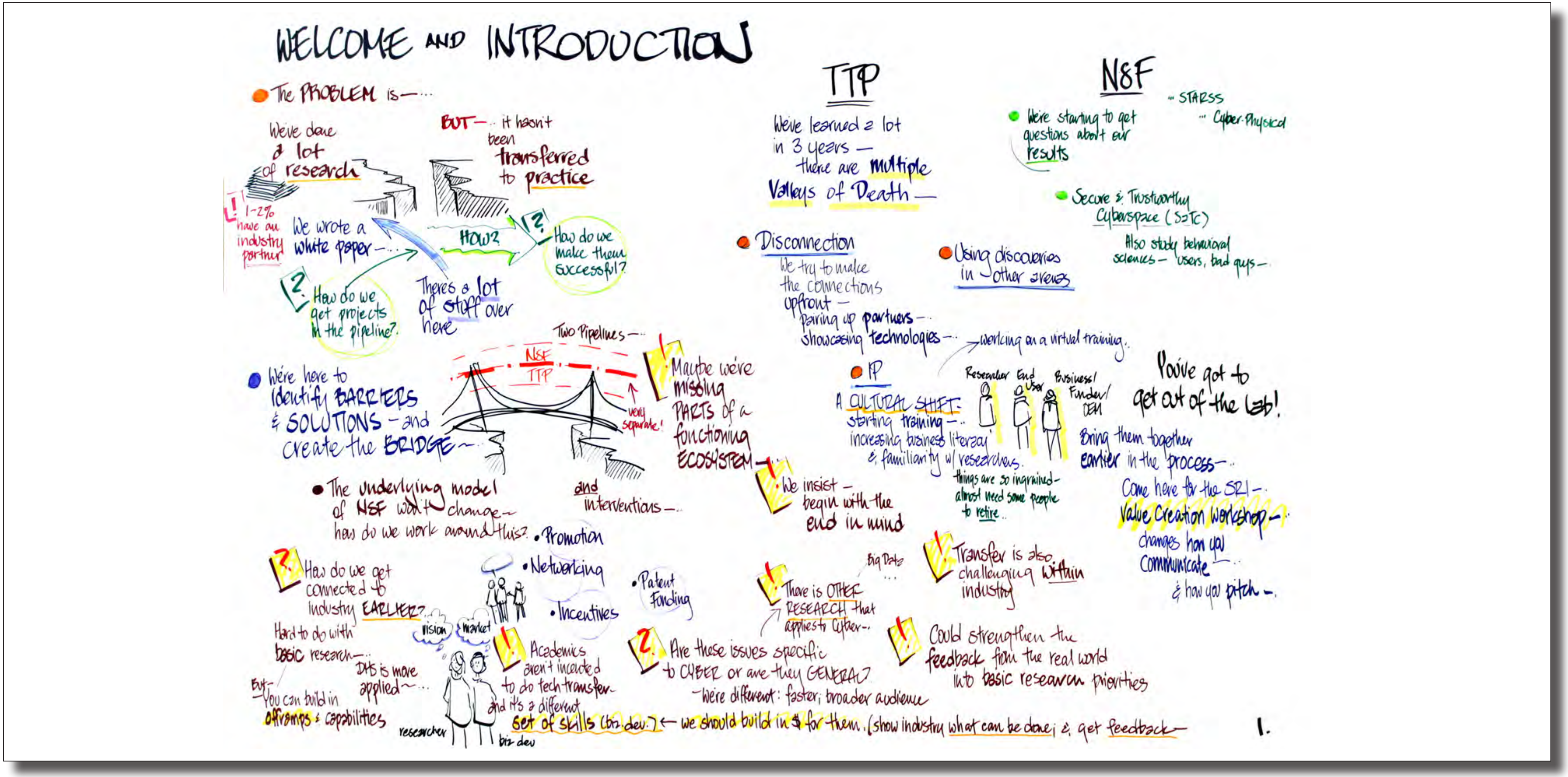
TECHNOLOGY TRANSFER TO PRACTICE IN CYBER SECURITY WORKSHOP

SRI International Offices
Menlo Park, California
February 25 & 26, 2015

Tom Benthin Graphic Facilitator

tombenthin.com

WELCOME & INTRODUCTION



WELCOME AND INTRODUCTION

- The PROBLEM is—…

We've done a lot of research

BUT—… it hasn't been transferred to practice

! 1-2% have an industry partner

We wrote a white paper—…

HOW?

? How do we make them successful?

? How do we get projects in the pipeline?

There's a lot of stuff over here

Two Pipelines—…

NSF

TTP

very separate!

- We're here to identify BARRIERS & SOLUTIONS – and create the BRIDGE—…

! Maybe we're missing PARTS of a functioning ECOSYSTEM—

- The underlying model of NSF won't change— how do we work around this?

and interventions—…

- Promotion
- Networking
- Incentives
- Patent Funding

? How do we get connected to Industry EARLIER?

Hard to do with basic research—…

DHS is more applied—…

But— You can build in offramps & capabilities

! Academics aren't incented to do tech transfer. and it's a different set of skills (biz. dev.) ← we should build in $ for them. (show industry what can be done; & get feedback—

? Are these issues specific to CYBER or are they GENERAL? —We're different: faster; broader audience

TTP

We've learned a lot in 3 years — there are multiple Valleys of Death —

- Disconnection
  We try to make the connections upfront —
  pairing up partners—…
  showcasing technologies—… →working on a virtual training.

- Using discoveries in other arenas

- IP
  A CULTURAL SHIFT: starting training—… increasing business literacy & familiarity w/ researchers.

things are so ingrained– almost need some people to retire..

! We insist – begin with the end in mind

! There is OTHER RESEARCH that applies to Cyber–.

Big Data …

! Transfer is also challenging within industry

! Could strengthen the feedback from the real world into basic research priorities

NSF

… STARSS

… Cyber-Physical

- We're starting to get questions about our results

- Secure & Trustworthy Cyberspace (S&TC)

Also study behavioral sciences – users, bad guys—

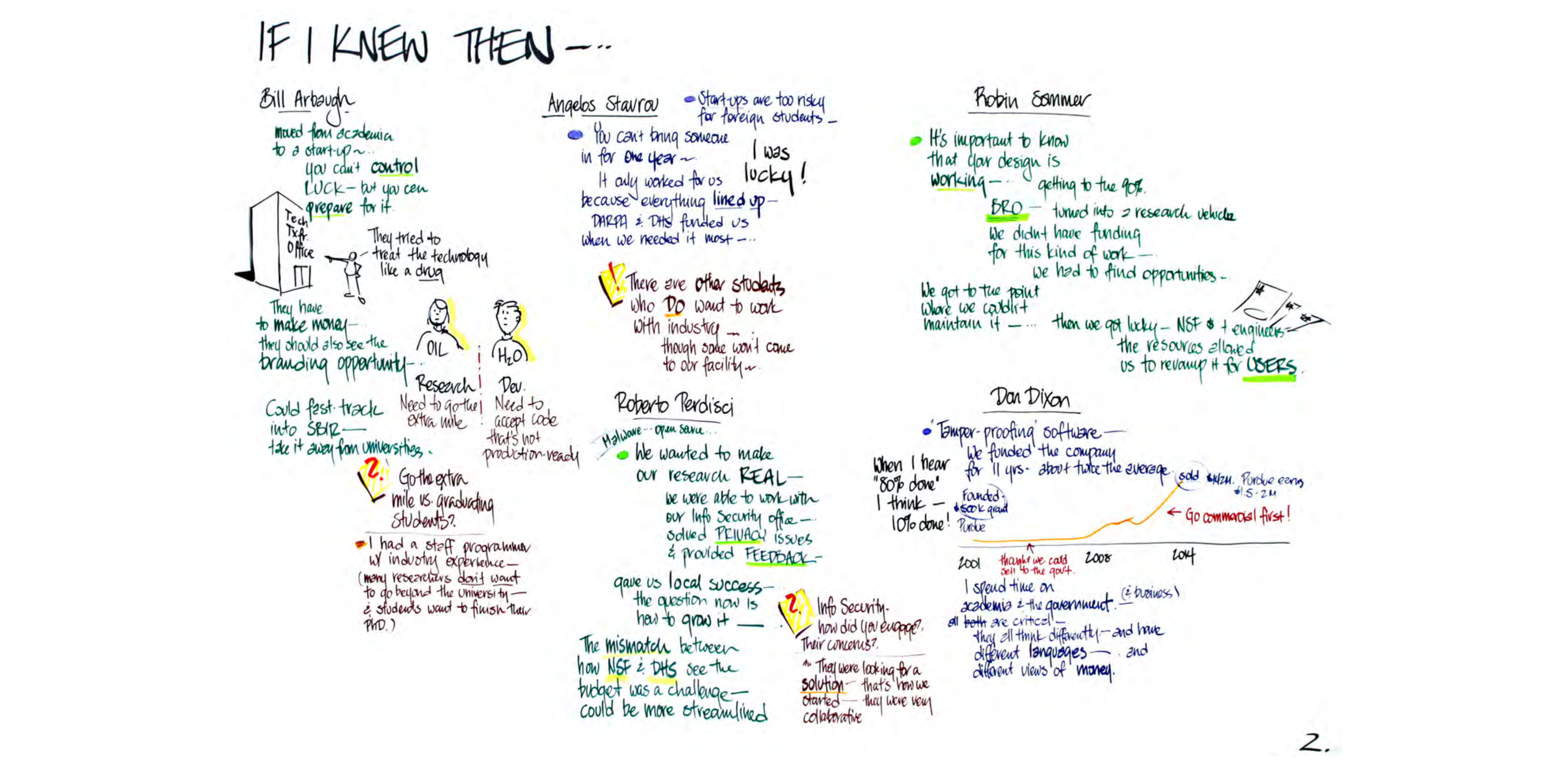
You've got to get out of the lab!

Bring them together earlier in the process—…

Come here for the SRI—… Value Creation Workshop—… changes how you communicate—… & how you pitch—.

1.

IF I KNEW THEN WHAT I KNOW NOW



IF I KNEW THEN —..

Bill Arbaugh

moved from academia to a start-up~..
you can't control LUCK— but you can prepare for it.

