CYBERSECURITY FUTURES 2030

SCENARIO NARRATIVES AND READING GUIDE

DECEMBER 2023

Contents

Background **3**

Scenario 1—Pebble in the Network **4**

Scenario 2—The Caves of Steel **8**

Scenario 3—Prelude to Risk **12**

Scenario 4—The Naked Sun **15**

Background

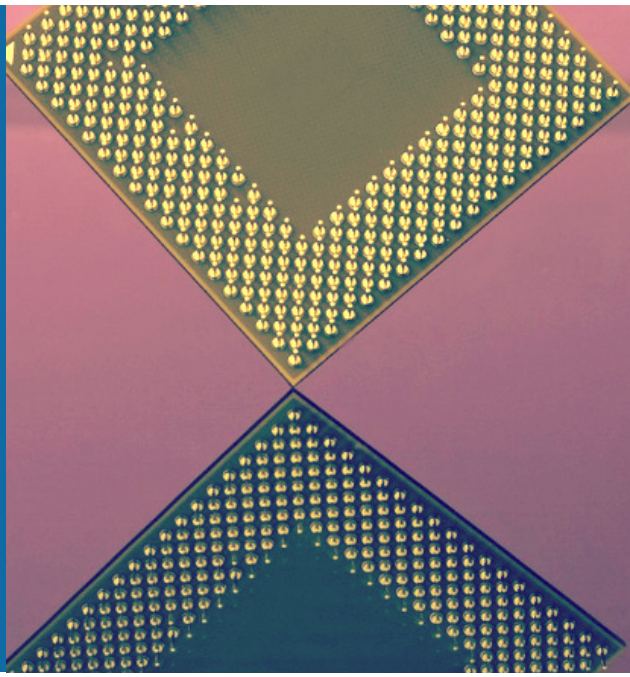
This document contains four scenarios that describe alternative futures in which the cybersecurity problem set that we know today has changed in distinctive ways. These scenarios were created by the Center for Long-Term Cybersecurity as provocations for our Cybersecurity Futures 2030 initiative.

Scenarios are not meant to be predictions. Rather, scenarios are tools for ordering perceptions about alternative future environments in which today's and tomorrow's decisions will play out. The purpose of these four scenarios is to sketch an imaginative map of the possibility space that cybersecurity decision-makers will navigate over the next five or so years. You can think of each scenario as a model that isolates a few critical driving forces; highlights how those driving forces change what people and organizations do; and then adds complexity by factoring in social, technological, economic, political, and/or environmental variables to build a plausible narrative that reveals how systems (human, political, technical, etc.) could evolve in the coming years. As with any model, the payoff is a set of hypotheses, in this case about the opportunities and challenges that will arise for organizations and individuals at the intersection of technology and society between now and 2030.

We have included reflections and a reading guide to accompany each of the following scenarios, summarizing global viewpoints on why these stories are happening, what else would be logically connected to or divergent from the main plot lines in various parts of the world, where blind spots lie, and how influential actors in business, government, and civil society might react and respond.

We hope these materials will help stimulate dialogue about the changing digital security landscape as you use these scenario tools in your own work.

Pebble in the Network



It is the evening of Sunday, 5 January 2030, and the question on the minds of experts, commentators, and industry leaders is, has the consensus of the 2020s finally reached its fraying point?

That consensus, which evolved from the hardening of positions in Washington, across Europe, in Moscow, in Beijing, and elsewhere in the wake of Russia's 2022 invasion of Ukraine, was a gradual coalescence of the US, Europe, and much of Asia on a technological trend line that would look familiar to a government official or business or civic leader: the centrality of semiconductor-based chips to the advancement of technology. By the mid-2020s, it was clear that the development of emerging technologies based on these chips — like AI, the internet of things, augmented reality, and digital assets among others — had generally benefited humanity. In this world, many nations have aligned with the US and Europe in continued cooperation on technology innovation, while other nations have become the transit points and trading posts between the West and countries that opted for other paths, such as Russia, Iran, India, and China. In the West, governments have seen a sustained, and surprising, stability and continuity of leadership and direction. Populism and nativism continue to animate political debates and elections, but remain simmering rather than erupting into large-scale change.

