RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PNG-R01**

Leveraging Crowd-Forecasting to Improve Our Understanding of Cybersecurity

Mary K. Brooks

Fellow
R Street Institute
@Mary_K_Broooks

Paul Rosenzweig

Principal
Red Branch Consulting
@RosenzweigP

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

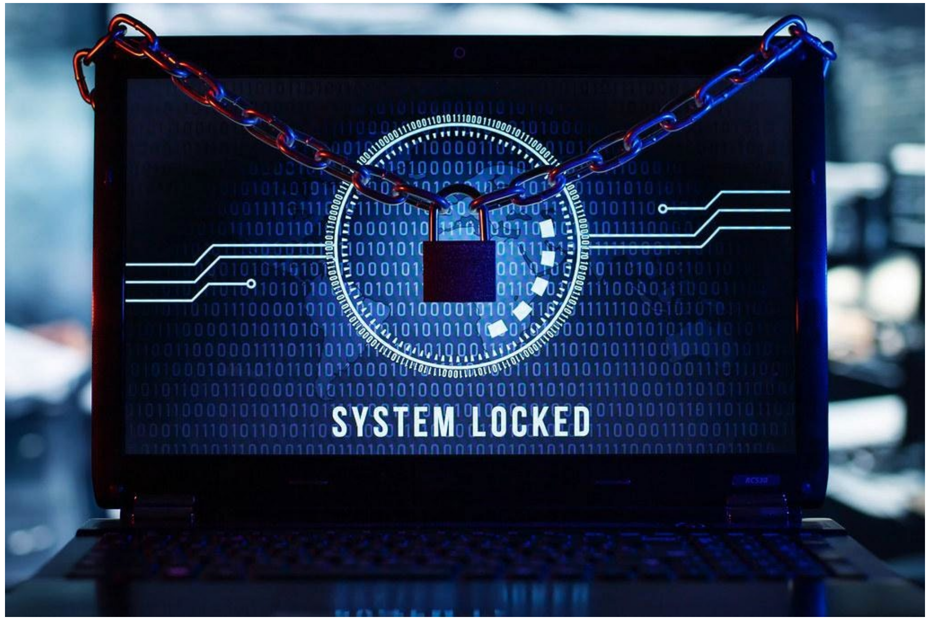
R Street
Free markets. Real solutions.

Our Agenda

- What is crowd-forecasting?
- Beta-testing the concept through Metaculus, LLC
- Preliminary results and lessons learned

First – An Example

- Will a U.S.-incorporated insurance company decide to stop binding coverage for ransomware payments before December 31, 2022?



- Answer that Yes or No
- Now let’s aggregate the wisdom of the crowd here at RSA

What It Might Mean

- **Strong Yes** -- Losses will exceed what the rate-paying market is willing to bear and individual insureds are likely to be on their own as insurers drop back.
- **Weak Yes** -- Choosing an insurer has become crucial in any company's risk mitigation plan as insurers clearly do not have an across-the-board handle on outcomes.
- **Ambivalence** -- To watch like a hawk.
- **Weak No** -- A discontinued insurance program is a management failure at that insurer, not an industry failure.
- **Strong No** -- Ransomware is pervasive enough that no insurer can dare stop covering it unless they plan to fold up their cyber insurance portfolio entirely.

RSAConference2022

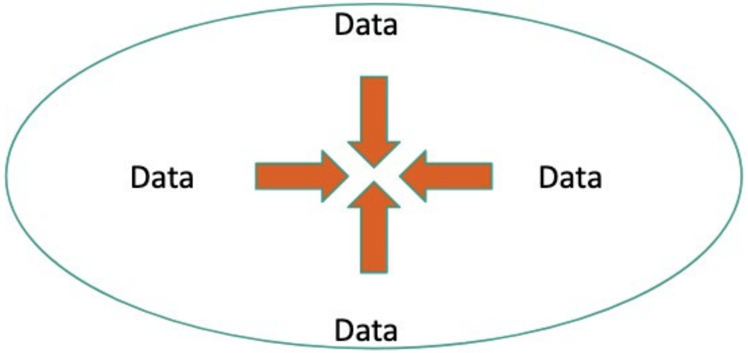
What Is Crowd-Forecasting?