They tried to treat the technology like a drug

They have to make money—..
they should also see the branding opportunity—..

Research
Need to go the extra mile

Dev.
Need to accept code that's not production-ready

Could fast-track into SBIR—
take it away from universities.

?! Go the extra mile vs. graduating students?

- I had a staff programmer w/ industry experience—
(many researchers don't want to go beyond the university—
& students want to finish their PhD.)

Angelos Stavrou

- Start-ups are too risky for foreign students—
- You can't bring someone in for one year~
It only worked for us because everything lined up—
DARPA & DHS funded us when we needed it most—..

I was lucky!

! There are other students who DO want to work with industry~.
though some won't come to our facility~.

Roberto Perdisci

Malware... open source...

- We wanted to make our research REAL—
we were able to work with our Info Security office—..
solved PRIVACY issues
& provided FEEDBACK—
gave us local success—
the question now is how to grow it —.

The mismatch between how NSF & DHS see the budget was a challenge—
could be more streamlined

?! Info Security-
how did you engage?
Their concerns?

~ They were looking for a solution— that's how we started— they were very collaborative

Robin Sommer

- It's important to know that your design is working—.. getting to the 90%.
BRO — turned into a research vehicle
We didn't have funding for this kind of work—
we had to find opportunities -
We got to the point where we couldn't maintain it —... then we got lucky— NSF $ + engineers—
the resources allowed us to revamp it for USERS.

Don Dixon

- 'Tamper-proofing' software—
We funded the company for 11 yrs- about twice the average.

When I hear "80% done" I think — 10% done!

Founded- $500K grant Purdue
sold $142M. Purdue earns $1.5-2M
← Go commercial first!
2001
thought we could sell to the gov't.
2008
2014

I spend time on academia & the government. (& business)
all ~~both~~ are critical—
they all think differently— and have different languages — . and different views of money.

2.

IF I KNEW THEN WHAT I KNOW NOW, cont.

IF I KNEW THEN — .. continued ..

Isn't the gov't in a better position to do early buying?

- No – I'm not required to ..

they'll do it when they're forced to.

I'm guessing someone's pushing the PAPER.

we might have also been too early – didn't test it —

critical to see what customers will PAY FOR —

It's so much easier to do commercial first —

systems Integrators want to custom-build systems —

here in the Valley were interested in increasing PRODUCTIVITY instead —.

If you could hire one consultant?

- Someone with business experience
- A lawyer
- A ~~Program~~ Product Project Mgr. (sales) (sales & tech)
- Someone who's done it before ~

Attitudes towards RISK are a big disconnect — ..

A dev team in the middle can make it connect — with a reachback to the inventor ~

PASSION is necessary but not SUFFICIENT — sometimes you really need the inventor — and they have to be available THEN.

We actively support our transferred tech

Some investors all want them to share the RISK as well

What % of start-ups will be successful?

- Don't think it matters — I was passionate

- It's a personal decision ~ .. I like what I'm doing now ~ the research lifestyle ("lifestyle security") — It's like moving to another country –

As your products scale, what about your research?

Our funding ends next year — will have both a start-up and an open-source community

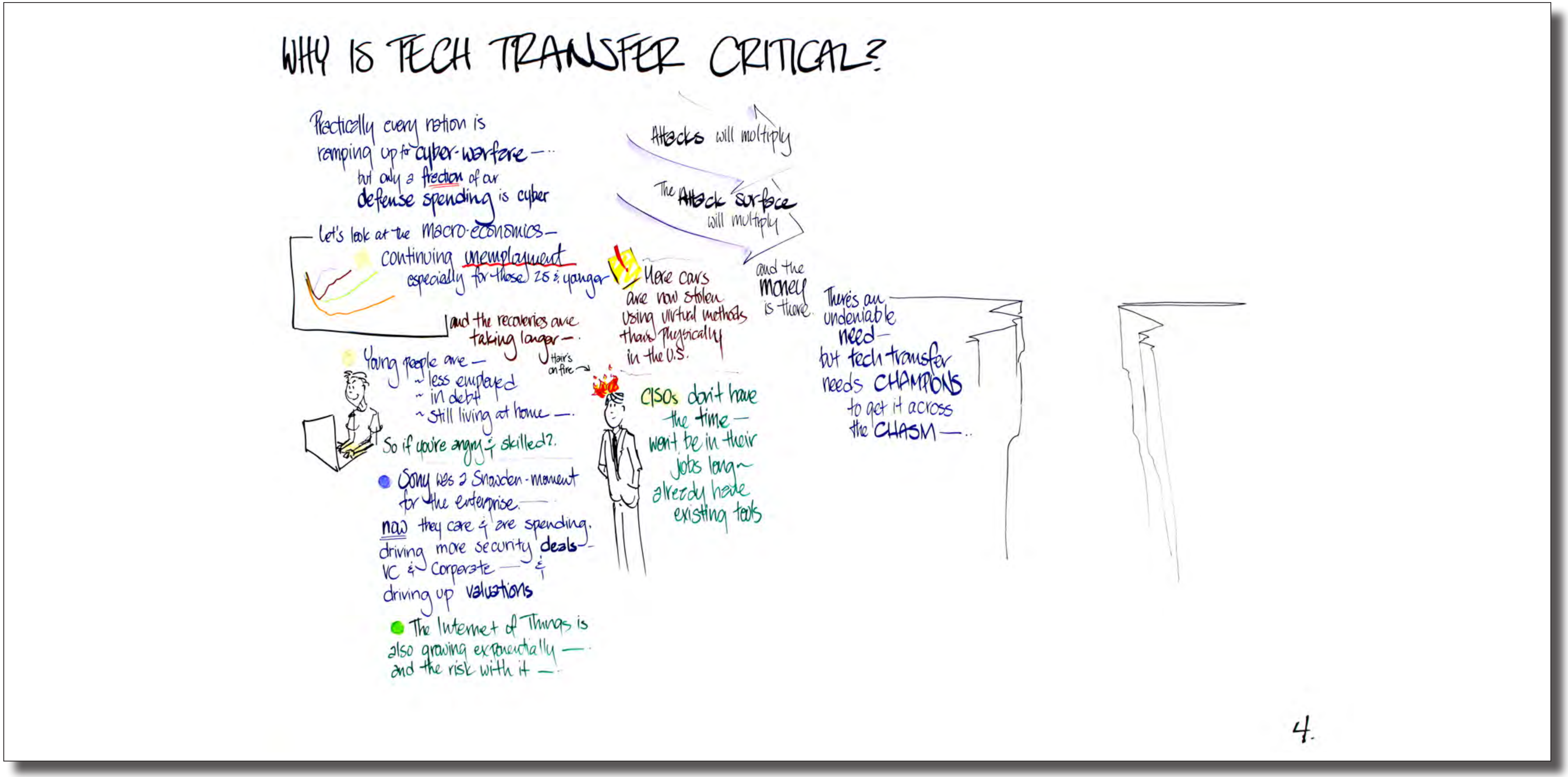
This is tough — each will undercut the other!

It's vital to build in connections early — at the end of a project, it's too late — a true researcher wants to move on to the next product ~ best can be for a student to carry it on

You need a Product Manager — universities can't fund it – you need a commercial entity to come in sooner ~ but with what funding?

3.

WHY IS TECH TRANSFER CRITICAL?



Practically every nation is ramping up for cyber-warfare —.. but only a fraction of our defense spending is cyber

Let's look at the macro-economics — continuing unemployment especially for those 25 & younger

and the recoveries are taking longer —.

Young people are —
~ less employed
~ in debt
~ still living at home —.

So if you're angry & skilled?.

- Sony was a Snowden-moment for the enterprise. —

now they care & are spending. driving more security deals — VC & Corporate — & driving up valuations

- The Internet of Things is also growing exponentially —. and the risk with it —.

Attacks will moltiply

The Attack surface will multiply

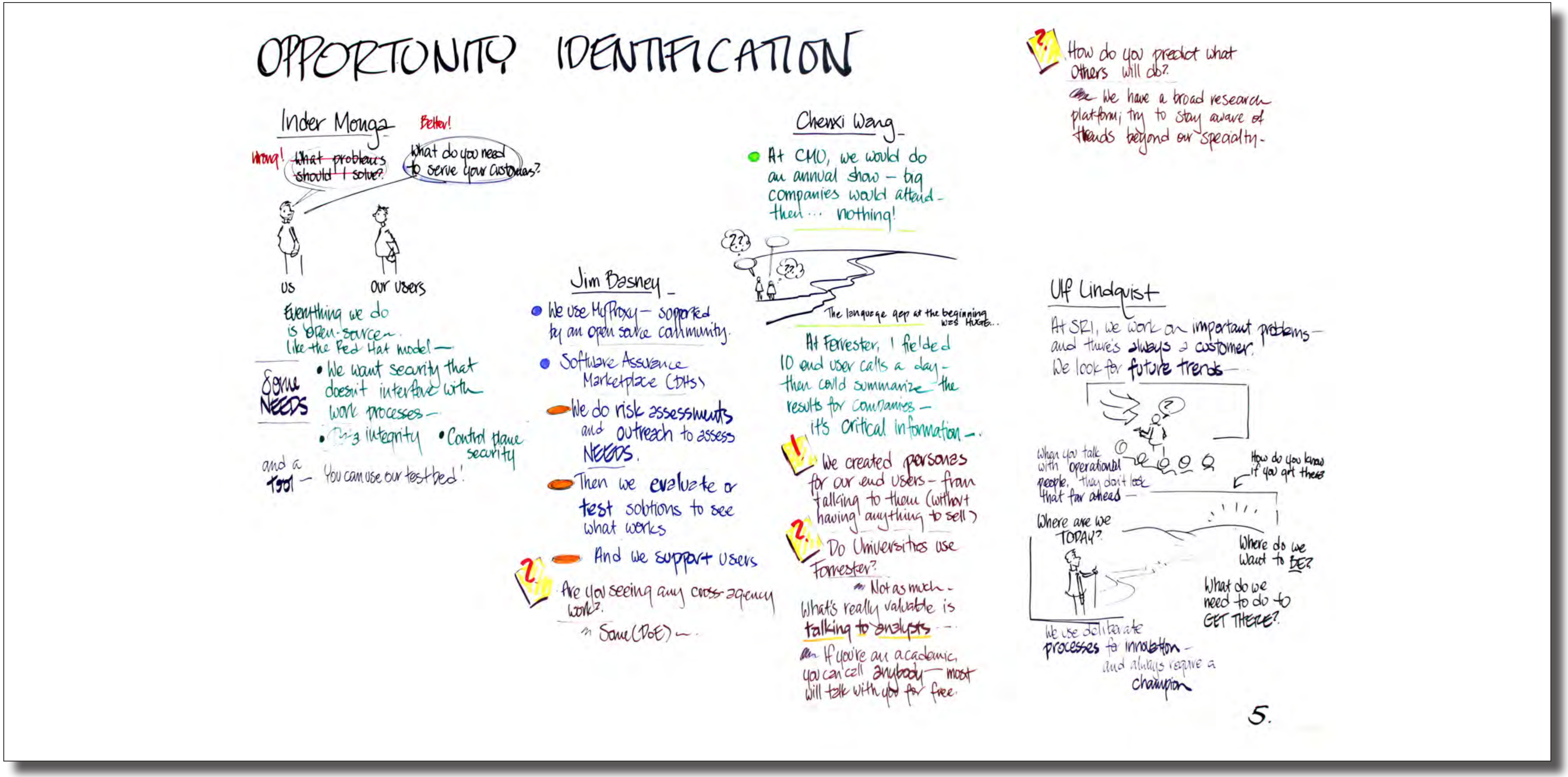
and the money is there.