Not that this consensus has been without its challenges. Taiwan Semiconductor Manufacturing Company's (TSMC's) investment in production to Europe was a result of Washington's decision to send additional troops to the island of Taiwan in response to China's political blockade in 2028 — a blockade that ultimately failed to deter US resupply of military resources. The fallout from this political blockade, in which China announced that US and Australian naval vessels and Taiwanese military vessels would not be allowed access to the island, continues to stymie efforts to address international peace and security challenges at the UN, leading some analysts to fear that the institution may crumble. As Russia and Ukraine dug in for a long fight lasting throughout the 2020s, Russia's lack of compliance with international law has also led to the collapse of various United Nations (UN) Group of Governmental Experts (GGE) and Open-

Ended Working Group (OEWG) processes that were previously focused on addressing the challenges posed by emerging technologies. In some cases, enough of a consensus remained among the US, Europe, and others to continue the work of these bodies in other multilateral gatherings, but without China, Russia, Iran, and India.

By 5 January 2030, however, enough irritants had been introduced into the system to raise the spectre that the consensus would falter. Following riots throughout the day on the Prager Strasse, in the heart of Dresden, Germany, four hooded figures are captured on closed-circuit television (CCTV) slipping past security at TSMC's new semiconductor manufacturing plant.

The Bundespolizei are immediately notified and race to the scene. The German Federal Office for Information Security (BSI) is also informed and spends the next six hours engaging with the European Union Agency for Cybersecurity (ENISA), as they are convinced that these figures were seeking to sabotage the plant, which is responsible for supplying much of Europe with the advanced chips required for AI firms, manufacturing plants, the aerospace sector, and consumer goods.

Within hours, news of the attack leaked to the *Bild* newspaper, and articles rapidly appeared online trading theories as to who might be responsible. Online debates consider the identities of the infiltrators. Some suspect they are Chinese operatives seeking to undermine TSMC's operations abroad amid tightening export controls on semiconductors, as well as continued restrictions of Advanced Semiconductor Materials Lithography's new photo-lithography systems, which are required by the next generation of semiconductors used in both military and civilian applications by the West. Others guess they are Russian proxies seeking to sabotage Europe's industrial base as Russia's "special military operation" in Ukraine approaches its eighth year. Still others suspect they are simply cybercriminals seeking access to intellectual property with the intention of selling it on the burgeoning black market to buyers in an increasingly isolated Russia, Iran, and India. *TikTokEUS* videos appear to support the cybercriminal theory, with those from populist, anti-immigrant groups suggesting that Germany is to blame for welcoming TSMC to its shores in the first place.

ENISA's cable to the new US National Cybersecurity Agency (NCA), an agency set up to harmonize US responses to cyber incidents following the Inch Pipeline attack that halted gas supplies across the country, describes an injection attack on TSMC's core network that overcame its AI-enabled cyber defenses and autonomously sought both horizontal and vertical privilege escalation. Hungary and Austria (consistent with their stance throughout the late 2020s) suggested this cable should not have been sent.

Meanwhile, the Taiwanese National Center for Cyber Security Technology (NCCST) has also confirmed that it can see signatures of a similar attack on TSMC systems in Hsinchu, though it remains unclear to NCA analysts whether it is the same variant from the Dresden attack. Given that all internet traffic to Taiwan from Europe is now routed via North America, the NCA has decided to fly analysts to TSMC's Phoenix, Arizona plant from its headquarters in Arlington, Virginia in an attempt to ascertain whether the tools used in the attack in Germany have spread.

For German Chancellor Scholz, already under pressure to resign from the Green Party amid Germany's failure to lead on European and global climate change initiatives, it is an embarrassing moment. The intrusion is even more embarrassing given the recent decision by TSMC, under instructions from Taipei, to manufacture 2-nanometer (nm) semiconductor chips at the facility for the European and North American markets (finally displacing the US plant in Arizona in the process).