Crowd-Forecasting

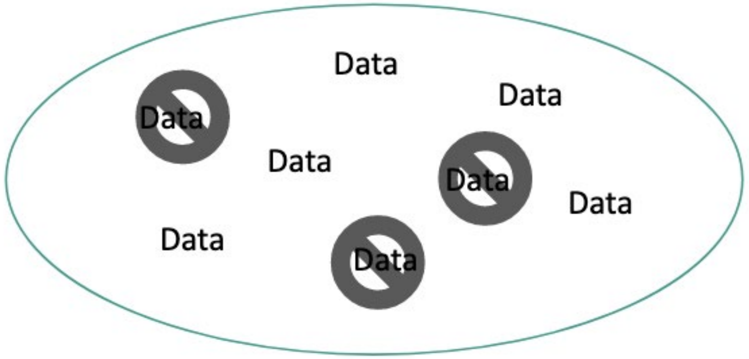
- **The Main Idea:** Sufficiently large groups of individuals who are incentivized to share predictions will more often accurately forecast the likelihood of future outcomes.

Three possible advantages for cybersecurity:

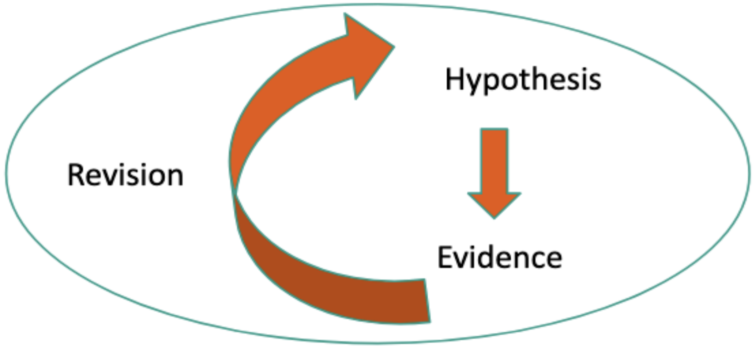
1. Information aggregation



2. Reduce Noise/Bias



3. Validation of Hypothesis



When Does Crowd-Forecasting Work?

- Robust use already:
  - Internal crowd-forecasting platforms at companies
  - Classified prediction markets within the IC (say no more …)
  - Financial industry
  - Fantasy Football leagues
  - Kalshi - A real prediction market!

- Additional challenges:
  - Settlement or Resolvability (*aka the fine print – like OPM Hack*)
  - Technical/Niche Questions (*aka generating enough predictions*)
  - Platform Manipulation / Moral Hazard (*aka playing to the test*)
  - Privileged Information (*aka confidential information*)

RSA Conference2022

The White Hat Cyber Crowd-Forecasting Challenge

Platform Design

Hosted by Metaculus, LLC

- Opened up a Cyber Crowd-Forecasting challenge (https://www.metaculus.com/tournament/white-hat/)
- Open competition + invited participants
- Questions released in 3 waves
- Preliminary resolution of some questions last month (so we could share with you)!
- Tournament ends Dec 31, with resolution by June 2023

Sample Questions

- **Geopolitics / Government**
  - What we want to know: Will Chinese aggression towards Taiwan sharply escalate?

    → Will China launch a successful (major) cyberattack on Taiwanese critical infrastructure before December 31, 2022?

- **Industry / Technology**
  - What we want to know: Will the chip shortage end anytime soon?

    → Will average semiconductor chip lead times (amount of time between order and delivery) drop to below 15 weeks at any point before July 1, 2022?

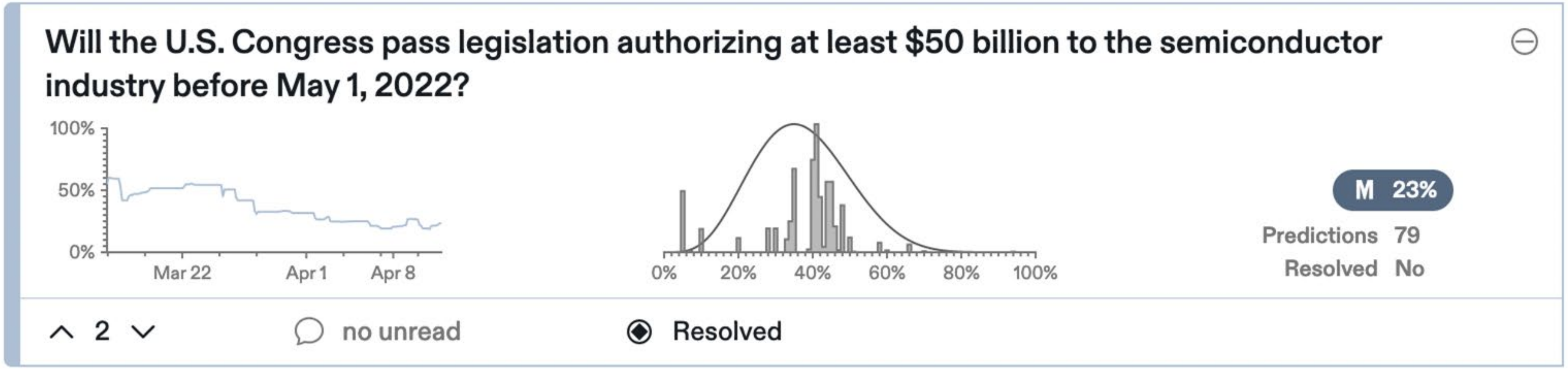
- **Technical / Incident**
  - What we want to know: Is it a good idea to increasingly rely on commercial online identity services? (The IRS seemed to think so!)

