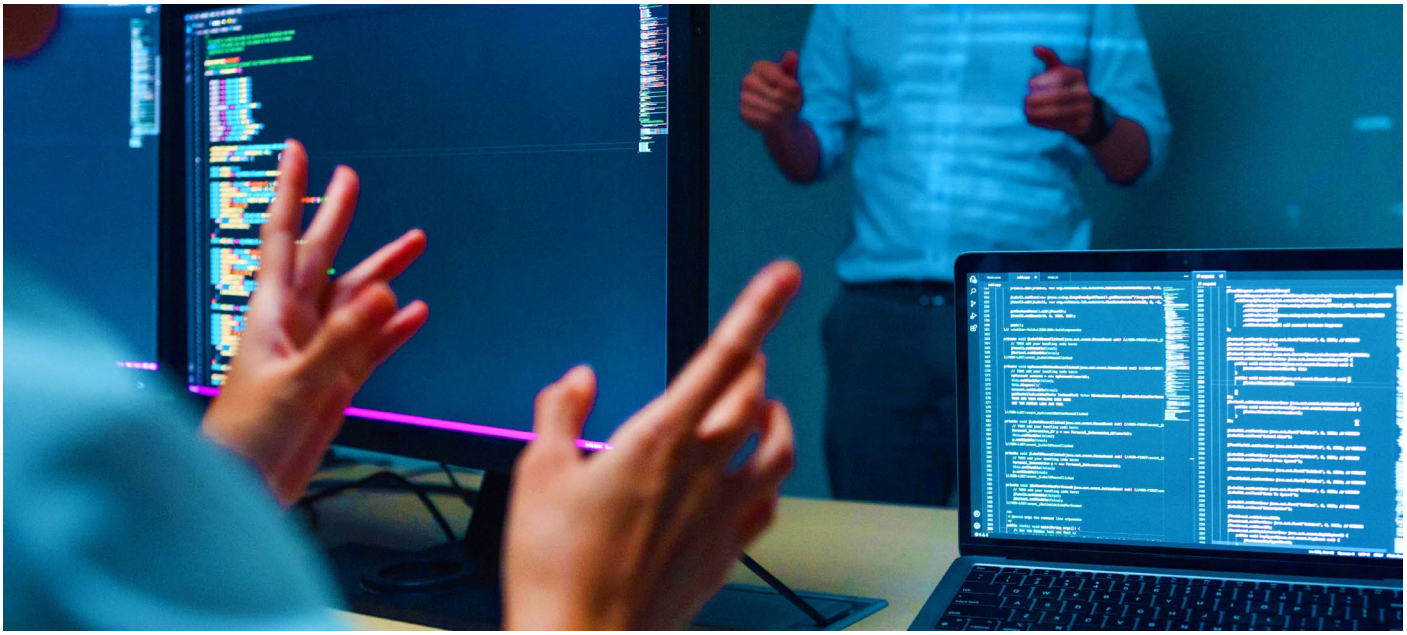
– Digital inclusion, or the equitable and safe access to and use of digital technologies, is another facet of sustainability that emerged in workshop discussions, with AI highlighted as likely to accelerate the divides between haves and have-nots. Participants repeatedly noted that technology upskilling and education (as noted in the previous finding) will be critical to working towards digital inclusion and must be pursued aggressively to protect the most vulnerable, reduce inequality between skilled and unskilled labour, reduce employment-driven migration and unrest, encourage stability and even reduce transnational cybercrime by redirecting potential criminals towards productive pursuits.

1.3 Regional variances

A major observation of Cybersecurity Futures 2030 is that digital security is being reframed as enabling humans' capacity to trust each other, technology and institutions at the speed of innovation. Different societies will respond to this challenge in different ways but considerable global consensus was found on the notion that operational progress on trust will play out across four prominent (and intertwined) thematic areas: regulation, privacy, tech adoption and the relationship between the US and China superpowers. The outlook of participants on these thematic areas fell into clusters based on the level of economic and technological development, as summarized in Table 1. These outlooks are likely to shape the choices and actions that policy-makers take in the coming years.

TABLE 1 **Outlook on regulation, data privacy, technology adoption and the US-China relationship, clustered by level of economic development**

Category	Developed economies	Emerging economies	Developing economies
Regulation	Tech regulations are discussed as protection against Big Tech encroachment	Focus on regulatory agility (match innovation)	Being used as a testing place because of lack of regulation; lack of capable governance
Data privacy	Data privacy is important, but so is data-sharing; balance between public good and individual interest	Worry about loss of data control	Focus on gaining control of data
Technology adoption	Focus on expanding innovation to stay on the cutting edge	Focused on control of tech access and production	Need for tech access for population
US-China relationship	**US:** A US-China alignment could cause realignment of traditional US allies **Europe:** As a US-China détente increases, tech innovation increases **Singapore:** Continued friction opens strategic opportunities to be a trusted intermediary and for independent political and economic relationships with both states	As a US-China détente increases, tech innovation increases Continued friction opens strategic opportunities to be a trusted intermediary	Worry about data privacy with Chinese technology (which is ubiquitous in most countries); worry about long-term costs of Belt and Road initiative



2 What's next? How to use this report

To put this report's findings into practice, decision-makers should evaluate how the changing cybersecurity landscape will impact their priorities.

