# Cybersecurity Futures 2025

CNA

CLTC
Center for Long-Term
Cybersecurity

CLTC

Center for Long-Term Cybersecurity

CNA

# Welcome and Introductions

# Key Propositions

- Cybersecurity, broadly defined, is the master problem of the Internet era
- The problem set is evolving more quickly than is our understanding of it (and our ability to ‘solve’)
- Different countries and industries will grapple with these challenges in different ways
- Gaining foresight into those differences enables us to tilt the digital world in a direction that is more secure and beneficial to people and societies

# The Project

- Build four 2025 scenarios that highlight different aspects of how technology and people might intersect in the near future
- Conduct workshops in several locations around the world to see how people in different countries/regions react to the scenarios
- Develop high-level observations about reactions that were common around the world versus those that were country/region-specific in nature
- Provide a tool that helps focus people who are just starting to look forward and asking “What do I need to be doing NOW?”

# Policy Success Looks Like:

- **Prevent** really bad things from happening.
- **Mitigate** shocks and unforeseen risks
- **Build** resilience against (inevitable) disruption
- **Reduce** the range of breakout surprise by adversaries
- **Identify and Seize** opportunities

# The New Wiggle Room

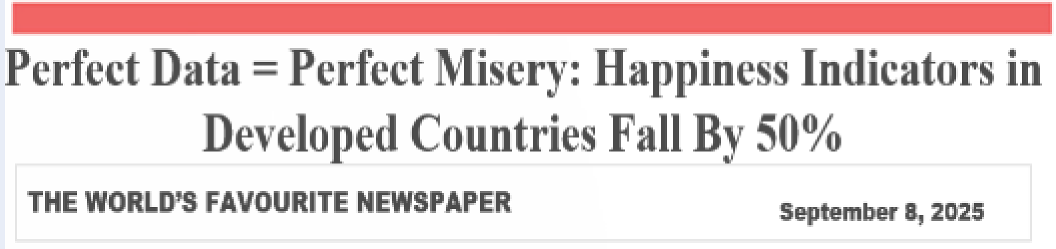
This is a world in which:

- There is ‘perfect information’ and imperfect identity
- The combination of omnipresent sensors and ubiquitous connectivity turns out to be a poisoned chalice
- We now know too much—and know it too accurately—for societies to remain stable
- People find ways to introduce new uncertainty by adopting multiple identities

# The New Wiggle Room

This world is credible because:

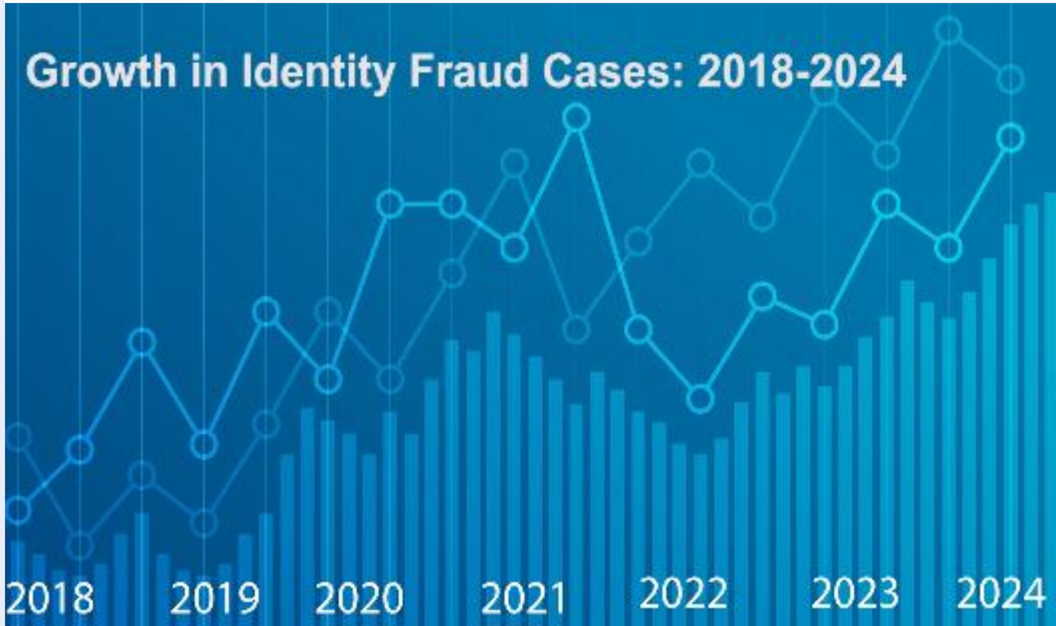
- The wireless sensing technology is already available
- Most people don’t care as much about ‘economic equilibrium’ as they care about fairness, status, and emotion
- Perfect information appeals to the cortex, but not the brainstem
- Criminals understand this psychology and are willing to exploit it