More cars are now stolen using virtual methods than physically in the U.S.

CISOs don't have the time — won't be in their jobs long — already have existing tools

There's an undeniable need — but tech transfer needs CHAMPIONS to get it across the CHASM —..

OPPORTUNITY IDENTIFICATION



OPPORTUNITY IDENTIFICATION

Inder Monga

Wrong! ~~What problems should I solve?~~

Better! What do you need to serve your customers?

Everything we do is open-source.
like the Red Hat model —

Some NEEDS

- We want security that doesn't interfere with work processes —
- [illegible] integrity
- Control plane security

and a Tool — You can use our test bed!

Jim Basney

- We use MyProxy — supported by an open source community.
- Software Assurance Marketplace (DHS)
- We do risk assessments and outreach to assess NEEDS.
- Then we evaluate or test solutions to see what works
- And we support users

?. Are you seeing any cross-agency work?
Some (DoE) —

Chenxi Wang

- At CMU, we would do an annual show — big companies would attend — then… nothing!

The language gap at the beginning was HUGE…

At Forrester, I fielded 10 end user calls a day — then could summarize the results for companies — it's critical information —

!. We created personas for our end users — from talking to them (without having anything to sell)

?. Do Universities use Forrester?
Not as much — What's really valuable is talking to analysts —
If you're an academic, you can call anybody — most will talk with you for free.

?. How do you predict what Others will do?
We have a broad research platform; try to stay aware of trends beyond our specialty.

Ulf Lindquist

At SRI, we work on important problems — and there's always a customer.
We look for future trends —

When you talk with operational people, they don't look that far ahead —

How do you know if you got there

Where are we TODAY?

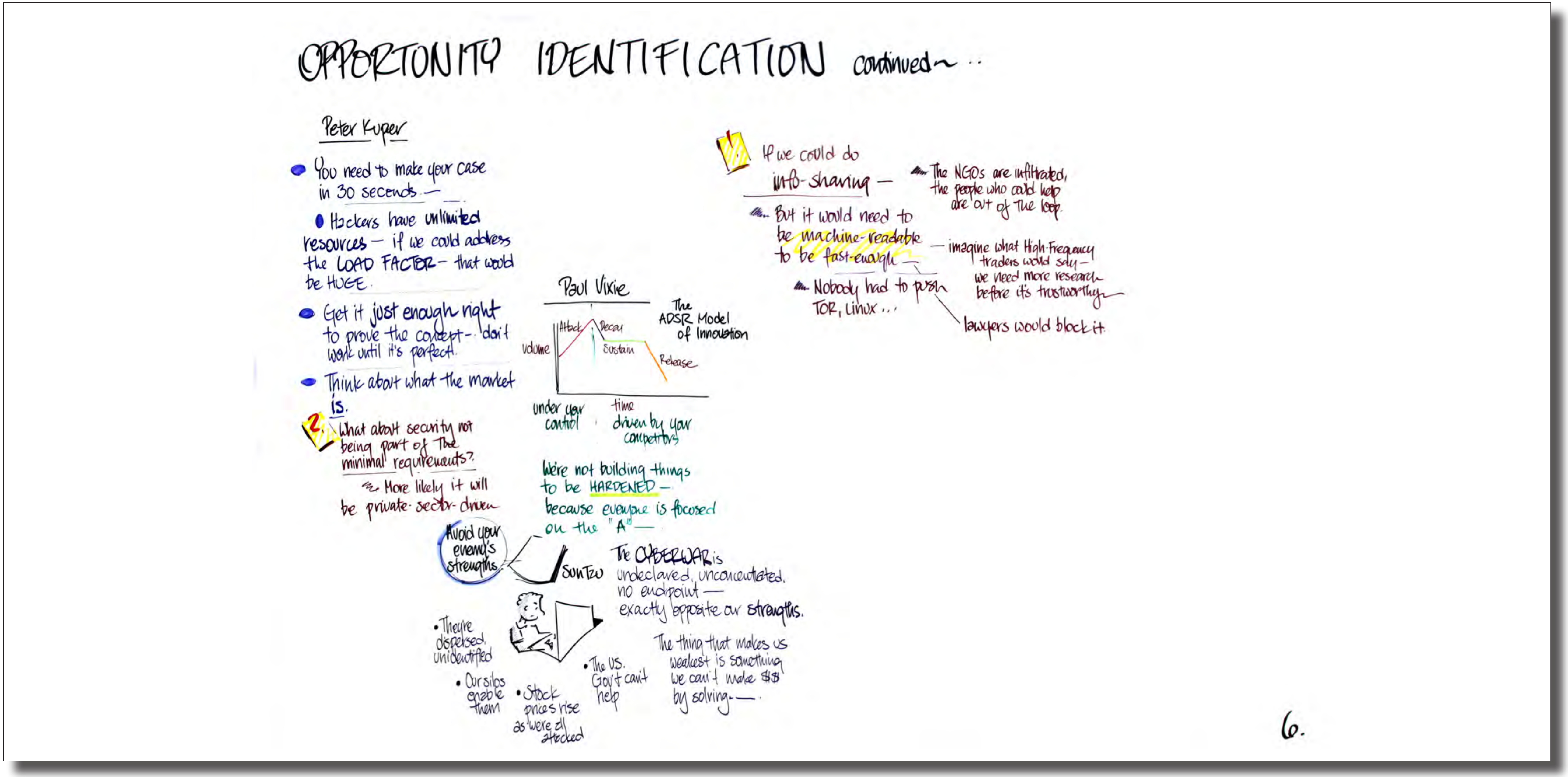
Where do we want to BE?

What do we need to do to GET THERE?

We use deliberate processes for innovation — and always require a champion

5.

OPPORTUNITY IDENTIFICATION, cont.



OPPORTUNITY IDENTIFICATION continued~ . .

Peter Kuper

- You need to make your case in 30 seconds —
- Hackers have unlimited resources — if we could address the LOAD FACTOR — that would be HUGE.
- Get it just enough right to prove the concept — don't work until it's perfect.
- Think about what the market is.

2. What about security not being part of The minimal requirements?

More likely it will be private-sector-driven

Paul Vixie

We're not building things to be HARDENED — because everyone is focused on the "A" —

Avoid your enemy's strengths

Sun Tzu

The CYBERWAR is undeclared, unconcentrated, no endpoint — exactly opposite our strengths.

- They're dispersed, unidentified
- Our silos enable them
- Stock prices rise as we're all attacked
- The U.S. Gov't can't help

The thing that makes us weakest is something we can't make $$ by solving —

If we could do info-sharing —

The NGOs are infiltrated, the people who could help are out of The loop.

But it would need to be machine-readable to be fast-enough —

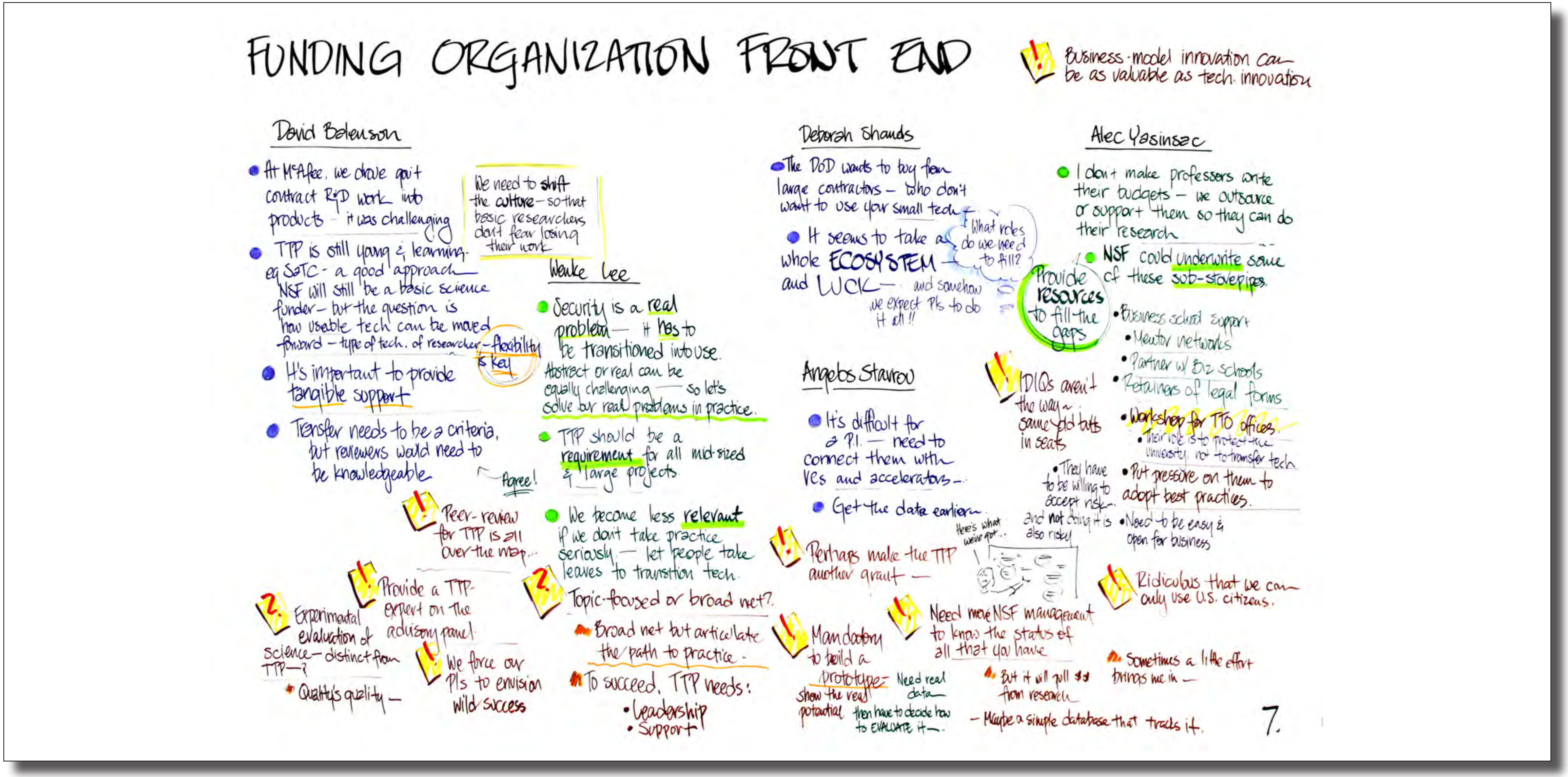
— imagine what High-Frequency traders would say — we need more research before it's trustworthy —