All of this takes place against the backdrop of increased uncertainty in Asia, as it also remains unclear whether Beijing will finally make a more determined attempt to retake Taiwan, rather than simply the war of words, encroachment on surrounding islands, and political blockade strategy that China pursued throughout the 2020s, and much depends on whether recent protests among the Chinese population will influence President Xi's stated goal of reintegrating the island by 2033. For some commentators, belligerent action has become more likely.

REFLECTIONS AND READING GUIDE: PEBBLE IN THE NETWORK

Pebble in the Network is a story about the fragility of the global consensus on semiconductor technology in the year 2030. A cyberattack on a critical semiconductor manufacturing plant in Germany raises suspicions and tensions between major geopolitical players, highlighting the vulnerability of supply chains, frayed international relations, and the potential for disruptive events to impact global stability.

Participants in multiple workshops recognized this as a world in which trends that advance technology development have empowered innovation and economic opportunities that benefit many major global actors. A common concern was the challenge of maintaining trust in an increasingly complex digital environment. In the UAE, participants highlighted the potential for the Middle East region to play a mediating role for major global powers that struggle to find common ground. In both Washington, D.C. and the UAE, discussions stressed the potential for geopolitical realignment caused by disruptions in the digital environment, and emphasized the need for trust-building and strong cybersecurity standards in this changing landscape. Rwanda focused on the impact of digitization on the African continent, including challenges related to dependency on foreign technology and the urgent need for education, awareness, and upskilling. In India, there was an emphasis on the importance of diversifying technology supply chains and strengthening democratic institutions to mitigate cyber risk. Singapore stressed the significance of supply chain security, sustainable tech, and alignment of their country's interests with major global powers. These insights collectively highlight the need for a balanced approach to technology development, proactive building and maintenance of trust, and strengthened cybersecurity policy.

As you review this scenario, you might consider the following questions:

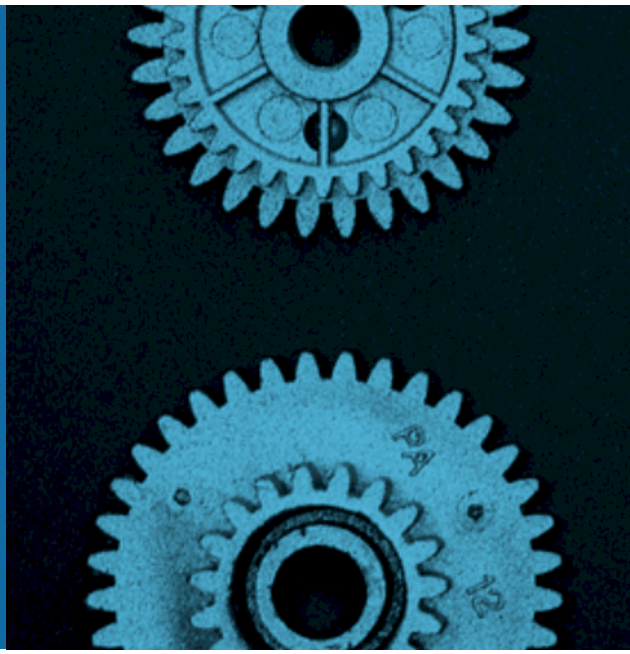
- → In your view, how do the geopolitical realities within this scenario impact efforts to govern the internet and secure supply chains for important technologies, like semiconductor chips?

- → What are the prospects for an intergovernmental response to this crisis, and what role do private

companies play in such a response?

→ The scenario suggests that regional power dynamics are increasingly influential in shaping digital security norms. What are the opportunities for nations at the crossroads of major powers to (1) shape the direction of multilateral activity, (2) emerge as leaders in digital policy and internet governance, and (3) serve as hubs for technology innovation?