    → Will it be publicly reported that a popular online identity verification service was breached in 2022?

RSA Conference 2022

Preliminary Results and Analysis

Preliminary Results -
What are we already seeing?

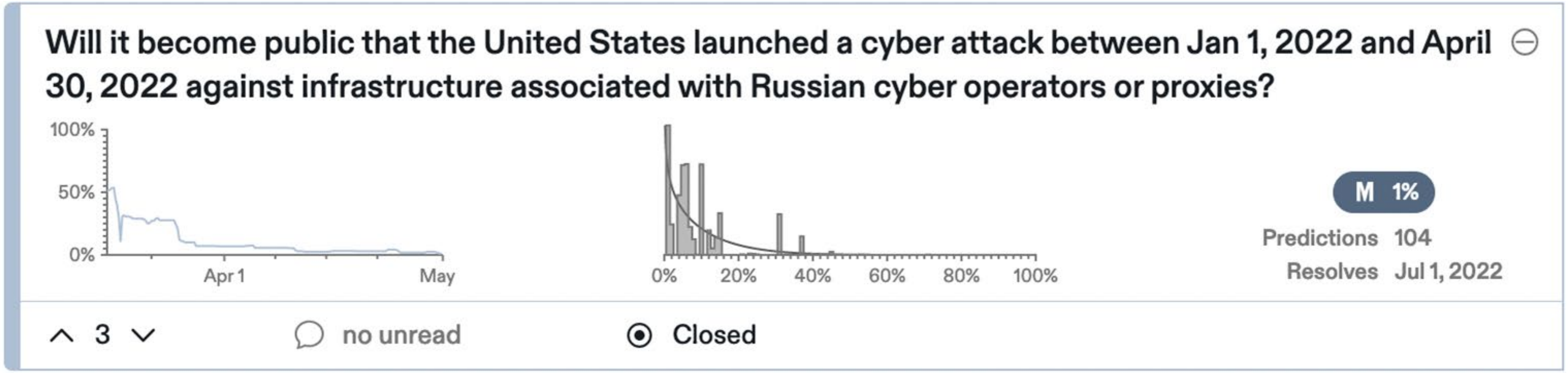


Will the U.S. Congress pass legislation authorizing at least $50 billion to the semiconductor industry before May 1, 2022?

M 23%

Predictions	79
Resolved	No

^ 2 ∨ no unread ◉ Resolved



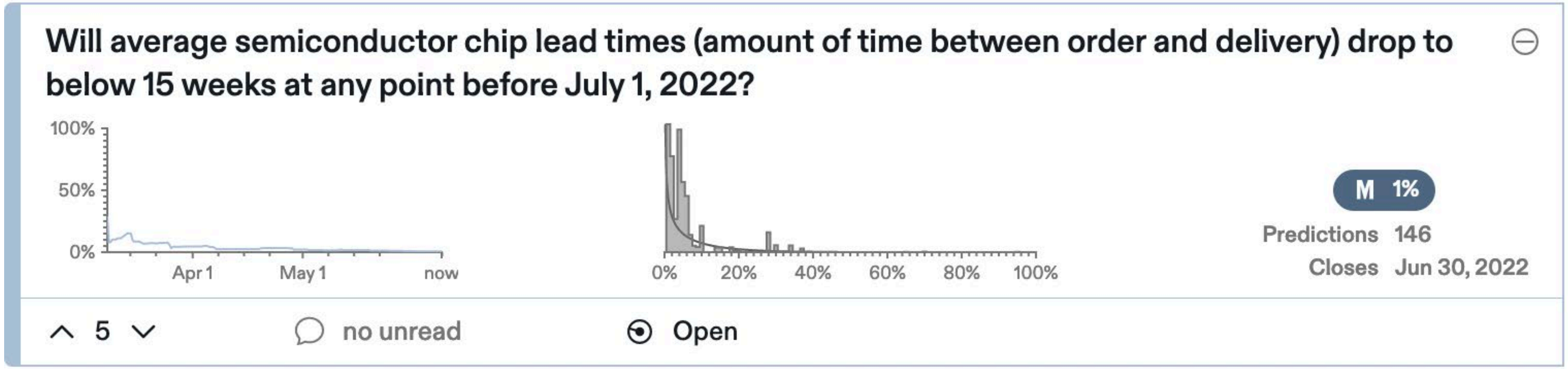
Will it become public that the United States launched a cyber attack between Jan 1, 2022 and April 30, 2022 against infrastructure associated with Russian cyber operators or proxies?