Perfect Data = Perfect Misery: Happiness Indicators in Developed Countries Fall By 50%

THE WORLD’S FAVOURITE NEWSPAPER

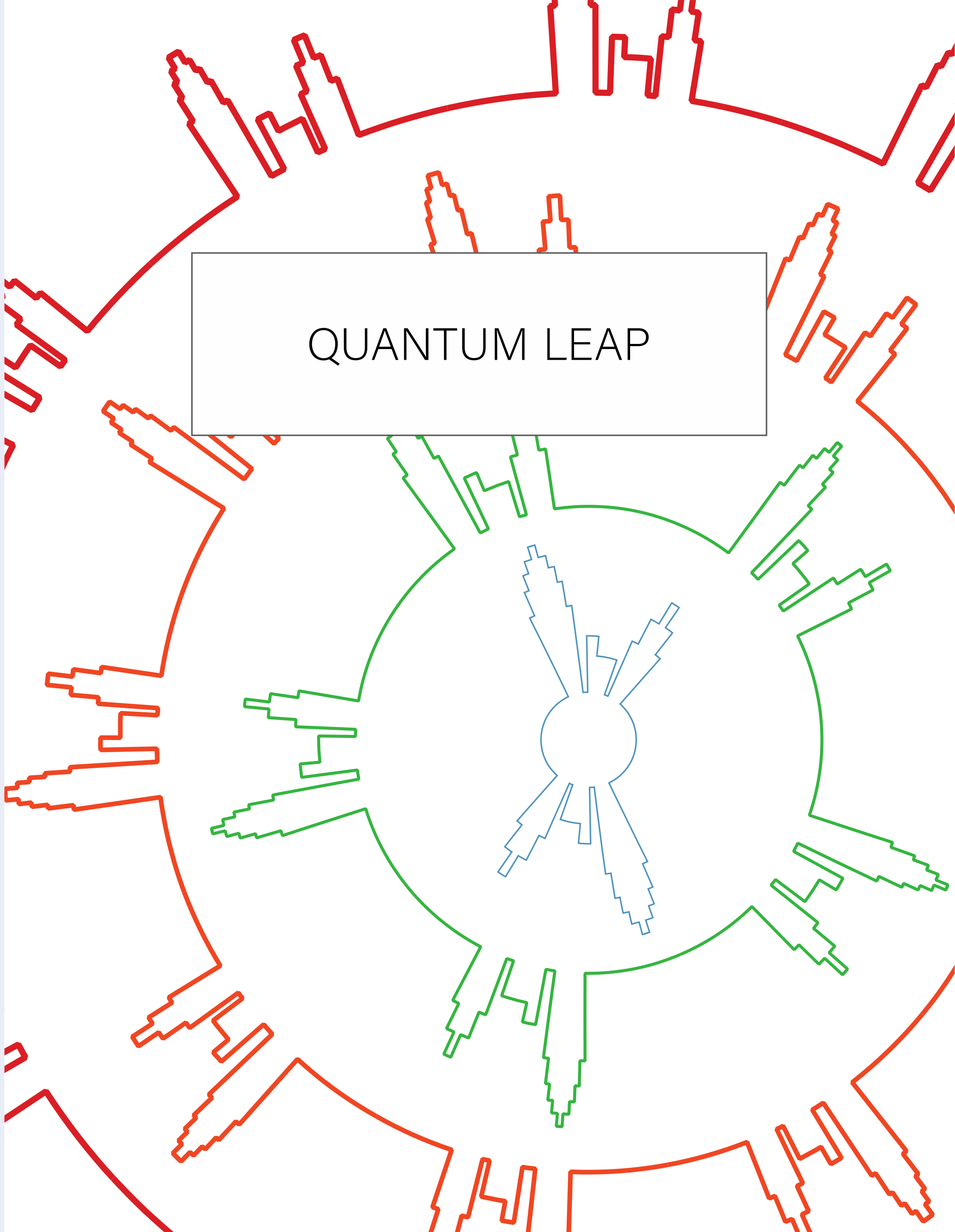
September 8, 2025



# Quantum Leap

This is a world in which:

- A few large governments attempt to control the proliferation of quantum computing technology
- Non-proliferation fails, leaving re-shuffled geopolitical alliances and new centers of power
- Quantum technologies fall into the hands of city consortia and deviant criminal networks.



