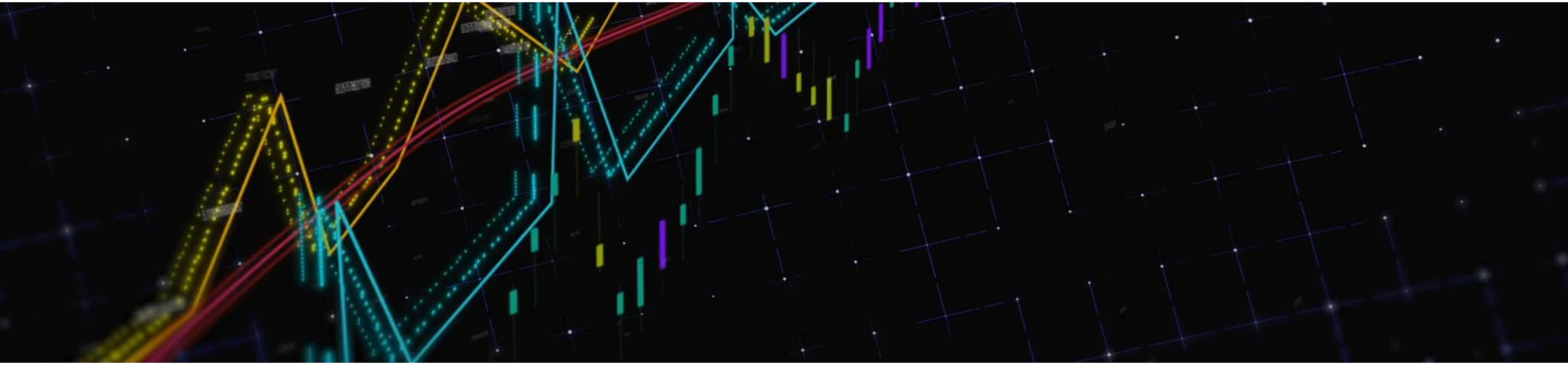
Given Our GenAI Era:

Why, What, and How Free Societies Must Develop Effective Deterrence of Actors Intending Bad Ends

more at: stimson.org/project/red-cell/ &
dbray@stimson.org

Opening Thoughts:

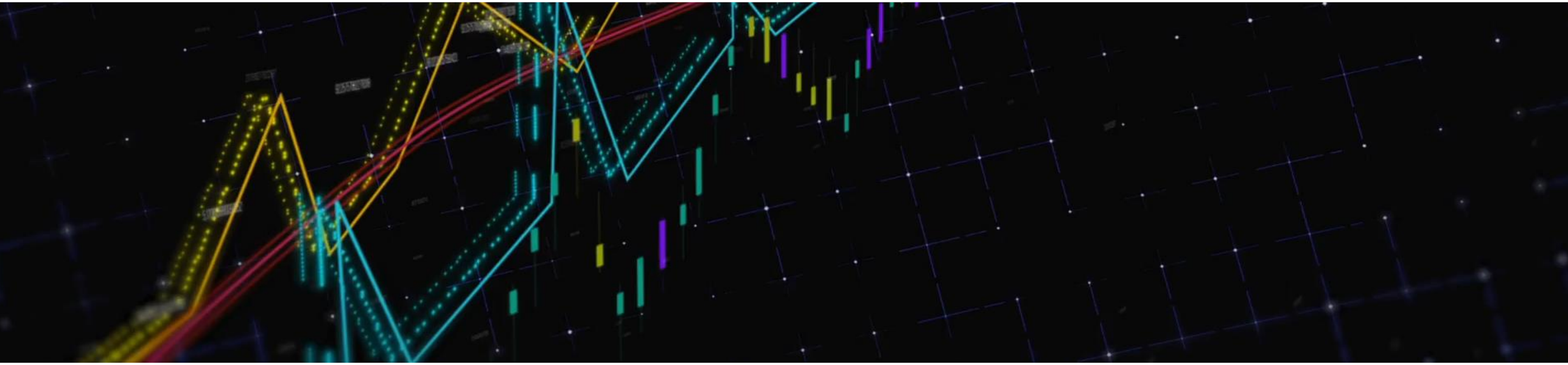
Living Amid Seismic Changes



Last 50 years: we've democratized tech previously just available to intelligence components of major nations in the 1970s

Opening Thoughts:

Living Amid Seismic Changes



However: <u>we have not upgraded how to do the work of defense, security, and civil society</u> given super-empowered populations

Given Our GenAI Era:

Part 1 – “Why”

more at: stimson.org/project/red-cell/ &
dbray@stimson.org

Trend 1:
AI Everywhere

Current GenAI, using Deep Learning, is massively data & CPU intensive – may be replaced by local & more agile AI methods

Trend 1:
AI Everywhere

napster

= ? GENAI vs.

ELSEVIER

Journal of Mathematical Psychology

Volume 107, April 2022, 102632

Tutorial

A step-by-step tutorial on active inference and its application to empirical data

Ryan Smith [a 1], Karl J. Friston [b], Christopher J. Whyte [c 1]

Active Inference = alternative approach that may prove better for more predictive, localized AI if present is *not* like past data

Trend 1:

Will GenAI ‘s impacts ≈ Gutenberg printing press on the 16th century Catholic Church?