The Caves of Steel



It is Thursday, 16 May 2030. Raymond signs off from his terminal at 21:00 sharp. Walking to his Rivian R3, his feet clack against the floor — recently polished by an autonomous robot responsible for keeping his first-floor office hallway clean, but only for his benefit as the only human employee left at the plant. He exits the building alone, his car the only one left in a parking lot built for thousands of workers.

All of this plant's workers were gradually replaced following a decision in 2027 by ARMcorp to reduce its human workforce. Those responsible for manufacturing electric vehicles for VolkTes and the Chinese Geely-Mercedes (the latter having benefited from the recoupling of the Chinese and American economies over the prior two years) have been replaced by 10,000 network-connected computers and an army of assembly line robots, with one human worker overseeing this metaphorical lighthouse.

As he winds his way home in Santiago Tianguistenco, Mexico, the town is empty. This town, which boasted 64,000 people in 2020, is now home to fewer than 20,000. The elimination of thousands of jobs at the former Mercedes-Benz plant created a chain reaction. With the town's economic lifeline gutted, tens of thousands of residents left for Mexico City during the late 2020s. Local news anchors on FOX-Televisa parrot alternating populist talking points blaming immigration on the US-Mexico border, stemming from the increasingly severe climate crisis, and the usual conspiracy of American-Chinese global domination and control.

This scene in post-industrial Mexico plays out in different forms the world over. Nations that pursued manufacturing and mining as a pathway to sustainable economic development were left with the ladder pulled up in front of them. American-Chinese robots now do all the work.

Those able to invest in and play a role in building AI tools have become the oligarchs of 2030, with the distribution of benefits from the combination of robotics and autonomy benefiting only a few. This is

despite efforts in the last throes of the Biden Administration to increase taxes on the major technology companies, who nevertheless managed to leverage their market power to buy out technology from the smaller AI firms while developing significant R&D efforts of their own.

Despite promises that these technologies would reshape society and usher in a new era of invention and creativity, the applications of these tools tend towards the mundane — with much of the profit-generating AI applications focused on replacing human labor. French and German activists within the labour movement had long argued that the focus on these applications would be too damaging for the global market to bear without significant upheaval, but few could have expected the significant political shifts that would follow.

In the 2026 US midterm elections, populists on both sides of the aisle rose to power — but while both sides agreed the country faced significant problems, populists from different political parties could not agree on the cause or the remedy. This stagnation contributed to a hotly contested election in 2028 that ultimately led to a Republican coalition focused on addressing the rise of crime associated with large increases in unemployment, closing US borders, and abandoning both Ukraine and Taiwan on the global stage. This isolationist streak also spread into US engagement with international bodies — with the US government occasionally failing to participate in intergovernmental meetings of the UN, International Monetary Fund (IMF), and World Bank, instead sending private firms to "observe" on its behalf. This has been particularly true in forums like the IMF, the Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Governance Forum, where large technology companies have a voice — one that is increasingly stronger than that of the government, in some cases — on the future of internet technology. The US election also made clear that the distance between disinformation and media — had there been any in 2023 — has now closed. To the extent that public discourse is controlled, at least in the US, social media platforms like X and OpenMeta set the rules, with algorithms continuing to sow division in a divided electorate that blamed one another for the collapse of the US economy for all but a select few.

As part of her crackdown on crime driven by widespread labour displacement, US President Hinson — like executives across the globe — has become increasingly comfortable with leveraging the tools of state power to surveil members of the public. A violent attack on the US Capitol Building on 6 January 2026, in particular, led the Department of Justice and Congress to allow for more intrusive monitoring of citizens' online behavior, and the collection of their data far beyond those permissions afforded by the interpretation of the Fourth Amendment in 2023. To justify this change in policy, President Hinson looked to the policies of PM Sunak in the United Kingdom and President Le Pen in France, who had faced similar challenges in the years prior to her taking office.