M 1%

Predictions	104
Resolves	Jul 1, 2022

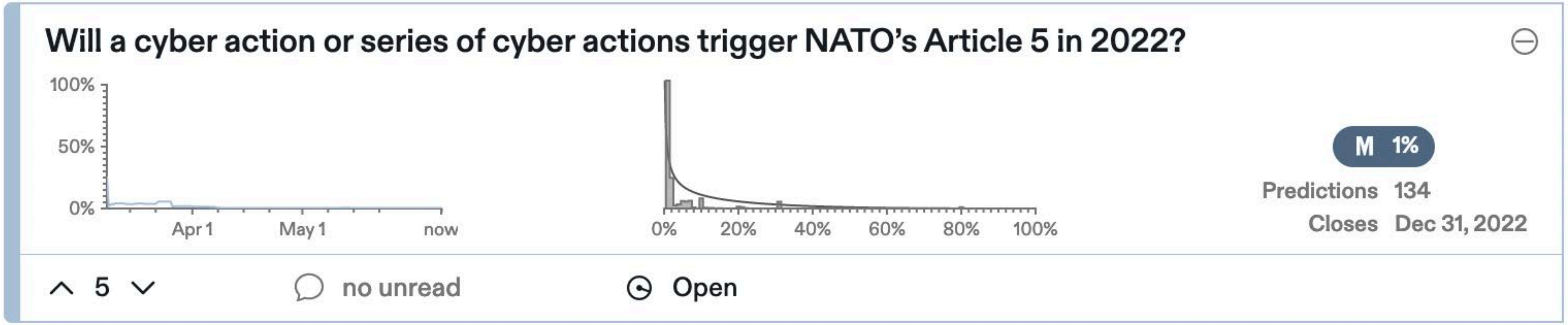
^ 3 ∨ no unread ◉ Closed

Preliminary Results - What are we already seeing? cont.



Will average semiconductor chip lead times (amount of time between order and delivery) drop to below 15 weeks at any point before July 1, 2022?

Predictions 146
Closes Jun 30, 2022

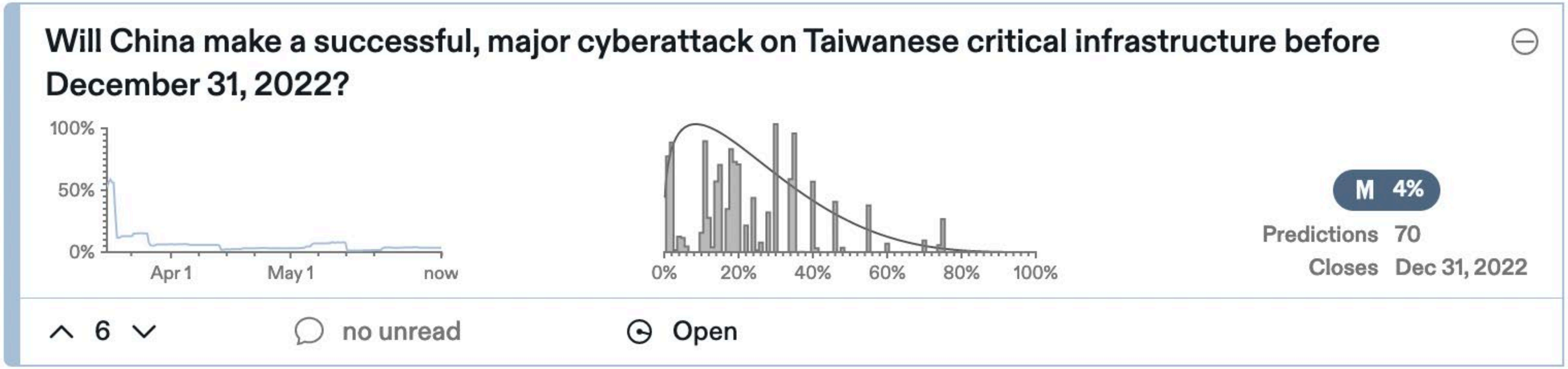


Will a cyber action or series of cyber actions trigger NATO's Article 5 in 2022?