The purpose of holding workshops in six very different places around the world is to uncover insights that can guide leaders from all geographies and sectors on what they can do to prepare for the digital security landscape of 2030 and beyond. What follows is a list of common strengths and vulnerabilities that participants noted mattered most when countries, businesses and individuals look towards their future risks and opportunities. This is followed by a list of objectives for anyone trying to mitigate risks and position themselves to take advantage of opportunities to improve digital security in the coming decade.

2.1 What strengths matter

- To thrive in an era of increasing digitalization, organizations will need to ensure they have a stable and secure supply chain of resources, including technology components and raw materials, as well as skilled, affordable workers. Resilient supply chains will help protect organizations from the social, economic, environmental and political volatility that participants believe are part of the global near-term future.
- As artificial intelligence and other technologies advance in the coming years, it will be more important than ever for companies, governments and other organizations to establish effective digital policies and regulations that demonstrate clear and stable priorities. Participants cautioned against over-regulation and contradictory regulation but they were emphatic that stable, internally consistent authorities are pathways for leaders and organizations to earn and maintain trust.
- The future is uncertain and, for many, the recent past (e.g. a global pandemic, increased cyberattacks, increasing polarization and military conflicts) has been a challenging time for cybersecurity. Participants noted that resilience, humour and optimism about the future and the opportunities that await those willing and able to seize them are critical in the run-up to 2030.
- Participants noted that humans need assurance that truth is attainable if they look in the right places. Having a digitally literate public and customer base that is media savvy and inoculated against MDM will be a source of strength for organizations that wish to succeed in an environment of continued deep fakes and other technology-based methods of degrading trust.

2.2 What weaknesses matter

> An inability to overcome social engineering will increase polarization, erode trust in digital products and platforms, and leave organizations in a weakened position.

- Collective failure to mitigate climate change and incapacity to adapt will limit innovation and technology adoption and will deprioritize cybersecurity. A continual cycle of preparing for, responding to and recovering from natural disasters and other climate-related challenges is a key weakness for the digital security landscape, as it will mean fewer resources to commit to promising security ideas and endeavours.
- Too much "digital consumerism" can be a weakness when it results in a dependency on the largest tech firms or on technology products and services exported by other countries. Organizations and countries alike should carefully consider the advantages of investing in innovation before automatically using market-ready solutions.
- An attack surface comprising a large number of people exposed to social engineering is a key weakness. Declining trust was a theme throughout all workshops. Participants noted that an inability to overcome social engineering – whether from internal or external sources – will increase polarization, erode trust in digital products and platforms, and leave organizations in a weakened position to solve other challenges and seize new opportunities.
- Economic and political unrest may be an obvious weakness in many ways, but in the context of digital security it had special salience for participants as a key impediment to the ability of companies and countries to attract external talent. Unrest was also seen as a vulnerability that reduces country and company attractiveness as partners to other nation-states and major firms.

2.3 What objectives matter

- Organizations should strategically plan to diversify their supply chains and engage in internal capacity building to limit impacts of uncertainty and instability. Whether the organization is a country or a company, leaders should ensure that this planning includes ways to counteract potential downsides, including becoming isolated from potential global partners.
- Digital inclusion is a core concern of the next decade. Leaders should actively look for ways to ensure that emerging technologies help the general population, for example by stabilizing national economies, addressing high costs of living, providing food security and advancing renewable energy.
- Leaders of all organizations should invest in education for the general population (media literacy, cybersecurity hygiene) and in job training to upskill a digital workforce. A well-educated public and workforce will serve to reduce the attack surface and help immunize populations from the increased variety, volume and technological sophistication of future MDM campaigns.
- While maintaining a highly educated public will help, there is no substitute for actively fighting against MDM and preventing the negative impacts of advances in AI technology and deployment. Leaders will need to strategically and tactically use regulation to guard against the downsides of AI products as they rise in prominence and take meaningful measures to combat MDM before it further degrades trust and unity.
- Complex problems demand complex solutions and the path to 2030 includes a host of complex problems. Countries should form and strengthen trusted research institutions, particularly in less-developed economies, to support governments in addressing the most challenging social and technical cybersecurity problems of 2030.