REFLECTIONS AND READING GUIDE: THE CAVES OF STEEL

The Caves of Steel scenario depicts a world in which an economic recoupling between China and the US has led to major advancements in robotics manufacturing. Automation and AI have led to mass

unemployment and a concentration of power among technology giants. This scenario highlights the consequences of technology-driven economic displacement, the rise of populism, and the erosion of privacy and civil liberties as governments use surveillance tools to address resulting societal challenges.

The anticipation of significant advancements in AI and automation technologies was a common source of both hopes and fears for participants across all of the global workshops. Participants felt that these technologies will change governments and societies in critical ways in the coming years, but are uncertain about what those outcomes will look like.

In the UAE, participants noted that the recoupling of the Chinese and American economies could result in reduced geopolitical tensions. Challenges related to disinformation, a global surge of populist movements, dependencies on major platform companies, and irresponsible AI implementation were also highlighted. In the Washington, D.C. workshop, we heard some similar concerns, with specific attention to the unwieldy growth rate of big tech, the growing role of algorithms in public discourse, the future of AI-augmented cyberattacks, and the potential for AI to widen the gap between the haves and have-nots. In Europe, participants' responses to the scenario criticized the dominance of tech giants and the overwhelming influence of social media platforms on public discourse. Discussions in Rwanda recognized these challenges, but also saw AI and the US-China recoupling as opportunities to move the needle on some of their most fundamental challenges, with less pressure from China and the US to "pick a side."

India and Rwanda have their own set of challenges related to rapid digitization within their regions, which points to cleavages between digital environments in developed, emerging, and developing economies. In response to this scenario, participants in India thought regions and governments with advanced digital infrastructure and rich data ecosystems would be better positioned to seize the opportunities related to advancements in AI and automation.

Singapore noted that countries with more economic diversity would be more resilient to the impacts of labour displacement in this scenario, and thought that individuals who can leverage AI tools in their work, or who provide non-technical personal services, will have the upper-hand as technology-induced job displacement intensifies. They also noted that trust between citizens and the state is at a low point in *The Caves of Steel*, leading to concerns about the average citizen's privacy and misalignment of public and state interests.

Collectively, these insights represent an urgent call for decision-makers to enforce strong and ethical AI policy, for businesses to develop and implement new technologies responsibly, and for individuals to be proactive about the changing job market, with all actors sharing a responsibility to better understand and tackle disinformation challenges. In spite of the consternation about the future impacts of AI, there is a sense of optimism that there is still a window of opportunity for us to tilt the scale in the right direction.

As you review this scenario, you might consider the following questions:

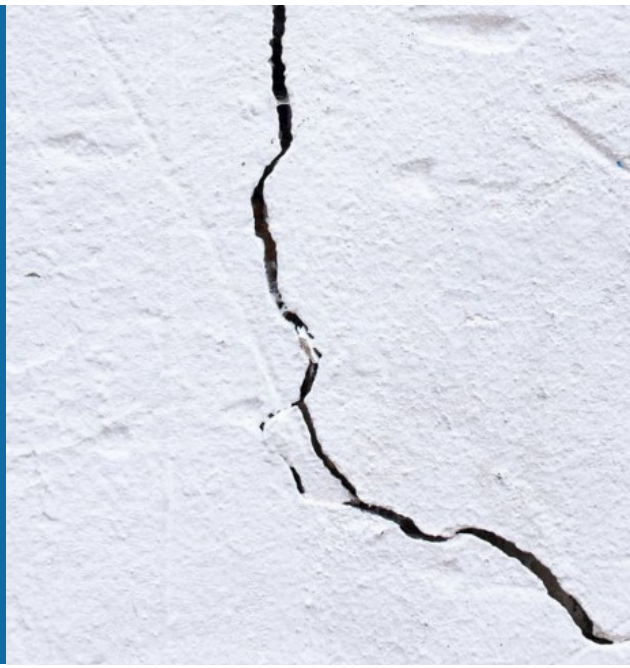
- What are some opportunities that AI has created within this scenario, and are there ways to make those opportunities beneficial to a wider swath of the population?