Nobody had to push TOR, Linux . . .

lawyers would block it.

6.

FUNDING ORGANIZATION FRONT END



FUNDING ORGANIZATION FRONT END

Business model innovation can be as valuable as tech. innovation

David Balenson

- At McAfee, we drove gov't contract R&D work into products – it was challenging
- TTP is still young & learning. eg SaTC - a good approach – NSF will still be a basic science funder – but the question is how usable tech can be moved forward – type of tech. of researcher – flexibility is key
- It's important to provide tangible support
- Transfer needs to be a criteria, but reviewers would need to be knowledgeable ← Agree!

We need to shift the culture – so that basic researchers don't fear losing their work

Wenke Lee

- Security is a real problem – it has to be transitioned into use. Abstract or real can be equally challenging – so let's solve our real problems in practice.
- TTP should be a requirement for all mid-sized & large projects
- We become less relevant if we don't take practice seriously – let people take leaves to transition tech.

! Peer-review for TTP is all over the map...

! Provide a TTP-expert on the advisory panel.

? Experimental evaluation of science – distinct from TTP – ?

- Quality's quality –

! We force our PIs to envision wild success

? Topic-focused or broad net?

- Broad net but articulate the path to practice.
- To succeed, TTP needs:
  - Leadership
  - Support

Deborah Shands

- The DoD wants to buy from large contractors – who don't want to use your small tech
- It seems to take a whole ECOSYSTEM and LUCK – and somehow we expect PIs to do it all!!

What roles do we need to fill?

Angelos Stavrou

- It's difficult for a P.I. – need to connect them with VCs and accelerators –
- Get the data earlier –

Here's what we've got...

! Perhaps make the TTP another grant –

! Mandatory to build a prototype – show the real potential. Need real data – then have to decide how to EVALUATE it –

! Need more NSF management to know the status of all that you have

- But it will pull $$ from research
- Maybe a simple database that tracks it.

Alec Yasinsac

- I don't make professors write their budgets – we outsource or support them so they can do their research
- NSF could underwrite some of these sub-stovepipes.

Provide resources to fill the gaps

- Business school support
  - Mentor networks
  - Partner w/ Biz schools
- Retainers of legal forms
- Workshop for TTO offices.
  - Their role is to protect the university, not to transfer tech
- Put pressure on them to adopt best practices.
- Need to be easy & open for business

! IDIQs aren't the way – same old butts in seats

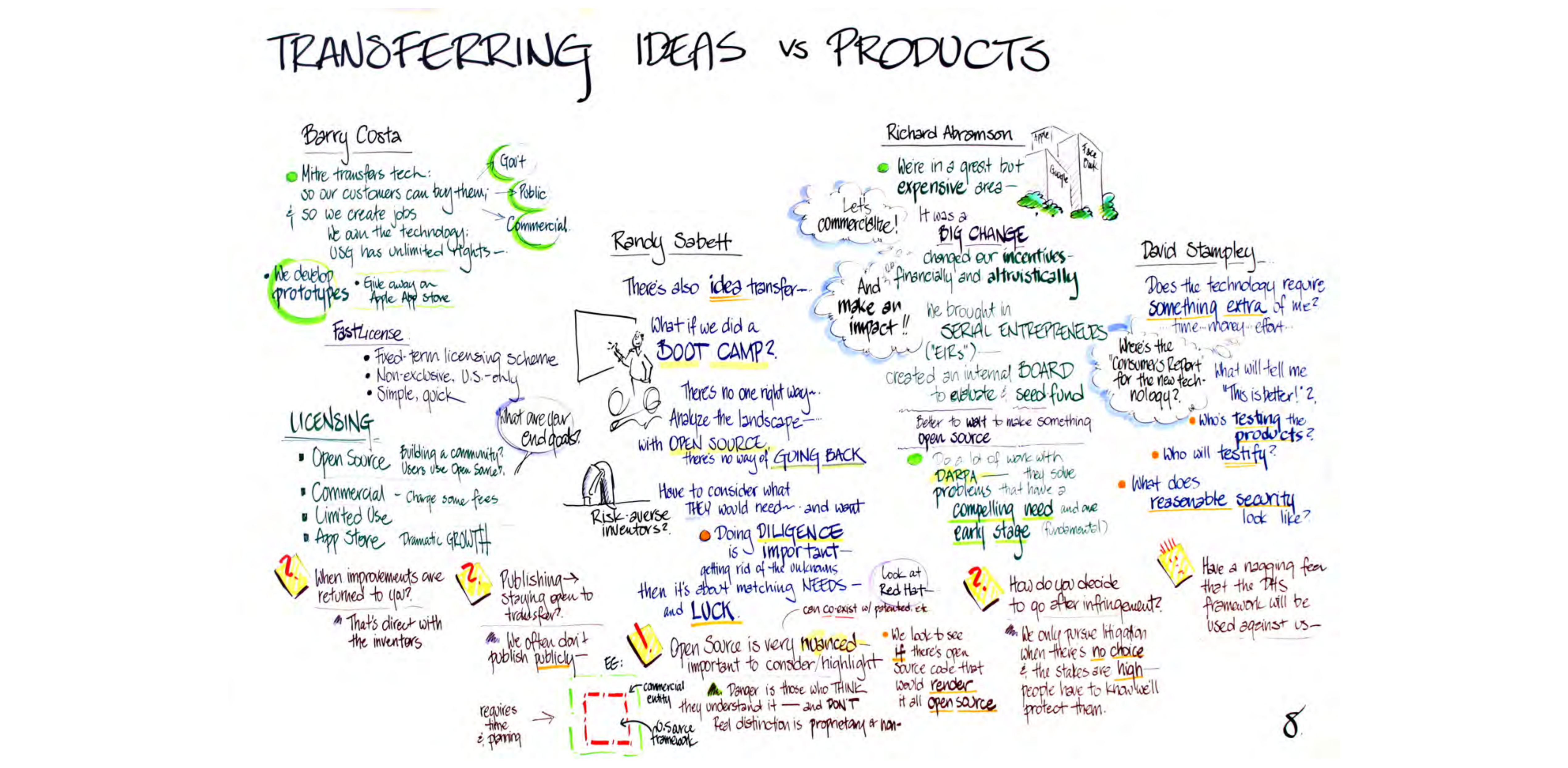
- They have to be willing to accept risk – and not doing it is also risky

! Ridiculous that we can only use U.S. citizens.

- Sometimes a little effort brings me in –

7.

TRANSFERRING IDEAS VS PRODUCTS



TRANSFERRING IDEAS vs PRODUCTS

Barry Costa

- Mitre transfers tech:
  so our customers can buy them; → Gov't → Public → Commercial.
  & so we create jobs
  We own the technology:
  USG has unlimited rights –
- We develop prototypes
  - Give away on Apple App store

FastLicense

- Fixed-term licensing scheme
- Non-exclusive, U.S.-only
- Simple, quick

What are your end goals?

LICENSING

- Open Source — Building a community? Users use Open Source?
- Commercial – Charge some fees
- Limited Use
- App Store — Dramatic GROWTH

?. When improvements are returned to you?

- That's direct with the inventors

?. Publishing → staying open to transfer?

- We often don't publish publicly –

Randy Sabett

There's also idea transfer –

What if we did a BOOT CAMP?

There's no one right way –.

Analyze the landscape –

with OPEN SOURCE, there's no way of GOING BACK

Risk-averse inventors?

Have to consider what THEY would need – and want

- Doing DILIGENCE is important – getting rid of the unknowns then it's about matching NEEDS – and LUCK.

Look at Red Hat –

can co-exist w/ patented, etc

EE:

! Open Source is very nuanced – important to consider/highlight

- Danger is those who THINK they understand it — and DON'T

Real distinction is proprietary or non-

requires time & planning →

commercial entity

O.Source framework

Richard Abramson

Apple

Google

Face Book

- We're in a great but expensive area –

Let's commercialize!

And make an impact!!

It was a BIG CHANGE changed our incentives – financially and altruistically

We brought in SERIAL ENTREPRENEURS ("EIRs") –

created an internal BOARD to evaluate & seed fund

Better to wait to make something open source

- Do a lot of work with DARPA — they solve problems that have a compelling need and are early stage (fundamental)

- We look to see if there's open source code that would render it all open source

?. How do you decide to go after infringement?