Trend 2:

Data Collides with Globalization

Rank	Name	Market Cap	Price	Today	Price (30 days)	Country
1	Microsoft MSFT	$3.085 T	$415.28	2.66%		USA
2	Apple AAPL	$2.675 T	$173.23	0.28%		USA
3	NVIDIA NVDA	$2.297 T	$919.13	7.16%		USA
4	Saudi Aramco 2222.SR	$2.069 T	$8.55	0.47%		S. Arabia
5	Amazon AMZN	$1.821 T	$175.39	1.99%		USA
6	Alphabet (Google) GOOG	$1.728 T	$139.62	0.49%		USA
7	Meta Platforms (Facebook) META	$1.274 T	$499.75	3.34%		USA
8	Berkshire Hathaway BRK-B	$876.32 B	$404.98	0.05%		USA
9	TSMC TSM	$749.00 B	$144.40	3.87%		Taiwan
10	Eli Lilly LLY	$717.32 B	$754.95	2.80%		USA

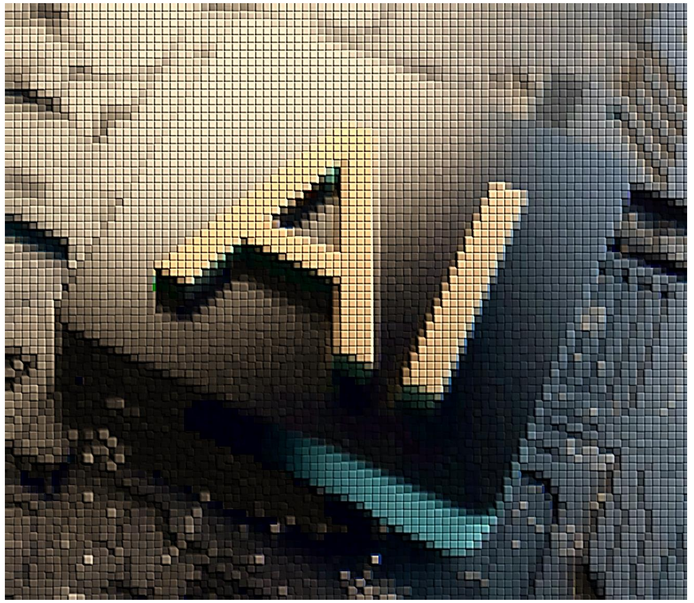
#	Country	GDP (nominal, 2022)	GDP (abbrev.)	GDP growth	Population (2022)	GDP per capita	Share of World GDP
1	United States	$25,462,700,000,000	$25.463 trillion	2.06%	338,289,857	$75,269	25.32%
2	China	$17,963,200,000,000	$17.963 trillion	2.99%	1,425,887,337	$12,598	17.86%
3	Japan	$4,231,140,000,000	$4.231 trillion	1.03%	123,951,692	$34,135	4.21%
4	Germany	$4,072,190,000,000	$4.072 trillion	1.79%	83,369,843	$48,845	4.05%
5	India	$3,385,090,000,000	$3.385 trillion	7.00%	1,417,173,173	$2,389	3.37%
6	United Kingdom	$3,070,670,000,000	$3.071 trillion	4.10%	67,508,936	$45,485	3.05%
7	France	$2,782,910,000,000	$2.783 trillion	2.56%	64,626,628	$43,061	2.77%
8	Russia	$2,240,420,000,000	$2.240 trillion	-2.07%	144,713,314	$15,482	2.23%
9	Canada	$2,139,840,000,000	$2.140 trillion	3.40%	38,454,327	$55,646	2.13%
10	Italy	$2,010,430,000,000	$2.010 trillion	3.67%	59,037,474	$34,053	2.00%

Combined market cap of the major data-intensive companies
≈ the combined GDP of all nations minus the top 4

Trend 2:

Data Collides with Globalization

Data = form of voice for people, if little or no choices in its use the people lose free speech



Data is *not* the new oil = hoarding breeds distrust, raising Qs for upgrading IC?

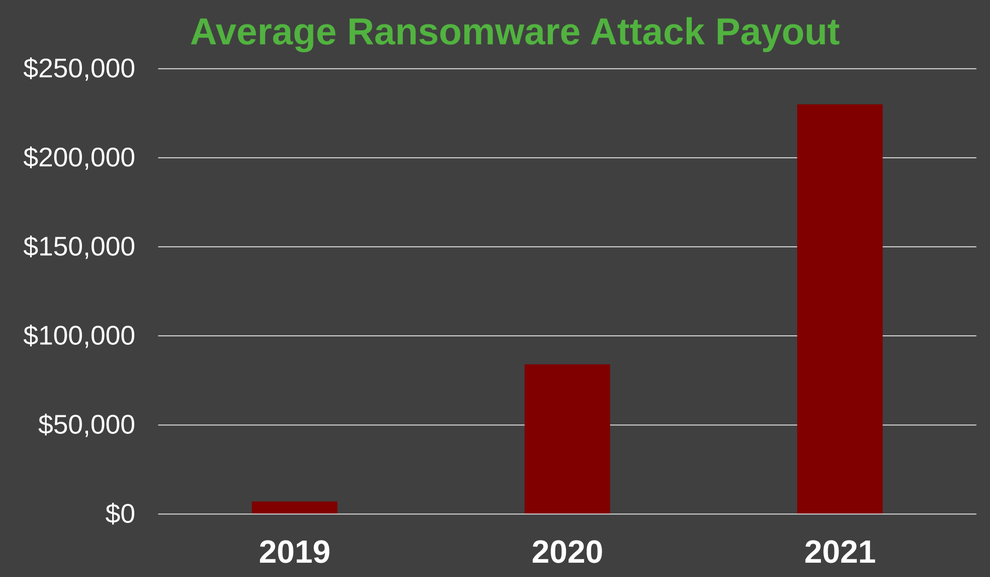
Most orgs still need to get digital fundamentals first, meanwhile may find too much <u>data hoarding challenges free societies</u>

Trend 2:

How can U.S. national security partner better with space and tech + adhere to Constitution?

Trend 3:

Cybersecurity: Ransoms + Scams



Ransomware damages in 2019: $11B, 2020: $20B, 2021: $43B+

“Our goal is to make money” – Colonial Pipeline attackers

Trend 3:

Cybersecurity: Ransoms + Scams

CEO Arrested for Selling $1 Billion in Fake Cisco Hardware on Amazon, eBay

Onur Aksoy allegedly imported thousands of fake Cisco networking devices from China.