- What challenges are caused by the rising political power of private technology firms, particularly in shaping national and global governance arrangements? What opportunities does it create?

- How does the dominance of US-based social media platforms affect the fight against MDM in other countries? Are there any international governance tools, political or technocratic, to address MDM?

- Some economies may be more resilient to technology-induced job displacement and/or its impacts. What attributes do these resilient economies have, and can vulnerable economies implement strategies to build resilience?

Prelude to Risk



'DODGY CHINA CHIPS GIVE DEMS VICTORY'

Thus reads the headline of *The New York Post Online* on Wednesday, 6 November 2030.

The story, quickly picked up by all major and alternative conservative outlets, reveals that new ES&S TRUST voting machines, subsidized by the United States Trustworthy Election Act of 2026, and purchased by many Southern districts during the runup to the 2030 election, included chips made by the Chinese manufacturer, Nexperia. *The Post* asserts that the inclusion of these chips was part of a deliberate conspiracy to defraud the Republican Party across the South. The strong showing by Democratic candidates in Georgia, North Carolina, and Tennessee is cited as proof of fraud.

The ripple effects to ES&S TRUST are immediate and widespread as dozens of governments throughout South America and Europe cancel contracts. The company had gone on a massive bidding spree after decoupling legislation swept NATO countries and other aligned governments. Now, the security of those machines — indeed, their compliance with legislation mandating "friendshored" supply chains in critical infrastructure — has been thrown into question. ES&S TRUST's stock sheds 60% of its value over the coming month.

The Trustworthy Election Act of 2026 was passed with the explicit intent to subsidize electronic voting machines that produced a verifiable audit trail. Independent reviews of these new TRUST-certified voting machines and their audit logs show no evidence of bias, but do uncover significant security concerns regarding older ES&S machines, though due to the nature of these machines (i.e., no audit mechanism), it is impossible to determine their impact on the midterm elections.

A bill is introduced in the US House of Representatives to invalidate votes cast on the TRUST machines.

A month later, Senator Merryweather Grant, a Republican from Texas, introduces a bill in the Senate to require all voting machines used in the United States to be built with US-made parts. This legislation threatens to overturn the détente between Washington and Beijing that followed President Xi's retirement in 2028.

. . .

On Christmas night of 2030, a video posted to WeTube appears to capture Senator Grant asleep at the wheel of his self-driving car when the car strikes an eight-year-old child. The girl is later identified as Octavia Olamina. In the video, which quickly spreads on US social media platforms, Senator Grant's face in profile is clearly visible as he accelerates away. In the hours following the video's release, however, two conflicting narratives arise.

The first narrative, widely reported by sources including *The Washington Post*, *BBC America*, and *The New York Times*, is supported by interviews with the Olamina family, and highlights details of Senator Grant's past history of drunk driving — a topic that first came to light during his Senate run in 2024. Protesters gather outside the Senator's Washington, D.C. residence.

Right-leaning media outlets are advancing a second narrative, as *Fox News Network* and *The New York Post Online* broadcast a video in which the driver of the vehicle that struck Octavia Olamina is a Hispanic man who was soon identified by *Fox News* as Jorge Guzman, an undocumented migrant with a criminal record in the United States and Mexico. The video of Senator Grant is cast as retaliation and further evidence of conspiracy.

On 4 January, the FBI and other US intelligence agencies identify specific, credible threats to the lives of the newly elected senators from North Carolina and Tennessee. Prominent figures on far-right media call for "a reckoning" — with the FBI noting an increase in internet chatter revolving around violent protests to take place across the country on 6 January, 2031.

REFLECTIONS AND READING GUIDE: PRELUDE TO RISK

The Prelude to Risk scenario portrays a divisive political landscape where the discovery of Chinese-made chips in US voting machines leads to accusations of election fraud. Manipulation of public sentiment through media narratives lead to escalating tensions, protests, and threats of violence. This scenario underscores the vulnerability of democratic processes to the challenges of disinformation.