- We only pursue litigation when there's no choice & the stakes are high – people have to know we'll protect them.

David Stampley

Does the technology require something extra of me? ... time ... money ... effort ...

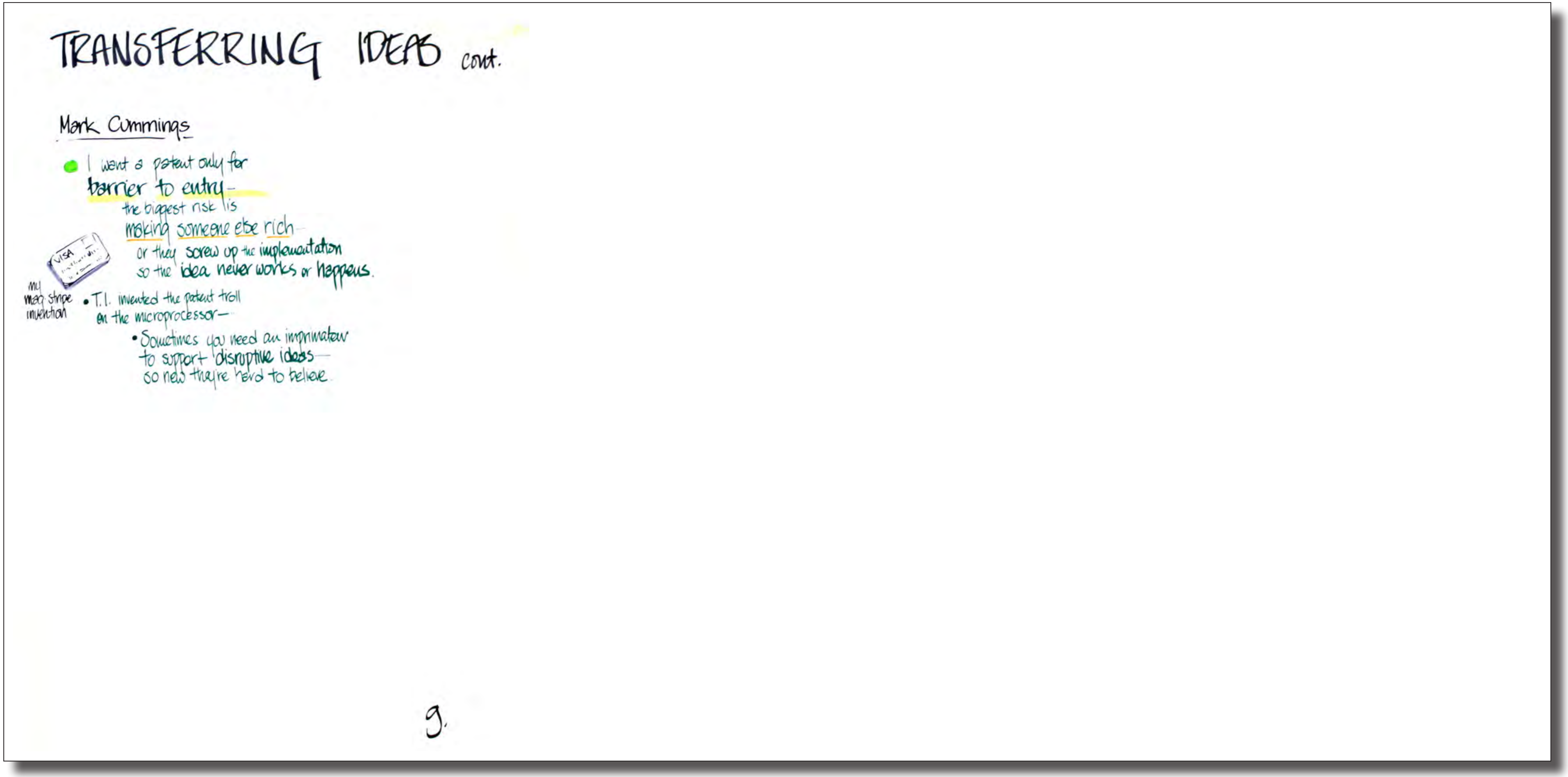
Where's the "Consumer's Report" for the new technology?

What will tell me "This is better!"?

- Who's testing the products?
- Who will testify?
- What does reasonable security look like?

Have a nagging fear that the DHS framework will be used against us –

TRANSFERRING IDEAS VS PRODUCTS, cont.



TRANSFERRING IDEAS cont.

Mark Cummings

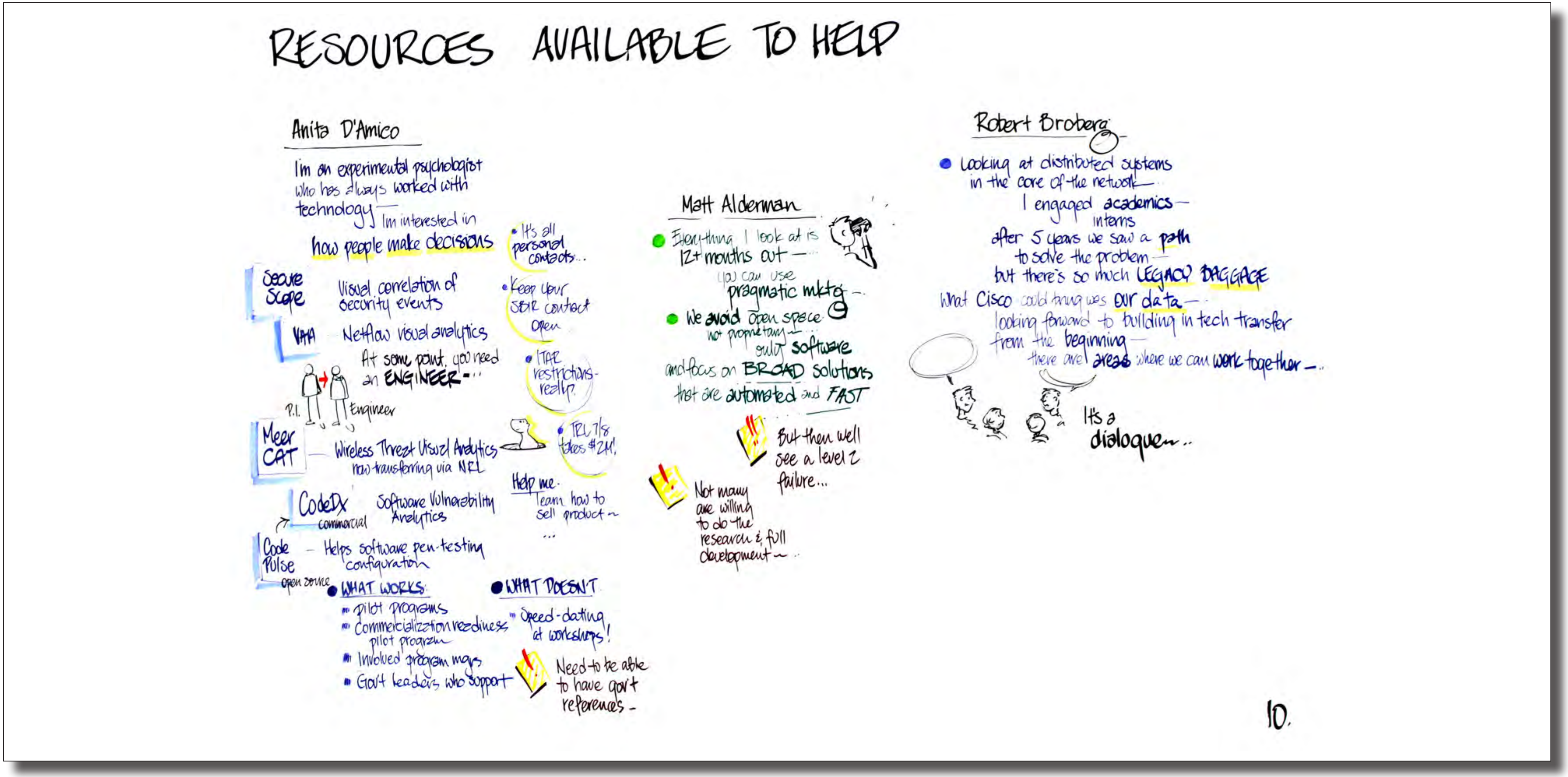
● I want a patent only for **barrier to entry** –
the biggest risk is
making someone else rich –
or they screw up the implementation
so the idea never works or happens.

my mag stripe invention

- T.I. invented the patent troll on the microprocessor –
  - Sometimes you need an imprimateur to support disruptive ideas – so new they're hard to believe.

g.

RESOURCES AVAILABLE TO HELP



RESOURCES AVAILABLE TO HELP

Anita D'Amico

I'm an experimental psychologist who has always worked with technology — I'm interested in how people make decisions

- It's all personal contacts...
- Keep your SBIR contact open
- ITAR restrictions - really.
- TRL 7/8 takes $2M!

Secure Scope — Visual correlation of security events

VAHA — Netflow visual analytics

At some point, you need an ENGINEER -..

P.I. → Engineer

Meer CAT — Wireless Threat Visual Analytics now transferring via NRL

Help me. Team how to sell product ~ ...

CodeDx commercial — Software Vulnerability Analytics

Code Pulse open source — Helps software pen-testing configuration

- WHAT WORKS:
  - pilot programs
  - Commercialization readiness pilot program
  - Involved program mgrs
  - Gov't leaders who support
- WHAT DOESN'T
  - Speed-dating at workshops!

Need to be able to have gov't references -

Matt Alderman

- Everything I look at is 12+ months out —... you can use pragmatic mktg -.
- We avoid open space not proprietary ... only software and focus on BROAD solutions that are automated and FAST

But then we'll see a level 2 failure...

Not many are willing to do the research & full development ~ ..