Disinformation Researchers Raise Alarms About A.I. Chatbots

Researchers used ChatGPT to produce clean, convincing text that repeated conspiracy theories and misleading narratives.

A company lost $25 million after an employee was tricked by deepfakes of his coworkers on a video call: police

- The person had attended a video call with deepfakes of the firm's UK-based CFO and other colleagues.
- Hong Kong police said scammers created the deepfakes based on publicly available video.

Wi-Fi jamming to knock out cameras suspected in nine Minnesota burglaries -- smart security systems vulnerable as tech becomes cheaper and easier to acquire

EDUCATION

Hackers are targeting a surprising group of people: young public school students

MARCH 12, 2024 · 5:01 AM ET

Significant concern in use of Generative AI to generate <u>fake AI images, audio, & videos</u> to generate fraud + brand disinformation

Trend 3:

How to find solutions to detect AI/bots that still adhere to the values of the Constitution?

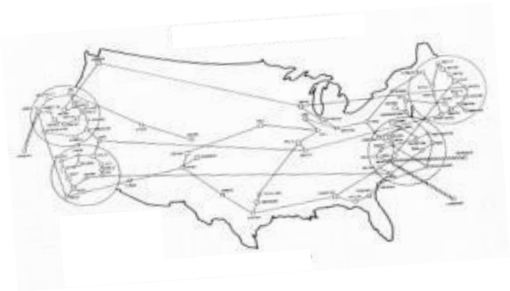
Why We Need New Forms of Deterence:

What Massive Changes Mean

1969

Why We Need New Forms of Deterence:

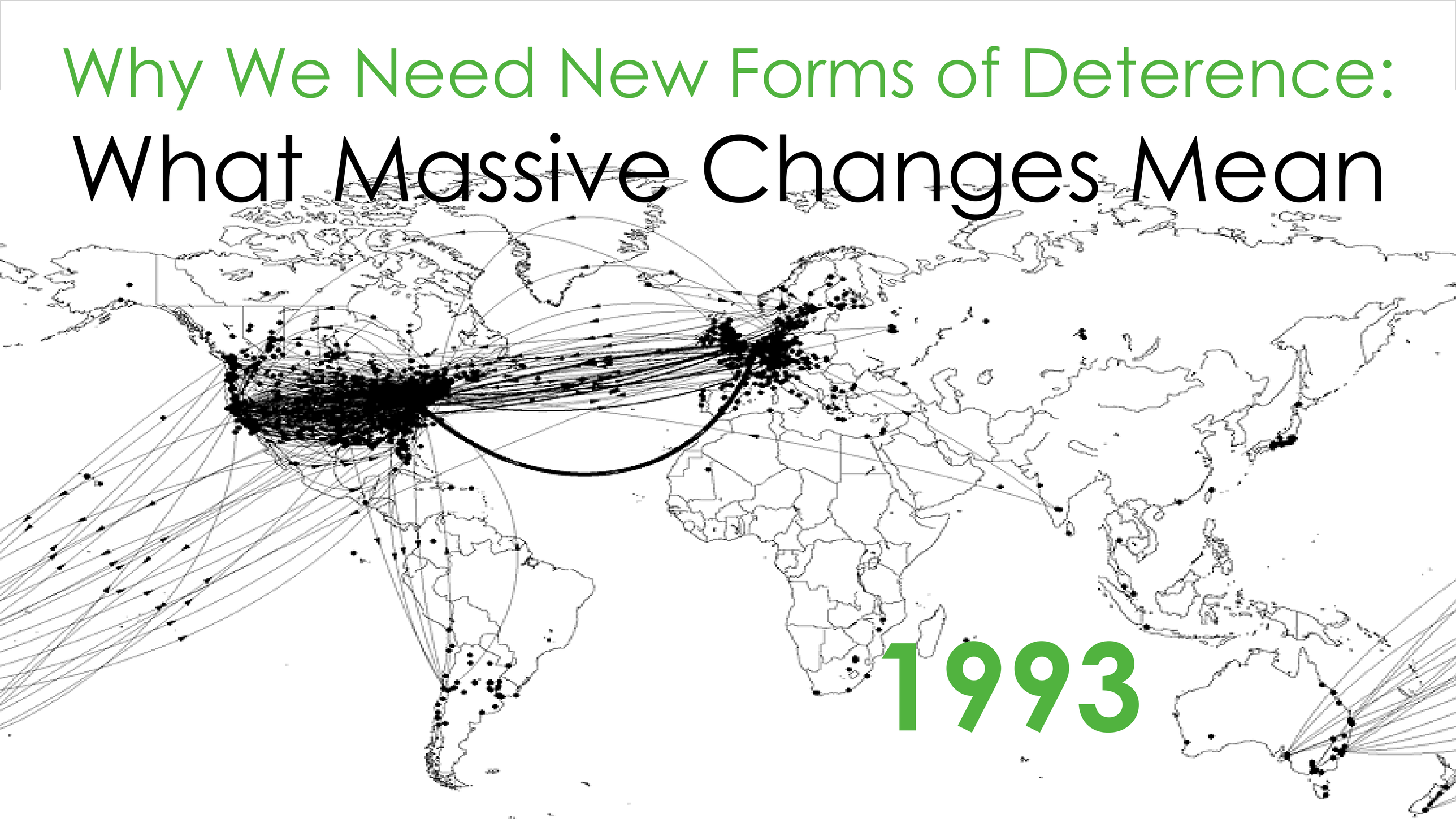
What Massive Changes Mean



1982

Why We Need New Forms of Deterence:

What Massive Changes Mean



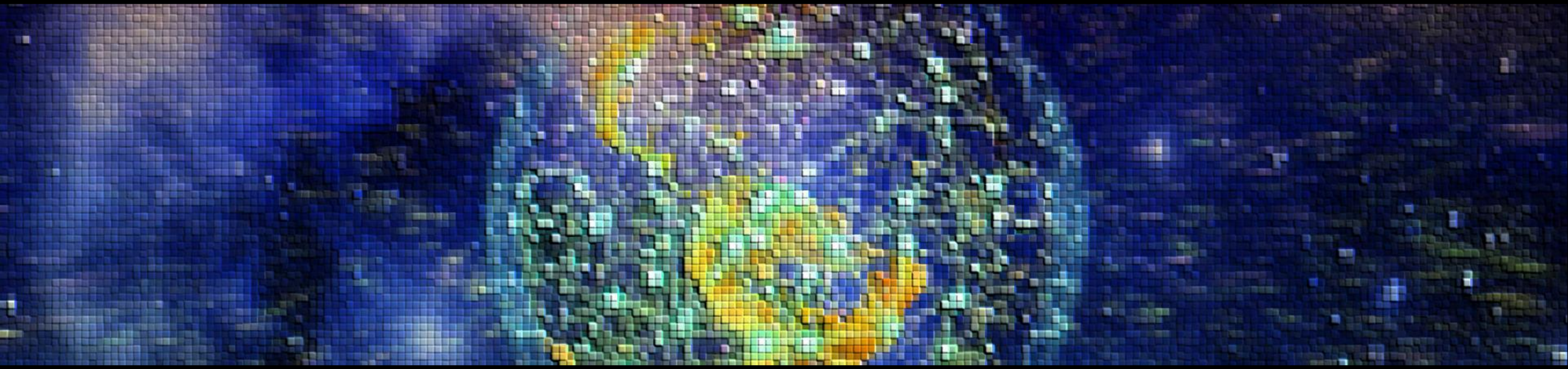
Why We Need New Forms of Deterence:

What Massive Changes Mean

Why We Need New Forms of Deterence:
What Massive Changes Mean

2013

Why We Need New Forms of Deterence:
What Massive Changes Mean



2013: 7.1 billion humans on Earth, ~7.1 billion network devices

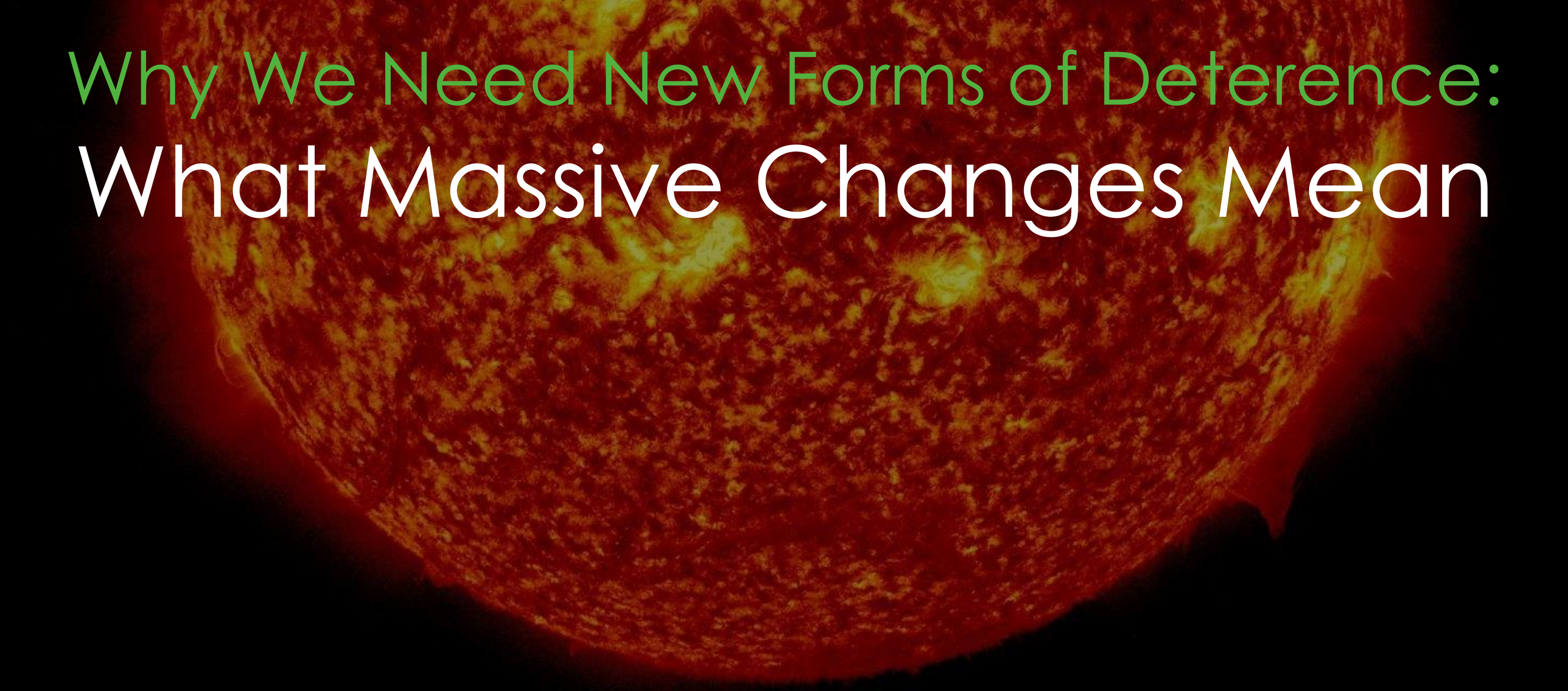
2024: 8.1 billion humans on Earth, ~45 billion network devices

Why We Need New Digital Deterences:
What Massive Changes Mean

If we put the 2^{32} numbers (~4.3 billion)
addressable by Internet Protocol version 4 into a Beach Ball