Discussions in several workshop locations had varying perspectives on the driving forces, strengths, weaknesses, and digital security challenges that emerge from this scenario. Participants in the UAE identified widespread digitization and increased access to information as positive driving forces, but also expressed concerns about dependencies on major multinational technology companies. In Europe, participants thought positively about efforts to improve US-China relations, hoping that greater

cooperation between the two states would alleviate global tensions. European participants identified disinformation as a key agent of uncertainty and distrust and expressed a sense of urgency to build trust within and across democracies to counter disinformation. Washington, D.C. participants shared concerns about misinformation and "deep fakes," but saw potential for new technologies, like generative AI, to improve security for critical infrastructure (CI) and help to upskill workers.

The discussion in India focused on the pace and scale of digitization, with a focus on supply chain security and "secure-by-design" technologies. This scenario highlighted the importance of proactive measures to promote digital security and instill trust and confidence in technology and government.

As you review this scenario, you might consider the following questions:

- → What might the overall progress on security for critical infrastructure look like in this scenario and why?

- → How would the implications of this scenario change if the scenario were set in a different large democracy?

- → Considering the focus on disinformation and trust erosion in this scenario, what measures can be adopted by governments, tech companies, and civil society to maintain or rebuild trust in digital systems and ensure the security of online information?

The Naked Sun

It is 04:00 on Wednesday, 3 July 2030. The power in Makayla's home office has been out for six hours. She knows it likely won't come back on until evening, when demand for air conditioning has dropped with the sun. Makayla does most of her work late at night or in the early morning, though today she has been able to take some work calls on her phone, which she keeps charged with battery packs. The temperature in her Memphis, Tennessee home is well above 38°C, and even when the power returns, she won't turn on the air conditioning. The cost of electricity is just too high.

Makayla works for St. Jude's Children's Hospital as a bioinformatician researching tailored gene therapies. She is one of three researchers in her department, and she's hopeful that they may soon hire a fourth. If so, they are sure to get many high-quality applicants, since even high-skilled jobs are scarce these days. Bioinformatics is booming thanks to the introduction of Chat-GPT 86, which allows researchers like her to present refined queries based on a patient's unique genome and get custom therapies created in the enormous automated lab installed in the hospital's new insulated basement. While this use was initially challenged by privacy advocates, the EU, followed by other governments across the globe, recognized the widespread societal benefits of data collection and sharing. While some countries created safeguards as an attempt to protect citizen privacy, some jurisdictions provided private firms more freedom, leading to firms relocating some of their operations to those countries.

Thankfully for Makayla, the power will be on at the hospital, thanks to its massive generators and solar panels. It has to be, both to support patient care and to run the energy-hungry gene lab. But gas is prohibitively expensive thanks to the end of low-cost oil, which resulted from the wreckage of infrastructure in the Gulf of Mexico, fires in Texas, and the rise of the Chinese petroyuan following the collapse of the US dollar. Commuting downtown to the air-conditioned hospital is something she saves for days when the temperatures are higher.

Still, it could be worse. In the United Kingdom, with the pound's value in freefall, a wage/energy-price spiral has exacerbated an already severe cost-of-living crisis. The euro is widely used on the street, with WhatsApp groups frantically messaging new currency exchange rates. In Canada, government-subsidized energy has been running up the national deficit year after year. The Liberal government has resorted to paying Canadians to move out of small towns, where they use gas-burning furnaces, and into cities, where new construction is heated with hydro-electric and nuclear energy.

In the kitchen, Makayla's mother-in-law, Paola, puts away the groceries the drone just delivered and considers what to cook for the family's supper. These days, almost everything they buy is shelf-stable so that the outages don't cause food waste, which they can ill-afford with the cost of groceries climbing ever higher as the droughts continue into the fourth year. She starts *arroz con gandules* with *sofrito*, grateful that the old gas range doesn't require electricity to run. Nevertheless, she misses her own kitchen. She was forced to relocate when her home in Mayagüez, Puerto Rico was destroyed by the storm surge preceding Carlotta, one of the twin hurricanes to hit the island in 2029. Once-sleepy Memphis is now home to thousands of climate refugees, but few from Puerto Rico. Most, including their neighbors, the Hurstons, relocated from New Orleans and the US Gulf Coast after the hurricanes of 2026 devastated the region. Paola, like so many, hasn't been able to find steady employment. She is lucky that her son and daughter-in-law both have jobs.