Robert Broberg

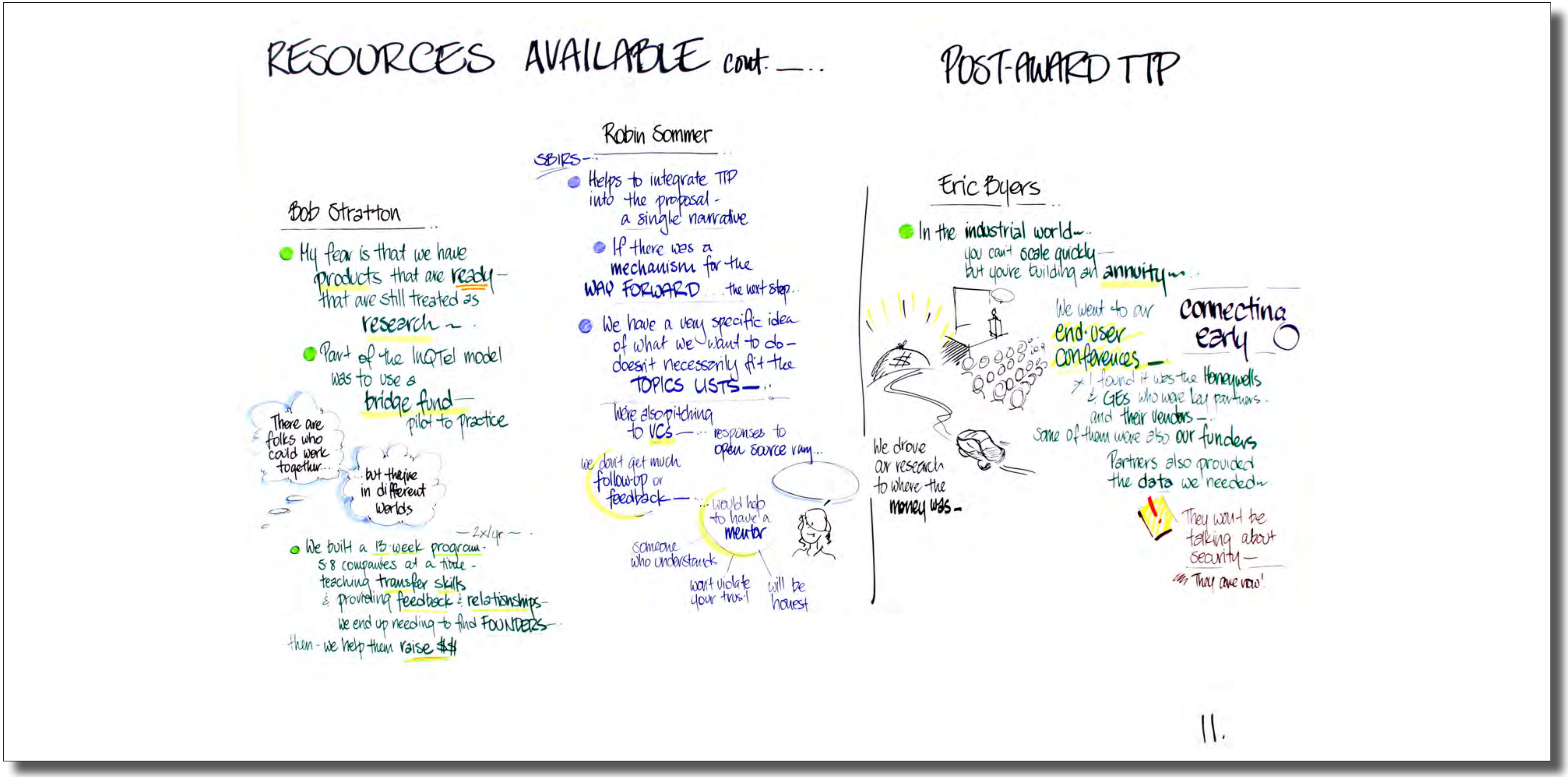
- Looking at distributed systems in the core of the network — I engaged academics — interns after 5 years we saw a path to solve the problem — but there's so much LEGACY BAGGAGE

What Cisco could bring was our data — looking forward to building in tech transfer from the beginning — there are areas where we can work together —..

It's a dialogue ..

10.

RESOURCES AVAILABLE TO HELP & POST-AWARD TTP



RESOURCES AVAILABLE cont. — ..

Bob Stratton

- My fear is that we have products that are ready — that are still treated as research ~
- Part of the InQTel model was to use a bridge fund — pilot to practice

There are folks who could work together...

... but they're in different worlds

- We built a 13-week program. — 2x/yr —
  5·8 companies at a time - teaching transfer skills & providing feedback & relationships - we end up needing to find FOUNDERS -
  then - we help them raise $$!

Robin Sommer

SBIRS - ..

- Helps to integrate TTP into the proposal - a single narrative
- If there was a mechanism for the WAY FORWARD . . the next step..
- We have a very specific idea of what we want to do - doesn't necessarily fit the TOPICS LISTS — ..

We're also pitching to VCs — ... responses to open source vary...

we don't get much follow-up or feedback — ... would help to have a mentor

someone who understands

won't violate your trust

will be honest

POST-AWARD TTP

Eric Byers

- In the industrial world - .. you can't scale quickly — but you're building an annuity ...

We drove our research to where the money was -

We went to our end-user conferences —

connecting early

* I found it was the Honeywells & GEs who were key partners. and their vendors — .. some of them were also our funders

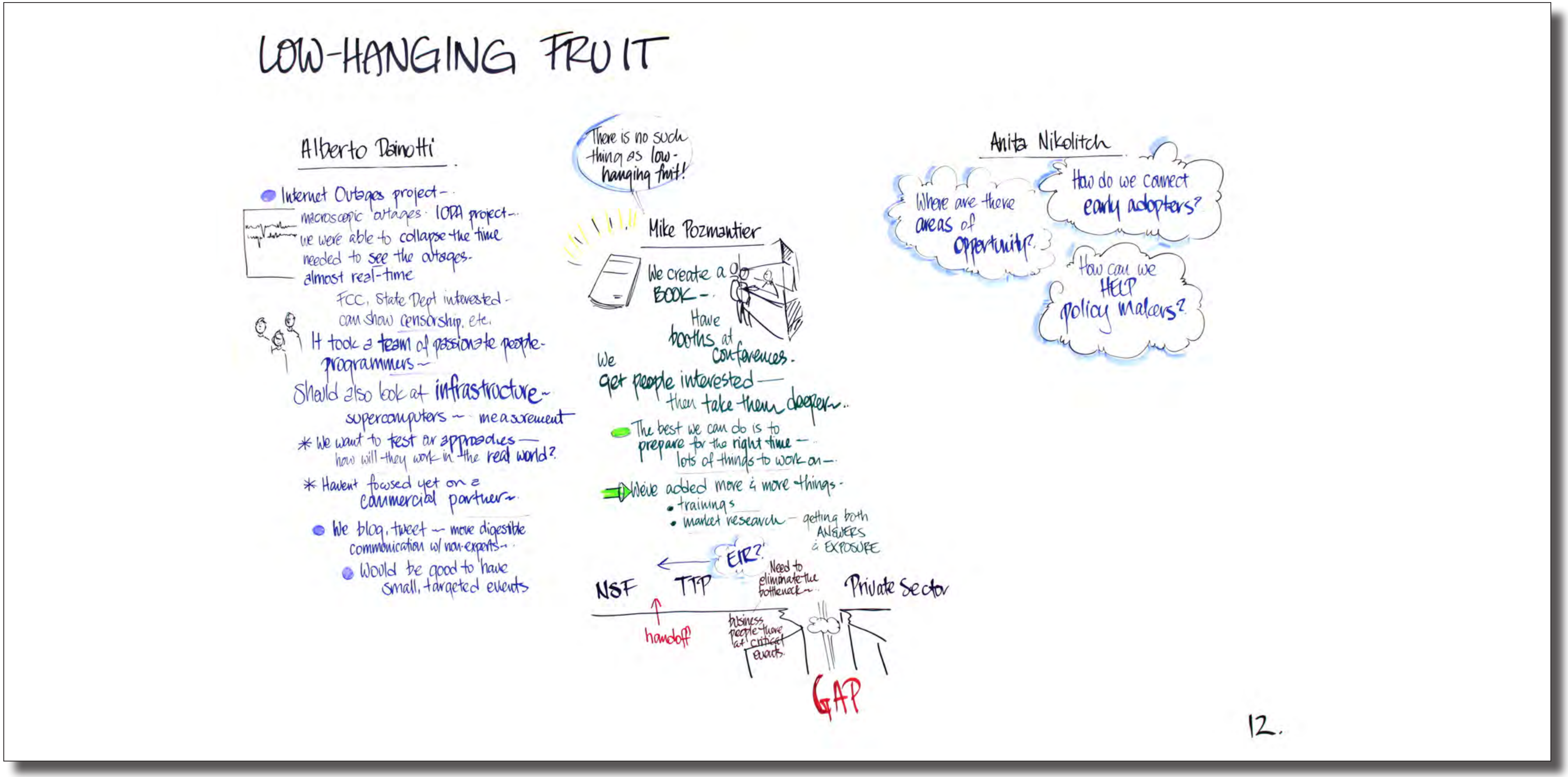
Partners also provided the data we needed -

They won't be talking about security —

They are now!

11.

LOW-HANGING FRUIT



LOW-HANGING FRUIT

Alberto Dainotti

- Internet Outages project - macroscopic outages · IODA project - we were able to collapse the time needed to see the outages. almost real-time

  FCC, State Dept interested - can show censorship, etc.

  It took a team of passionate people - programmers ~

  Should also look at infrastructure ~ supercomputers ~ measurement

  * We want to test our approaches — how will they work in the real world?

  * Havent focused yet on a commercial partner ~

- We blog, tweet ~ more digestible communication w/ non-experts ~
- Would be good to have small, targeted events

There is no such thing as low-hanging fruit!

Mike Pozmantier

We create a BOOK - .

Have booths at conferences.

We get people interested — then take them deeper ~ ..

- The best we can do is to prepare for the right time - lots of things to work on - .

⇒ Weve added more & more things -
- trainings
- market research - getting both ANSWERS & EXPOSURE

EIR?

NSF

TTP

handoff

Need to eliminate the bottleneck ~

business people there at critical events.