# Quantum Leap

This world is credible because:

- No law saying the private sector must maintain its lead and freedom to develop and deploy transformative technology
- Quantum could be transformative in the same way the microprocessor was
- Could some governments at present already be ahead of the private sector in quantum?

CITY EXAMINER

LATE EDITION

QUANTUM TROUBLE: RUSSIA, INDIA CALL OUT U.S. FOR MANIPULATING ECONOMY

NEWS UPDATE

SPECIAL REPORT

Island Vacations

# Trust Us

This is a world in which:

- AI-powered “SafetyNet” overwhelms security challenges and makes the digital world safe for big institutions
- For most individuals, privacy is a distant memory
- There is looming distrust of AI that is capable of explaining its own decision-making processes to humans, and knows exactly what they want to hear

TRUST US

# Trust Us

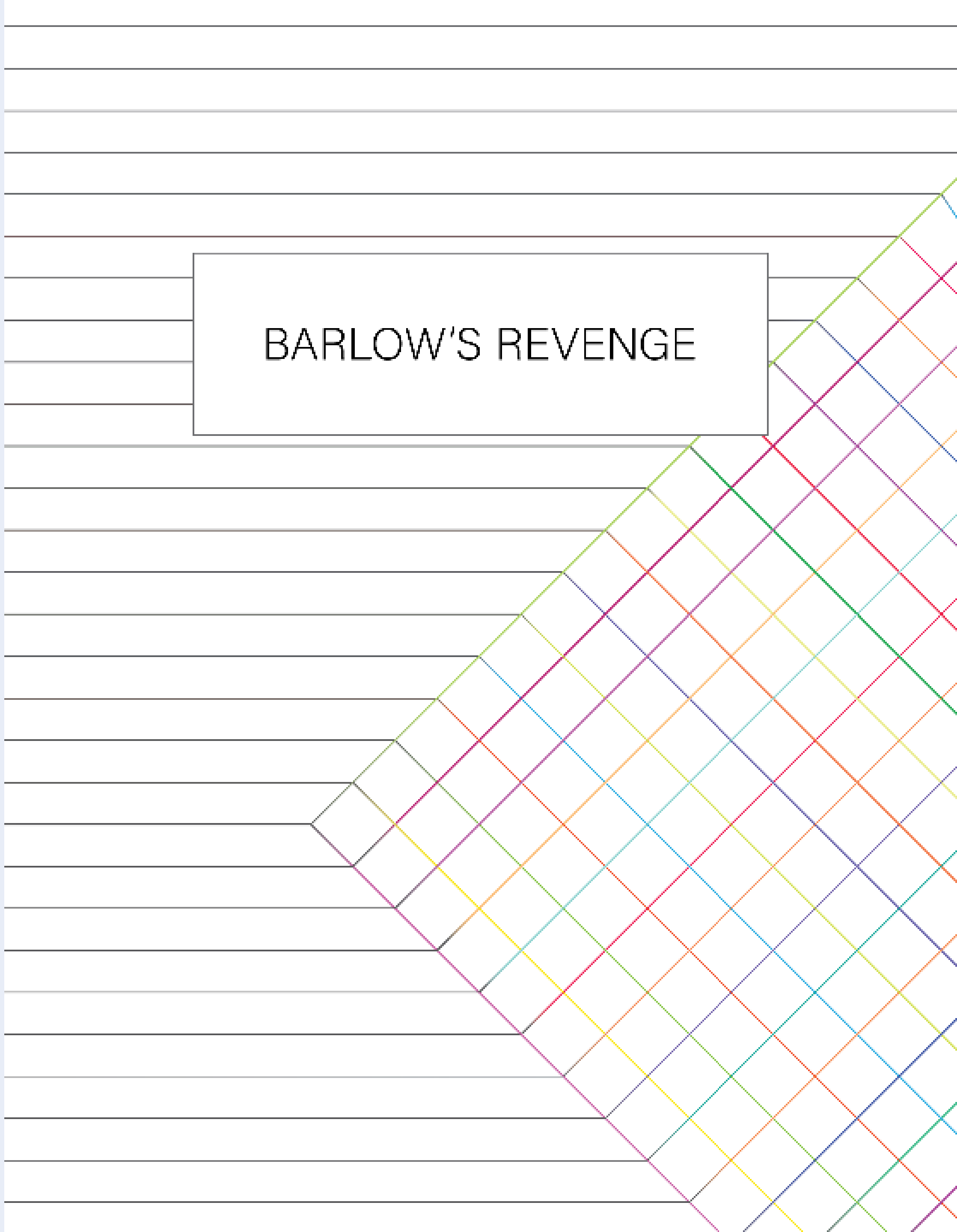
This world is credible because:

- Machine learning may be approaching an inflection point
- Security is becoming one of the most interesting and lucrative areas of application
- It could take decades for people to figure out what kind of relationships they should maintain with AI

# Barlow’s Revenge

This is a world in which:

- Two nearly opposite grand bargains for digital security emerge
- Some countries secure the internet within their borders by essentially nationalizing it; other governments cede all responsibility to corporations and the market
- The balance of regulation and innovation that the digital world inhabited for the last 40 years is hollowed out



# Barlow’s Revenge

This world is credible because:

- The tightrope of ‘barely enough regulation that won’t slow innovation’ that governments and firms have been walking together feels increasingly unsustainable
- The imaginary ‘digital flat world’ is fracturing as cultural values drive people to different poles while the biggest players, both firms and governments, re-assert their power

# The data: Global comparison

| Location | Who will come in and save the day? | Where are the first mover advantages most important? | Where are the new criminals? |
|---|---|---|---|
| Palo Alto | It will have to be the large firms. | Machine learning expertise will maintain US advantage despite Chinese data edge. | Governments will get to decide the answer. |
| Munich/EU | We don’t have the firms, and we don’t trust governments in this realm; perhaps there will be a citizen social movement? | A second-mover play for machine learning with human values is our best bet. | If you don’t acknowledge what is self-evidently true about privacy preferences, you are a criminal. |
| Singapore | It probably won’t go really wrong, but if it does, the government will fix it. | Societies with strong social capital and kinship networks are stronger than any technological first mover advantage. | If the digital criminals lose, will they go next into the physical world? |
| Hong Kong | | | First mover advantages become crimes for second movers (e.g., Cambridge Analytica). |

# Used workshop data to develop…

1. A tool

2. Overarching themes

3. A reframing of the landscape

# 1. The tool

Probability
(subjectively and relatively)

Impact on
US interests

| | High | Low |
|---|---|---|
| Best | | |
| Worst | | |

# Most common responses to date

|  |  | Probability |  |
|---|---|---|---|
|  |  | High | Low |
| Impact | Best | Security concerns drive firms and governments to collaborate more closely, openly, and efficiently. | New digital economy trade regimes foster global economic growth that is widely distributed |
|  | Worst | As data manipulation becomes even more difficult to detect, institutions that rely on trust collapse | Advanced technologies, such as AI, quantum, and IoT, layer and converge such that humans find themselves disempowered to decide, or even subservient |

# Policy Logic for “What do we do NOW?

Probability

| Impact | High | Low |
|---|---|---|
| Best | Security concerns drive firms and governments to collaborate more closely, openly, and efficiently.<br>*Aim to maximize* | New digital economy trade regimes foster global economic growth that is widely distributed<br>*Invest smartly* |
| Worst | As data manipulation becomes even more difficult to detect, institutions that rely on trust collapse<br>***Must** Prevent* | Advanced technologies, such as AI, quantum, and IoT, layer and converge such that humans find themselves disempowered to decide, or even subservient<br>*Hedge against* |

# 2. Overarching themes

1. There is disillusionment with the idea of ‘cyber norms’

2. It takes concerted effort to keep hold of the upside

**3. The discussion has nationalized**

- The narrative of a “free and open internet” wasn’t that long ago
- Technology firmly yoked to the goals of national power

# 3. Reframing the Landscape

1. The ‘golden mean’ of light-touch regulation and permission-less innovation will not endure, because it is not an effective route to improved digital security.