Makayla's phone buzzes. It is her husband, Xavier, who is a machinist's mate in the US Navy. His aircraft carrier is currently on a tour in the Arctic patrolling the western edge of the Barents Sea — a geopolitical hot spot in the years since the collapse of the Arctic Council. Makalya is happy to be able to tell her husband that the rent on their home is only increasing 15% next year; they have both been worried that the high demand would mean a message from Berkshire Hathaway that their rent would increase by 25% again this year. A rise in 15% will cut into their budget, but 25% would mean moving yet again. She does not tell him about the shortness of breath she's been having. It's probably nothing, and doctors are expensive. They speak briefly about their child, who will be 15 years old soon and is already considering telecollege — good news, but a substantial expense. Xavier reassures her that Russia is unlikely to test US resolve, but Makayla points out that her news feed is full of saber-rattling on both sides. In any case, it's good to see her husband's face.

REFLECTIONS AND READING GUIDE: THE NAKED SUN

The Naked Sun scenario portrays a future in which advanced AI-driven medical research empowers the development of tailored gene therapies. Yet technological advancements have also exacerbated resource scarcity, climate change, and economic disparities, altering where and how people live and work.

Workshop discussions examined the intersection of technology, energy dependence, and climate-related disruptions, and how they might shape the daily struggles and opportunities of individuals, enterprises, and nations.

In the UAE and Singapore, participants were optimistic that climate change could emerge as a common enemy for global actors, especially for those who struggle to get along. Participants also discussed challenges, including technology-induced geopolitical disruption and resource misuse. In the UAE, participants worried that increased regional instability, political polarization, diversifying digital policy, and the potential for internet fragmentation could lead to more tribe-like societies.

European workshop participants found hope in this scenario in advancements in medicine and the potential for the spread of AI technologies to level the playing field for groups that have been left behind in previous waves of digitization. Workshop participants in Washington, D.C. identified issues related to cheap, easy, and lucrative cybercrime, and the rise of extreme virtual communities and fragmented media to fuel populist narratives that can sway public discourse. Participants in India felt that countries with a greater degree of self-reliance would have more resilience to challenges related to supply chain security and resource dependencies.

Participants across regions shared concerns about energy scarcity driven by computing demands and global digitization, the rising cost of living, and the effects of climate changes. Shared global standards and norms, transparent partnerships (both internationally and public-private,) and trust-building emerged as urgent priorities. While the web of challenges related to technology innovation, climate change, geopolitics, and sustainability are uncertain, the connections between these four issues are becoming clearer and more inextricable. On the other hand, we heard glimpses of hope about the potential for democratizing AI, advancing medicine, and achieving global cooperation. To realize these benefits, decision-makers must act now, with an intentional focus on promoting trust and transparency broadly — across governments, across sectors, between governments and their constituents, and between companies and their consumers.

As you review this scenario, you might consider the following questions:

- → This scenario is set in the United States. How might the events described impact individuals in other areas differently, and what options would private citizens in those regions have available to access more security?

- → What are the levers available to governmental decision-makers to improve security for a wider swath of residents of their nations? What options are available to the private sector to improve the outcomes for their business objectives and their employees?

- → What institutions are capable of improving the lives of people globally in this future? How might differing approaches to issues like climate change, immigration, or digitization impact these outcomes? Is a more unified, bifurcated, or fragmented approach more advantageous in addressing these complex challenges?

- → How should companies and governments think about the connections between innovation, sustainability, social change, and digital security? What kinds of partnerships should be created to develop effective strategies to combat challenges at these crossroads?