Private Sector

GAP

Anita Nikolitch

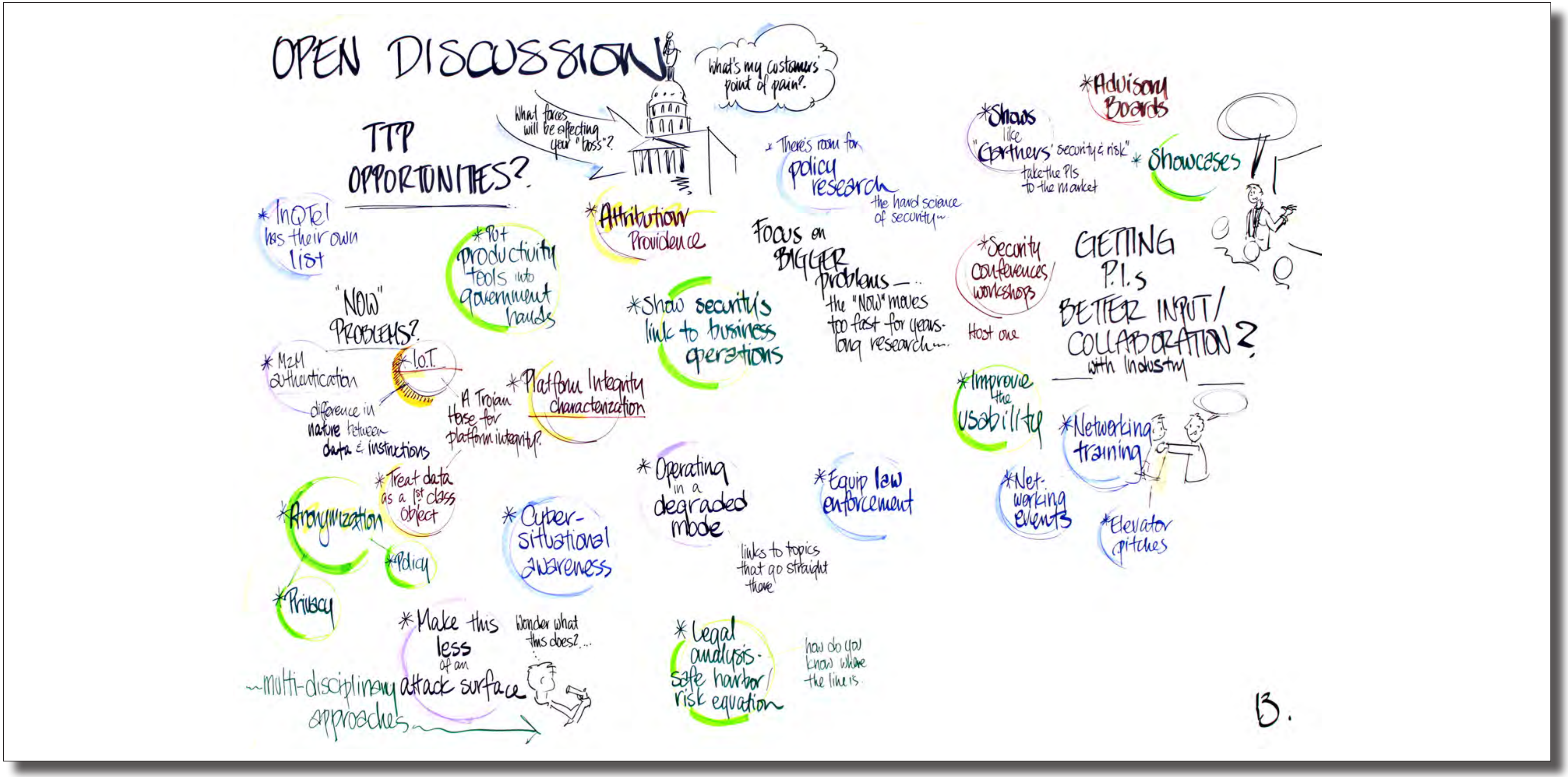
Where are there areas of opportunity?

How do we connect early adopters?

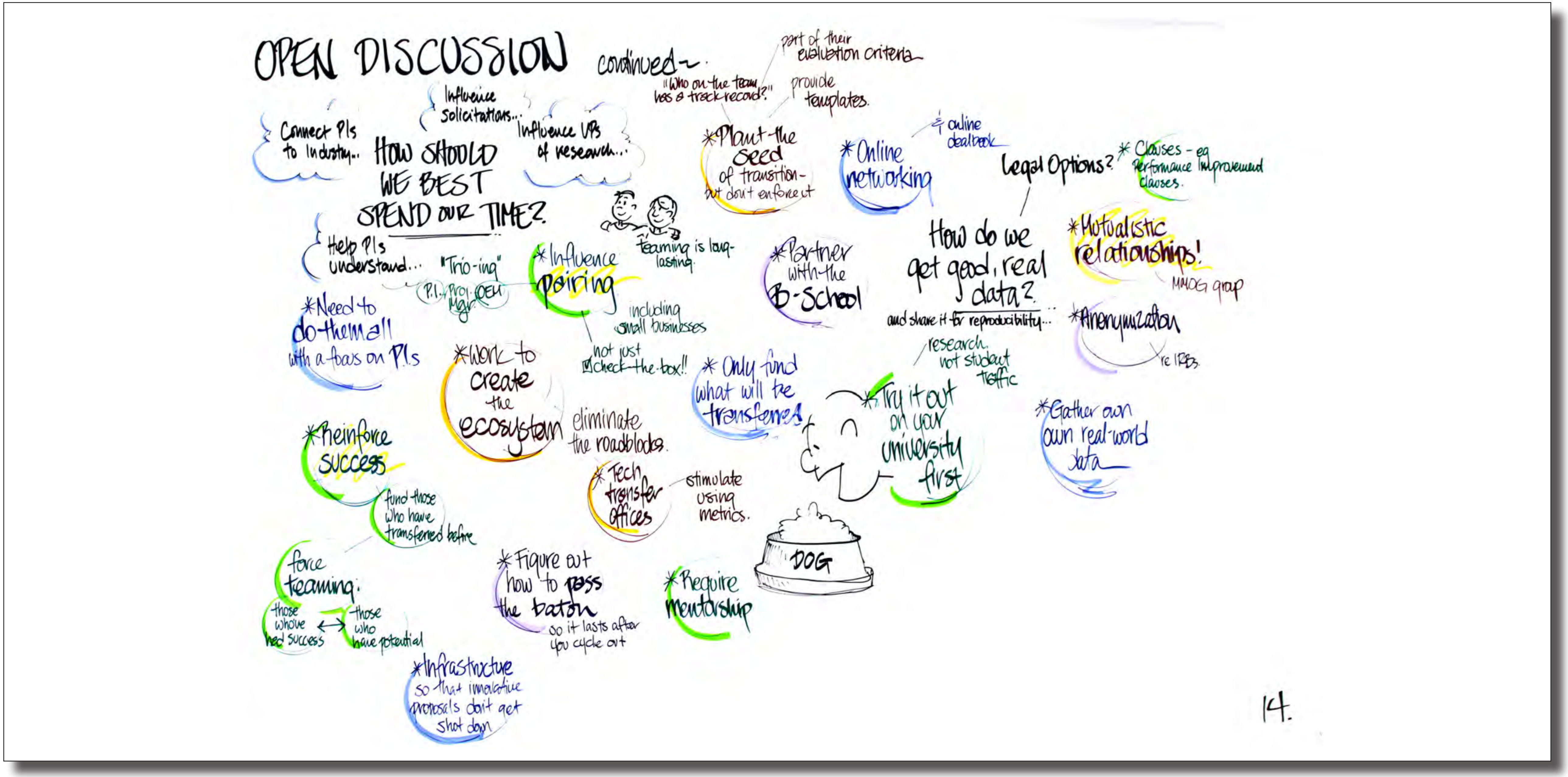
How can we HELP policy makers?

12.