Why We Need New Forms of Deterence:

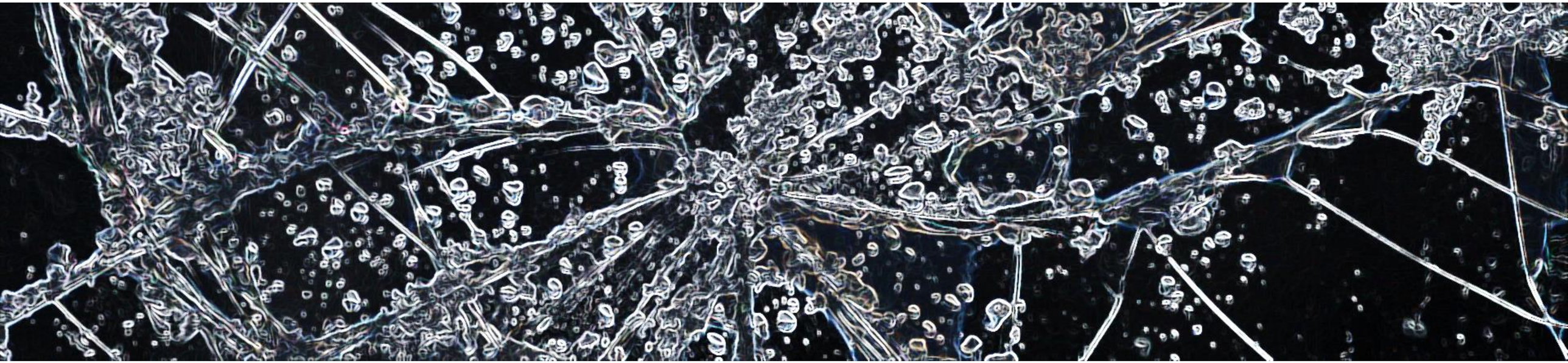
What Massive Changes Mean



For IPv6, the 2^{128} numbers (~340 followed by 36 zeros) associated with this address space = the Volume of our Sun

Why We Need New Forms of Deterence:

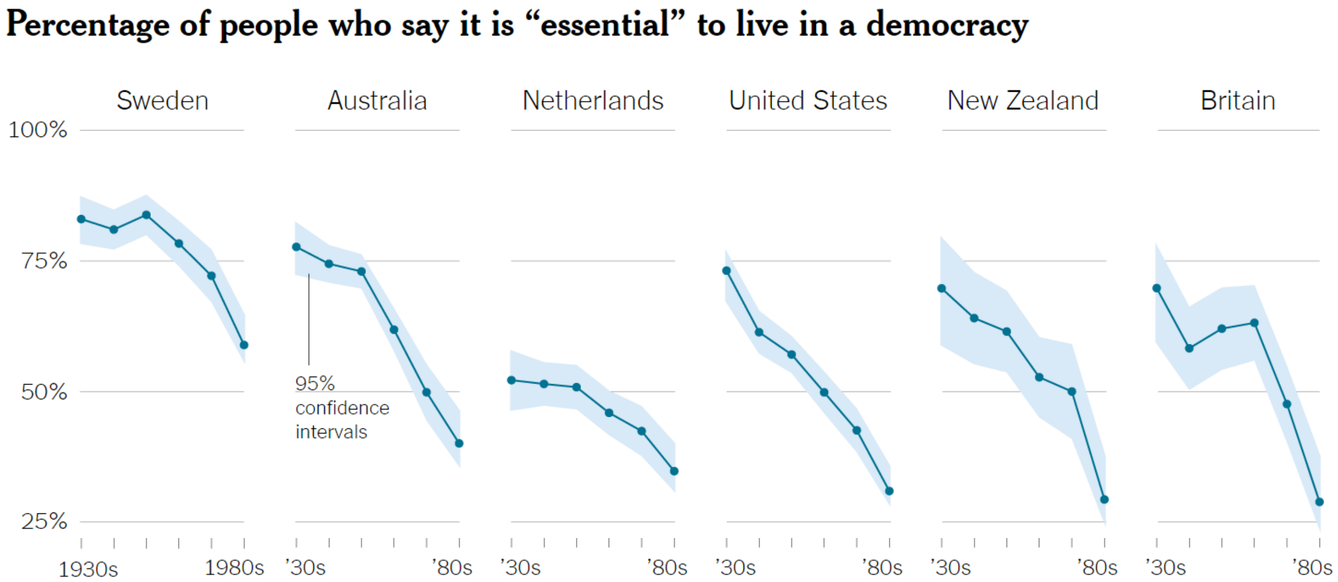
Stresses and Social Changes



Bad actors will use tech to attack U.S. national strengths in ways we cannot similarly use tech to counter → need new strategies

Why We Need New Forms of Deterence:

Stresses and Social Changes



2018: Young people in the US who prefer capitalism <45%

<19% think military coups are bad if a government is incompetent

Why We Need New Forms of Deterence:

Stresses and Social Changes

With inflation, COVID-19's economic recovery has been K-shaped for the U.S., isolating some and increasing loneliness

Why We Need New Forms of Deterence:

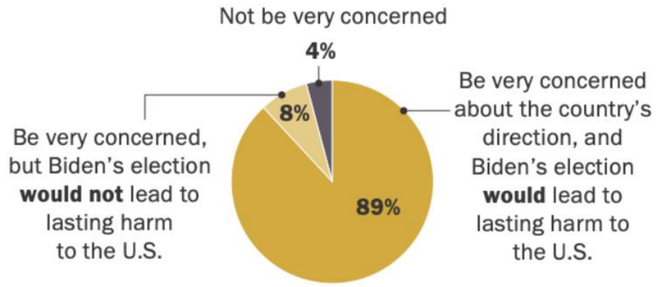
Stresses and Social Changes

China's population growth is slowing and is close to a standstill — throwing into jeopardy its global economic and geo-political ambitions, experts warn.