Based upon their priorities, different actors will choose different actions to play to their strengths, manage weaknesses and pursue objectives. Table 2 provides an example of the kinds of priorities that emerge from the trends identified in this report and possible actions that leaders could take to adapt.

The next phase of this project will focus on working with decision-makers to generate additional priorities and thinking more broadly about how findings from this report could reshape organizations' futures. Grappling with these kinds of questions should be a defining focus in 2024 for C-suites, boards and government agencies internationally.

TABLE 2 | **The kinds of priorities that emerge from the trends identified in this report and possible actions that leaders could take to adapt**

If	Then
You believe in global access to cyber self-education…	Take steps to create memorandums of understanding (MOUs) with universities and training institutions and create incentives for learners to complete.
You decide to focus on developing homegrown cyber talent…	Prioritize upcoming workforce issues, including training and upskilling, and find ways to balance self-sufficiency with strategic partnerships.
You agree that having a cyber-educated general population is critical…	Focus on educating the next generation and training all citizens to have a minimal level of cyber-literacy.
You hope to attract international skilled cyber labour…	Target key partnerships to make your markets and cost of living stable and attractive to those workers and brand yourselves as innovators to attract labour to your country or company.
You hope to attract displaced or replaced unskilled cyber labour…	Develop programmes to upskill workers who are available but not trained and provide support for integration.
You want to limit transnational cybercrime…	Find ways to prevent mass unemployment caused by shifts in automation and demands for higher-skilled labour.
You want to prevent the digital divide from widening the wealth gap…	Make sure you are bridging socio-economic gaps with technology protections (e.g. better medical care for all), instead of allowing technologies (like AI) to exclusively provide benefits to the wealthy and powerful.

Contributors

Lead authors

Ann Cleaveland
Executive Director, UC Berkeley Center for Long-Term Cybersecurity

Alan Cohn
Partner, Steptoe & Johnson

Matthew Nagamine
Manager, Strategic Partnerships, UC Berkeley Center for Long-Term Cybersecurity

Dawn Thomas
Co-Director, Center for Emergency Management and Operations; Director, Center for Critical Incident Analysis, Institute for Public Research, CNA

Alison Rimsky Vernon
Senior Research Scientist, Organization, Roles and Missions, CNA

Additional contributors

Joanna Bouckaert
Community Lead, Centre for Cybersecurity, World Economic Forum

Akshay Joshi
Head of Industry and Partnerships, Centre for Cybersecurity, World Economic Forum

Acknowledgements

The authors are grateful to the many individuals and organizations who have engaged in Cybersecurity Futures 2030. We would like to thank the staff and leadership at the World Economic Forum's Centre for Cybersecurity for their collaboration throughout this process, with special thanks to Joanna Bouckaert for programmatic support. Thank you to Andrew Reddie and Ruby Booth for leadership and expertise in scenario development. We thank CNA's Institute for Public Research and Steptoe & Johnson for their contributions of time and expertise. We would particularly like to thank our workshop hosts: the Dubai Future Foundation, CNA's Institute for Public Research, the organizers of CyberTech Africa, the Observer Research Foundation, CSA Singapore and the academic and NGO community in Switzerland, including Swissnex, the CyberPeace Institute, the Center for Digital Trust (EPFL), the Center for Security Studies (ETHZ) and the University of Geneva. Most importantly, we would like to thank the community of experts from industry, government and civil society who engaged in our workshops, contributed ideas and critiques and helped derive and synthesize the insights from this process.

We are grateful to our corporate partners, Fortinet, Meta, Okta and Repsol. This project was made possible by their gifts in support of independent academic research.

Production

Danielle Carpenter
Editor

Laurence Denmark
Creative Director, Studio Miko

Xander Harper
Designer, Studio Miko

Charles Kapelke
Editor

CLTC's mission is to amplify the upside of the digital revolution, help decision-makers act with foresight, and expand who has access to and participates in cybersecurity. Housed in the University of California, Berkeley, CLTC works on multiple fronts to anticipate the cyber challenges of the future and articulate solutions that allow the world to adapt and prepare.

CNA is an independent, non-profit research and analysis organization dedicated to the safety and security of the United States. The CNA's Institute for Public Research supports civilian government agencies in justice, public health, emergency response and other critical fields.

Endnotes

1. McCallum, Ken, *Emerging Threats, Innovation, And Security,* 17 October 2023, panel presented at Talks from the Hoover Institution, California.
2. Saxenian, AnnaLee, "From Brain Drain to Brain Circulation: Transnational Communities and Regional Upgrading in India and China", in *Global Labour in Distress*, Volume I, edited by Pedro Goulart, Raul Ramos, and Gianluca Ferrittu, 83-119, Palgrave Macmillan, 2022.

WORLD ECONOMIC FORUM

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