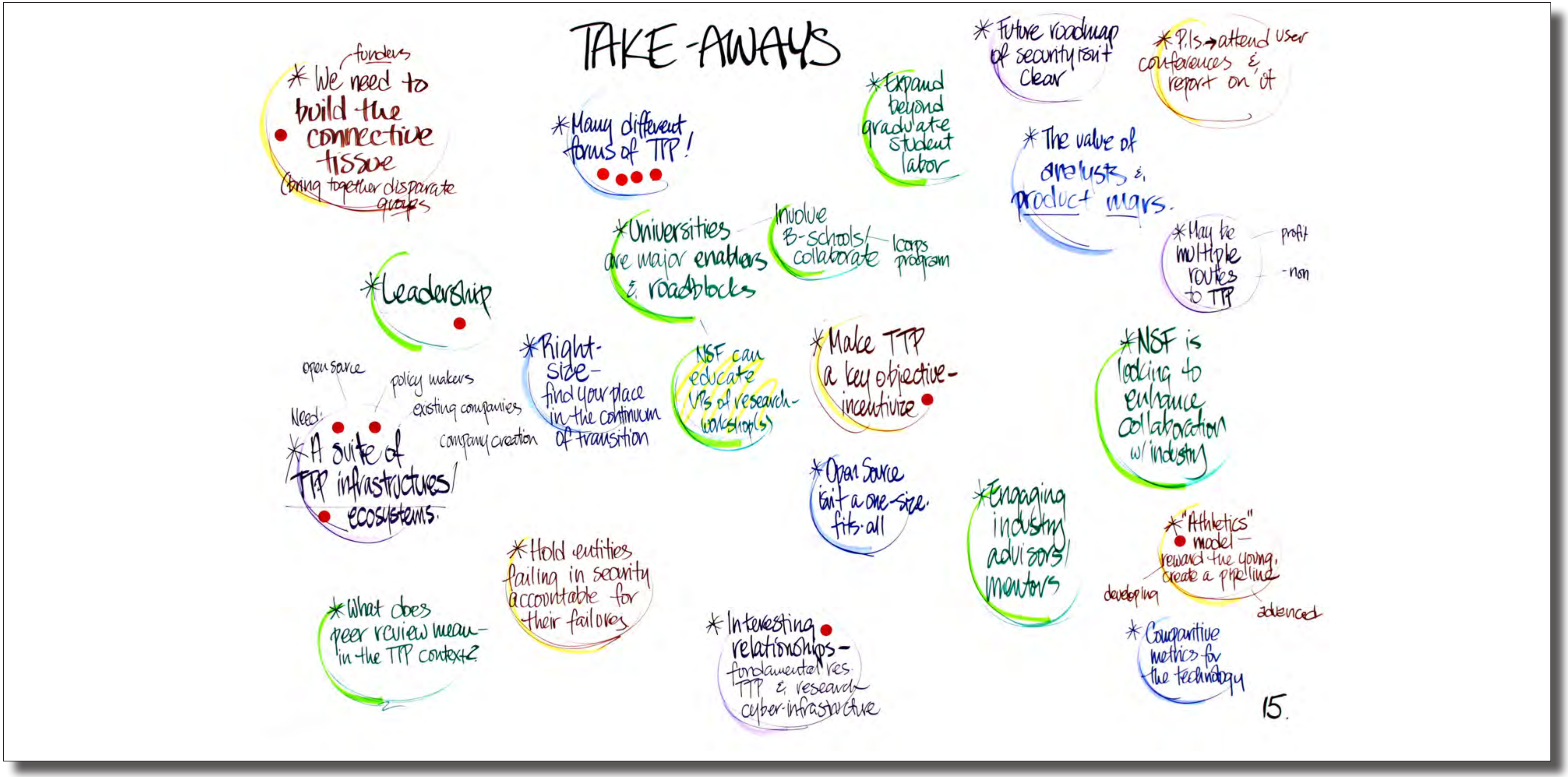
OPEN DISCUSSION


OPEN DISCUSSION
What's my customers' point of pain?
What forces will be affecting your "boss"?
TTP OPPORTUNITIES?
* InQTel has their own list
* Put productivity tools into government hands
* Attribution Providence
* There's room for policy research
the hard science of security...
Focus on BIGGER problems —.. the "NOW" moves too fast for years-long research...
*Shows like "Garthers' security & risk"
take the PIs to the market
*Advisory Boards
* Showcases
*Security conferences/ workshops
Host one
GETTING P.I.s BETTER INPUT/ COLLABORATION? with Industry
"NOW" PROBLEMS?
* M2M authentication
difference in nature between data & instructions
* I.o.T.
A Trojan Horse for platform integrity?
* Platform Integrity characterization
* Show security's link to business operations
* Improve the usability
* Networking training
* Treat data as a 1st class object
* Anonymization
* Policy
* Privacy
* Cyber-situational awareness
* Operating in a degraded mode
links to topics that go straight there
* Equip law enforcement
* Net-working events
* Elevator pitches
* Make this less of an attack surface
Wonder what this does?...
~multi-disciplinary approaches
* Legal analysis. safe harbor/ risk equation
how do you know where the line is.
B.

OPEN DISCUSSION, cont.


OPEN DISCUSSION continued~
HOW SHOULD WE BEST SPEND OUR TIME?
Connect PIs to Industry...
Influence solicitations...
Influence VPs of research...
Help PIs understand...
"Trio-ing"
P.I. + Proj. Mgr. + OEM
*Need to do-them all with a focus on PIs
*Influence pairing
teaming is long-lasting.
including small businesses
not just ☑ check-the-box!!
"Who on the team has a track record?"
part of their evaluation criteria
provide templates.
*Plant the seed of transition - but don't enforce it
*Online networking
& online dealbook
*Partner with the B-School
Legal Options?
*Clauses - eg Performance Improvement clauses.
How do we get good, real data?
and share it for reproducibility...
research. not student traffic
*Mutualistic relationships!
MMOG group
*Anonymization
re IRBs.
*Work to create the ecosystem
eliminate the roadblocks.
*Only fund what will be transferred
*Try it out on your university first
DOG
*Gather own own real-world data
*Reinforce success
fund those who have transferred before
force teaming:
those who've had success ↔ those who have potential
*Tech transfer offices
stimulate using metrics.
*Figure out how to pass the baton
so it lasts after you cycle out
*Require mentorship
*Infrastructure so that innovative proposals don't get shot down
14.

TAKE-AWAYS



TAKE-AWAYS

* We need to build the connective tissue (bring together disparate groups)

funders

* Many different forms of TTP!

* Expand beyond graduate student labor

* Future roadmap of security isn't clear

* P.Is → attend user conferences & report on it

* The value of analysts & product mgrs.

* Universities are major enablers & roadblocks

Involve B-schools/ collaborate

Icorps program

* May be multiple routes to TTP

profit

-non

* Leadership

* Right-size - find your place in the continuum of transition

NSF can educate VPs of research - workshop(s)

* Make TTP a key objective - incentivize

* NSF is looking to enhance collaboration w/ industry

Need:

open source

policy makers

existing companies

company creation

* A suite of TTP infrastructures/ ecosystems.

* Open Source isn't a one-size-fits-all

* Engaging industry advisors/ mentors

* "Athletics" model - reward the young, create a pipeline

developing

advanced

* Hold entities failing in security accountable for their failures

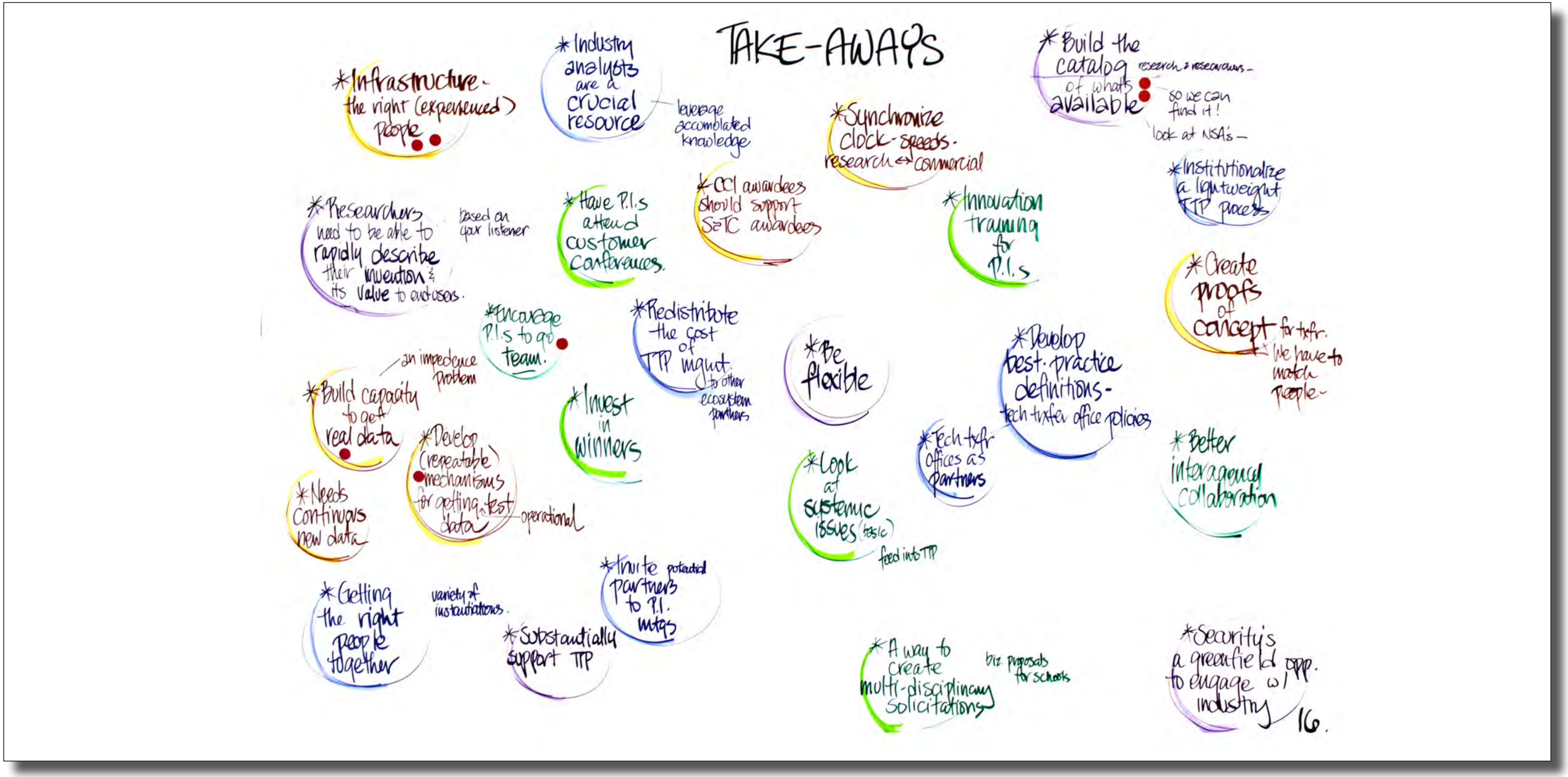
* What does peer review mean - in the TTP context?

* Interesting relationships - fundamental res. TTP & research cyber-infrastructure

* Comparitive metrics for the technology

15.

TAKE-AWAYS


TAKE-AWAYS
*Infrastructure - the right (experienced) people
*Industry analysts are a crucial resource
leverage accumolated knowledge
*Synchronize clock-speeds - research ↔ commercial
*Build the catalog of whats available
research & researchers -
so we can find it!
look at NSA's -
*Researchers need to be able to rapidly describe their invention & its value to end-users.
based on your listener
*Have P.I.s attend customer conferences.
*CCI awardees should support S&TC awardees
*Innovation training for P.I.s
*Institutionalize a lightweight TTP process
*Create proofs of concept for txfr.
We have to match people -
*Encourage P.I.s to go team.
*Redistribute the cost of TTP mgmt. to other ecosystem partners
*Be flexible
*Develop best-practice definitions - tech txfer office policies
an impedence problem
*Build capacity to get real data
*Develop (repeatable) mechanisms for getting test & operational data
*Invest in winners
*Tech txfr offices as partners
*Look at systemic issues (basic) feed into TTP
*Better interagency collaboration
*Needs continuous new data
*Getting the right people together
variety of instantiations.
*Substantially support TTP
*Invite potential partners to P.I. mtgs
*A way to create multi-disciplinary solicitations
biz. proposals for schools
*Security's a greenfield opp. to engage w/ industry
16.