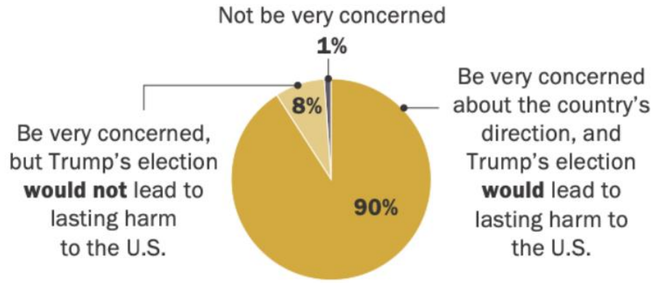
The world's second-largest economy reported an increase of 72 million people in the last 10 years in the once-a-decade census, to a total of 1.1411 billion.

But the National Bureau of Statistics said annual growth over the last decade averaged 0.53 percent, down 0.04 percent on the previous decade. The slow-down bolsters evidence of what economists refer to as a demographic time bomb, where many Chinese people could grow old before they grow rich.

*% of **Trump supporters** who say they would ____ about the direction of the country if Joe Biden was elected president*



*% of **Biden supporters** who say they would ____ about the direction of the country if Donald Trump was reelected president*



>85% of U.S. party voters believe other party hurts country

multiple regional conflicts in 2024 + PRC's economy slowing

Given Our GenAI Era:

Part 2 – "What" & "How"

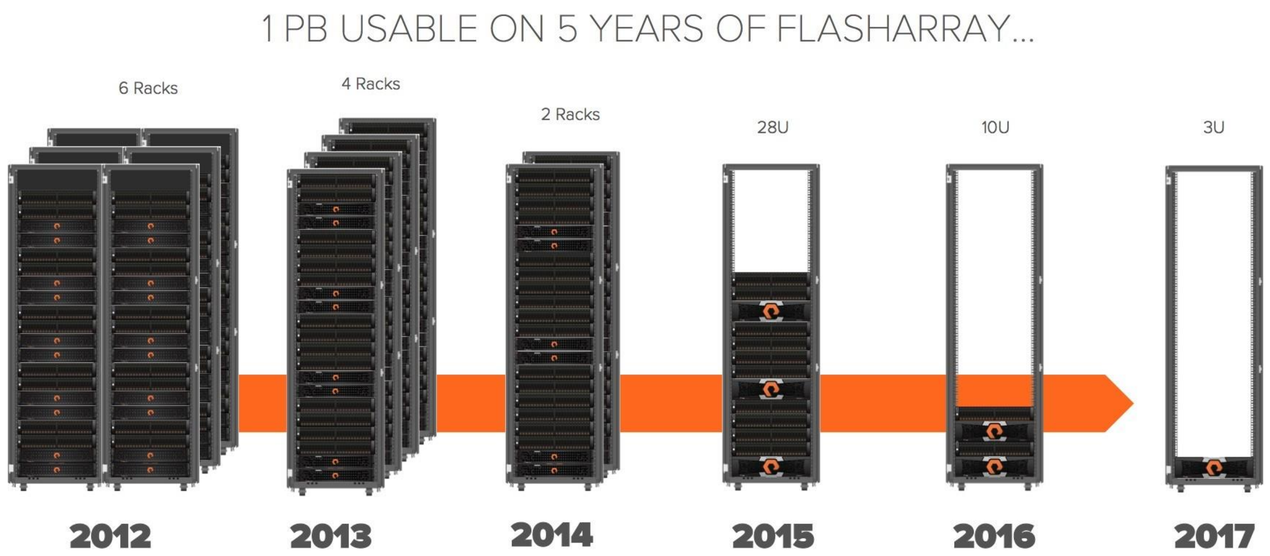
Do We Need A "Civilian ARPA" for AI?

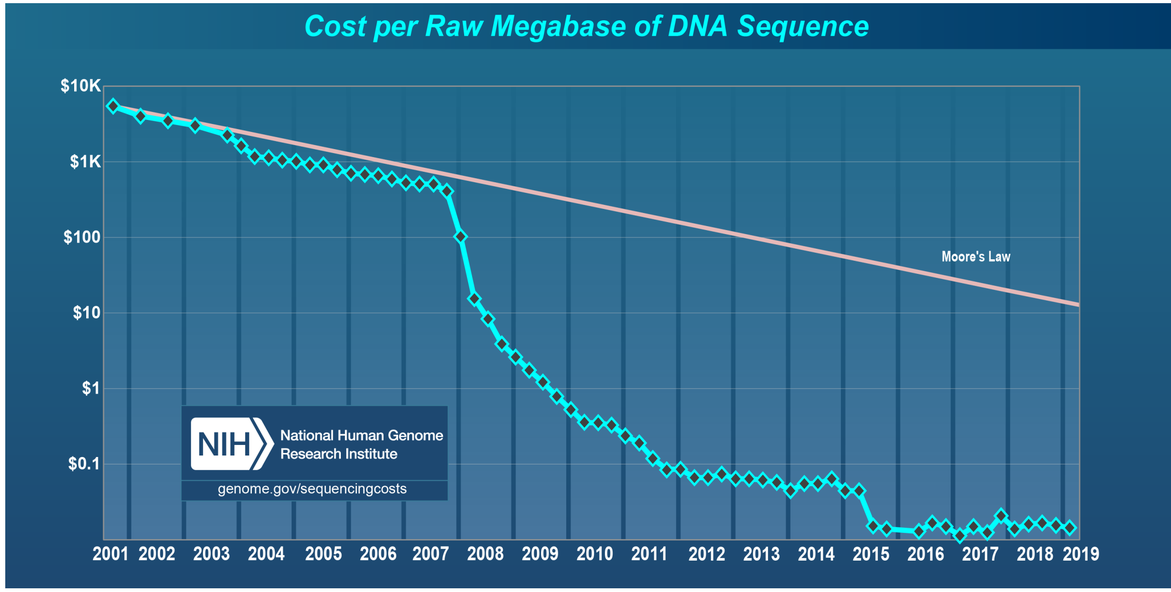
The case for leveraging artificial intelligence to improve public service