Predictions 134
Closes Dec 31, 2022

R Street
Free markets. Real solutions.

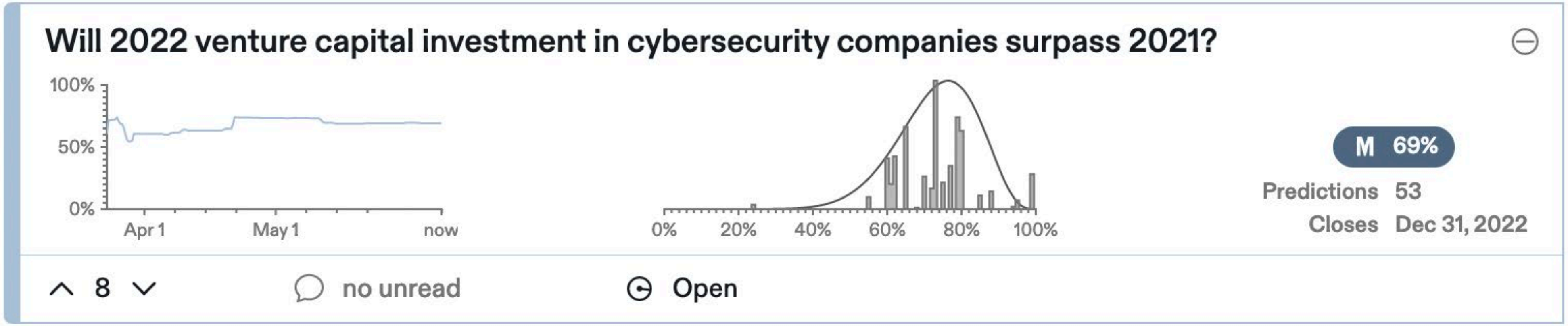
Preliminary Results - What are we already seeing? cont.



Will China make a successful, major cyberattack on Taiwanese critical infrastructure before December 31, 2022?

Predictions 70

Closes Dec 31, 2022



Will 2022 venture capital investment in cybersecurity companies surpass 2021?

Predictions 53

Closes Dec 31, 2022

Street

Free markets. Real solutions.

Preliminary Analysis - What are we already seeing?

- By subject
  - Clear geopolitical interest
  - A complexity limit for public platforms?
- By participants
  - Unofficially - SMEs doing well?
- A bonus for longer timelines?
- Some mistakes! (Of course)
  - Timing glitch
  - The unexpected

Toward the Future

- Finish the real-world beta test
- Report out results
- Operationalize if warranted
- Join us: https://www.metaculus.com/tournament/white-hat/

Our Thanks To…

- Platform Host Metaculus LLC –
  - especially CEO Gaia Dempsey, Tom Liptay, and Alyssa Stevens

- Dan Geer

All those who took our calls, brainstormed questions or challenges, or reviewed our work, including:*

Tatyana Bolton, Adam Siegel, Samantha Braun, Allan Friedman, Regina Joseph, Mark Roulston, Adam Svendsen, Dan Schwarz, Vinh Nguyen, Matt Devost, Jim Miller, Bob Butler, Muayyad Al-Chalabi, Paul Markakis, Dr. Christopher Ford, Dr. Craig Weiner, Paul Kurtz, Martin Brown, Bob Gourley, Bob Flores, Richard Greenberg, Michael Tanji, Chris Kubecka, Liz Wharton, Bryson Bort, and Spencer Oriot.

*Standard disclaimer: Inclusion in this list does not indicate endorsement. All errors remain our own.

References

- Brooks & Rosenzweig, *Let's Bet on the Next Big Policy Crisis – No, Really*, https://www.lawfareblog.com/lets-bet-next-big-policy-crisis-no-really

- Brooks & Rosenzweig, *How Crowd-Forecasting Might Decrease the Cybersecurity Knowledge Deficit*, https://www.lawfareblog.com/how-crowd-forecasting-might-decrease-cybersecurity-knowledge-deficit

- Brooks & Rosenzweig, *Betting on Cyber: Offering an Analytical Framework for a Cybersecurity Crowd-Forecasting Platform*, https://www.rstreet.org/wp-content/uploads/2021/12/FINAL_RSTREET248.pdf

- Brooks & Rosenzweig, *Come Compete in the White Hat Cyber Forecasting Challenge*, https://www.lawfareblog.com/come-compete-white-hat-cyber-forecasting-challenge

- White Hat Cyber Challenge, https://www.metaculus.com/tournament/white-hat/