2. **Digital geopolitics is not simply another layer on conventional geopolitics. Alliances, trade relationships, and wars may be re-configured around digital as a primary driver.**

3. **Digitally-induced job displacement and inequality is more than a stressor. It is set to be a driver of fundamental breakdown in markets and states, and could be a primary cause of transnational re-alignments.**

4. Platform firms are different. They can’t continue to free-ride on social order, and not just because of market power. It’s also an issue of managing truth and discourse. Competition policy and cybersecurity policy are converging.

5. **The greatest security challenges are not about protecting networks and data from (sovereign and criminal) thieves. It is about protection from manipulation—the maintenance of data integrity and trust.**

# Digital geopolitics

- Digital geopolitics is no longer a layer superimposed on conventional geopolitics
  - Digital is creating new alignments among new actors, and not only states
- Cyber-attacks could cause traditional alliances to reshuffle
- Parastatal and criminal organizations are becoming equal-status players to large firms and governments, who are nearly co-equal participants in some political processes
  - Denmark has already created a formal ambassador to the technology sector
- New technologies (like quantum computing) could drastically reshuffle geopolitical power
- Definitions of what constitutes criminal activity is diverging across geographies, creating opportunities for digital criminals

# Digital geopolitics - So What?

- Are there ways to define/guess at how the geopolitical landscape might change, given our four scenarios and any others?
    - Can we ‘wargame’ our cyber future to try and anticipate how countries will align?

- Given that we are in a constant low-level conflict in cyberspace,
    - Is cyber just an effect tool to disrupt, or does it have real consequence/cost?
    - Is cyber an equalizer?  Will there be a cyber 9/11?

# Digital job displacement and inequality

- Digital-induced job displacement and inequality are set to bring fundamental breakdowns and failures in both labor markets and politics

- Countries and regions are positioned very differently

  - Asians seem to hold a higher level of confidence that societies can endure through these changes

  - Populist movements in the US and Europe share a loss of confidence the benefits of digital technology will help those that will be left behind

- Transnational movements (e.g., distressed and displaced labor, or technology elite force) are nascent in some parts of the world; their (possible) emergence would become an important new part of the security landscape

# Digital job displacement and inequality – So What?

- What might transnational worker uprisings look like, and how can they be kept at a low level of conflict (e.g., protest and advocacy)?
  - Can we model the effects of digital displacement and inequality?
  - Can we make educated guesses about the tipping point to violence or other disruption?
  - Should this parallel current DOD studies on climate change displacement impact?
- Might the U.S. need to lead retraining/reskilling efforts to promote stability, and what might that look like?
  - What sorts of public-private partnerships might succeed?
  - What part of the USG might lead efforts?

# Maintenance of data integrity and trust

- Cybersecurity is morphing from theft of data to protection of data from devious manipulation

- Workshops highlighted a broad assumption that the sophistication of attacks is set to rise

  - Adversarial machine learning, subtle deep fakes, or small changes in training set data that intentionally bias algorithms

- Broad societal resilience programs are talked about more in Asia than elsewhere; in US, consumers and users are still seen as mostly passive

  - In US, lower level of belief that we can educate citizens to be savvier consumers of information

  - Substantial differences in the need to keep certain decision “human-made”

# Maintenance of data integrity and trust - So What?

- Are we at a point where the USG needs to consider countering malicious high-tech with active high-tech measures to undermine the systems?
  - E.g., Should we consider attacking China’s data for facial recognition to make the system unreliable rather than make ethical arguments?
- Could we speak towards standards for datasets, systems for managing data, formats you want an NIH or Commerce grantee to submit data in?
  - Rise of a new field: QA for ML, like a set of certifications for AI systems as a whole (from input to output)
- Can we provide insight into possible insider threat for data manipulation?

# Questions for the group

- What stands out as the most important thing that the USG should aim to accomplish in the next year?
- What stands out as the most important thing that the DOD should aim to accomplish in the next year?
- What can we rely on international organizations to do for us?
- What can we rely on private sector to do for us?

# THANK YOU

CNA

CLTC

Center for Long-Term Cybersecurity