By: Dr. David Bray | October 12, 2016

Why We Need New Forms of Deterence:

Stresses and Social Changes

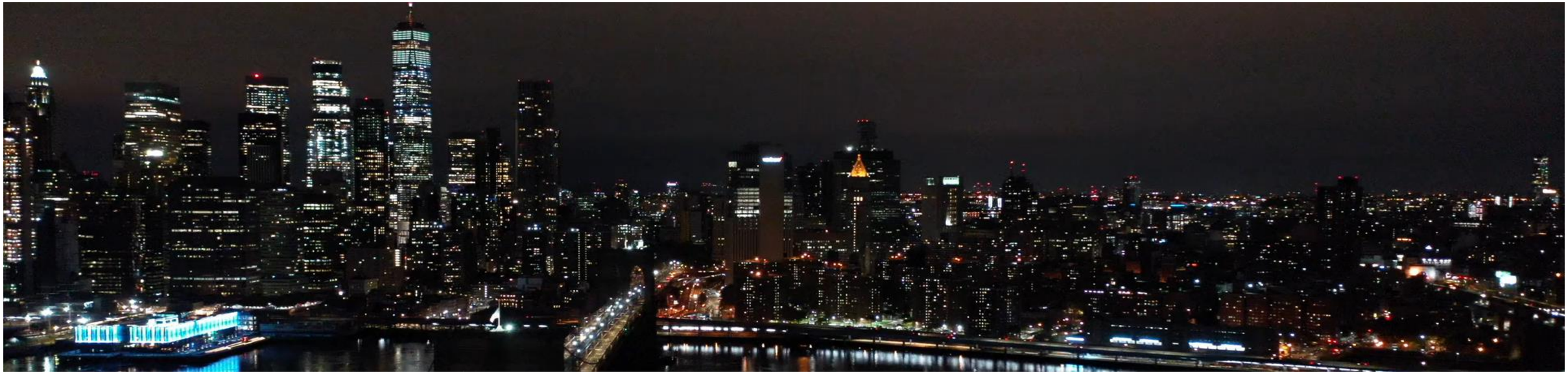




Assessing authentic vs. inauthentic increasingly hard +
how to avoid drowning in data vs. actual actionable insights?

Why We Need New Forms of Deterence:

Stresses and Social Changes



Will need to democratize tradecraft of "information discernment" + whole-of-society "digital dignity" consistent with Constitution

Different Deterrence Regimes:
Addressing GenAI Abuses

Note: **deterrence focuses on human actors behind a GenAI**
GenAI systems not assumed to "think" like humans
stopping GenAI systems akin to other cyber systems

Potential measures: GenAI blocking, intentional algorithmic confusion, data poisoning, digital corruption, and focused EMP

Different Deterrence Regimes:

Addressing GenAI Abuses

Nations will need to track potential foreign & non-state AI threats and enact deterrence

Biggest risk of GenAI is *not* existential, rather that the commons and connections that hold free societies together is abused and corrupted

GenAI abuses include: flooding the zone, mass impersonations, and corrupting quality data needed by free societies to operate

Different Deterrence Regimes:
Addressing GenAI Abuses

Within a Society, Gen AI abuses counter to:

… Civil Norms

… Laws

… National Defense

	Professional Societies?	Diplomacy
Domestic Regulatory + Diplomatic Regulatory		
Public Safety + Security?	Intelligence + Defense?	Diplomacy + Defense

By:

Domestic Actors

Nonstate International

Foreign Nation-state

Different Deterrence Regimes:
Addressing GenAI Abuses

Gaps: **must demonstrate credible "costs" to deter human actors**
must be able to correctly attribute and reach human actors
must <u>not</u> lose public trust and support while defending

By:

- **Domestic Actors**
- **Nonstate International**
- **Foreign Nation-state**

Different Deterrence Regimes:

Abuses Counter to Nat'l Defense

Ideas: **proportional digital, financial, and kinetic costs doctrine**
multi-nation triangulating & attribution alliance
random citizen juries included in oversight mechanisms

Public Safety + Security?	Intelligence + Defense?	Diplomacy + Defense

Domestic Actors

Nonstate International

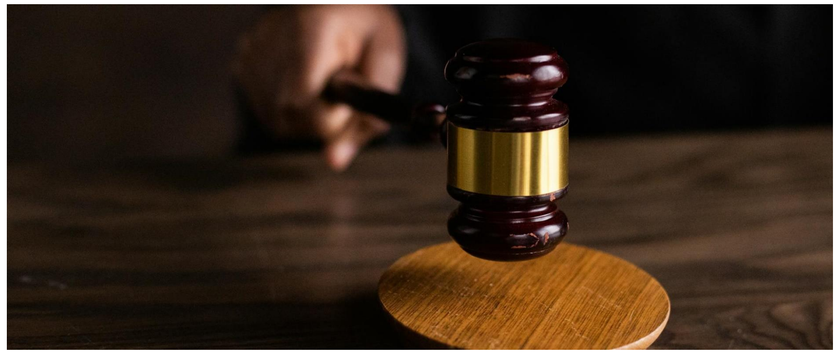
Foreign Nation-state

Different Deterrence Regimes:

Abuses Counter to Laws

Ideas: **clear liability regime and bilateral/multilateral agreements**
clear convention of rights of people to be free of AI abuse?
must <u>not</u> become surveillance state in response to risks

Domestic Regulatory + Diplomatic Regulatory



Domestic Actors

Nonstate International

Foreign Nation-state

Different Deterrence Regimes:

Abuses Counter to Civil Norms

Ideas: **must avoid heavy approach that forces AI underground**
akin to “ham radio licenses”, licenses to unleash a GenAI?
certified ethical data scientist / ethical GenAI developer?

Diplomacy

Professional Societies?

Domestic Actors

Nonstate International

Foreign Nation-state

Different Deterrence Regimes:

Whole-of-Society Solutions

Ideas: **improve GenAI+human behaviors & intents identification**
ISPs+Platform protocols limiting abusive GenAI movement
random citizen juries included in oversight mechanisms

By:

- **Domestic Actors**
- **Nonstate International**
- **Foreign Nation-state**

Different Deterrence Regimes:

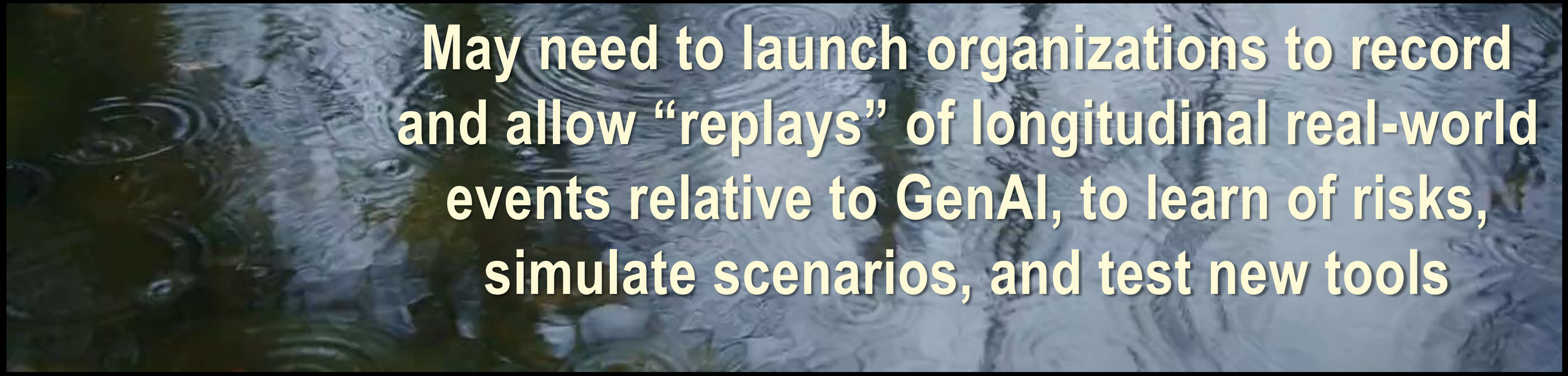
Whole-of-Society Solutions

Ideas: **must have national privacy protections updated for GenAI**
need data stakeholderism, perhaps data coops, for public
potentially crowdsource spotting/tips re: GenAI abuse

By:

- **Domestic Actors**
- **Nonstate International**
- **Foreign Nation-state**

Different Deterrence Regimes:
Whole-of-Society Solutions



Will need operational NGOs to tackle issues plus more ways for individuals to have “voice” – cannot be done by gov’t alone

Closing Thoughts:

Still Not Winning in “Cyber”

Lest we focus too much on GenAI risks, we’re still not winning on protecting people from cyber harms, including scams & extortion

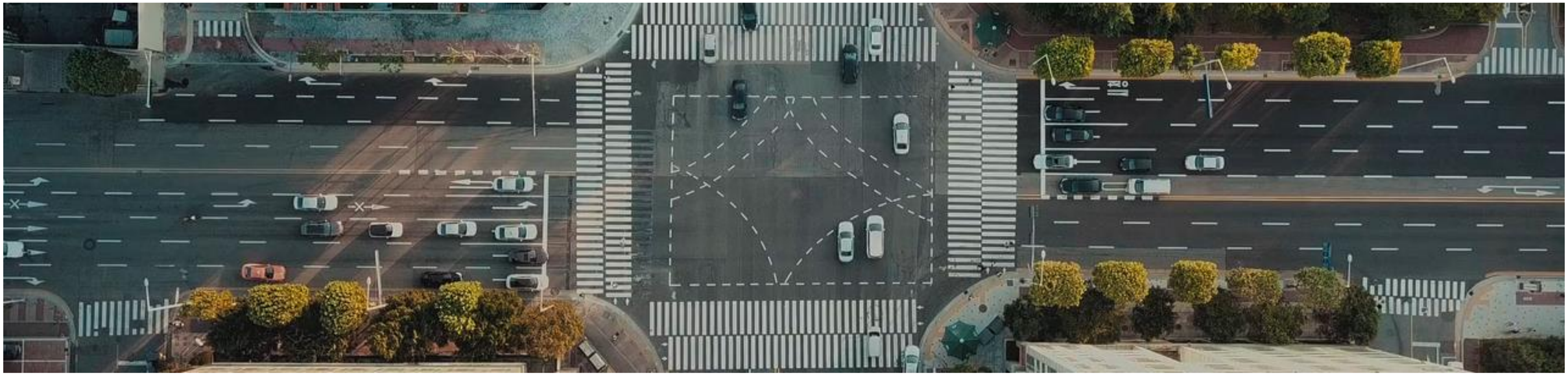
Closing Thoughts:

Need to Empower People

What do tools for “information discernment”, identifying, reporting GenAIs misuse & abuses look like for the public?

Closing Thoughts:

More Operational Spaces



Need places public can trust to operationalize non-politically, perhaps Labs & Non-Profits with bipartisan oversight?


Be Bold, Be Brave, Be Benevolent
Additional Questions?
more at: stimson.org/project/red-cell/ &
dbray@stimson.org