All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

AI, Influence, and CyberSecurity - Oh My!

This is the article derived from a transcript of a practice run of my keynote presentation for the RSA Pitchforce event on April 29, 2025. Here we go:

The basic issue here is that we are, I believe, at a major inflection point in technology and society and so what we do now is going to influence the future for a long time to come. So the question is what do we want and how will we go about getting it, and obviously this is my perspective on that.

So when I say inflection points

- There are dramatic changes going on in our understanding of physiology and how it works all the way down at the molecular level up to the larger whole body mind issues.
- There's a great deal of understanding in cognology, that is cognitive systems, of people through things like functional MRIs for example, and so forth.
- A lot of sociological capacity. Unlike many years ago when there were a couple of newspapers and perhaps a couple of TV channels, we now have an enormous capacity to study and affect sociology across mass populations.
- Our computational capacity is continuing to expand to the point where we have enormous capacity to do things, way more than certainly I anticipated would continue under Moore's law, which should have ended some years ago except we kept developing new things.
- Content capacity is also growing. The amount of content we now have stored and available for use is something like the history of everything in humanity. It's pretty darn close with all the videos and all the written works essentially all available online.
- And then the ability to produce things with engineering is stunningly changing with the ability to do additive and subtractive manufacturing including nano-manufacturing and produce nano-mechanisms and so forth.
- And the issue is our willingness to proceed. Are we going to continue expanding all of these things at pace or to the extent that we can?

And what happens, of course, is a change in amount can produce a change in kind. And that's what we're starting to see. We're starting to see a change in kind that's reflective of the change in amount. We, now integrating across these things, there are all sorts of things we can think and do.

So, what do we want for our future? Star Trek or Star Wars.

If you look at the Star Wars picture on the upper left of the bottom corner, it's a planet destroyer, taking the beautiful green planet at the bottom left and turning it into the desolation, actually in the case of Star Wars, just a bunch of dust. Or do we want the Star Trek vision where we use our technology to destroy the planet killer, saving the planet?

To me, this is about truth or consequences.

I believe we can't build a desired future based on a foundation of lies and what we need is a trustworthy set of mechanisms, content, entities and people. And the question is how do we build that honest foundation? And I think it comes down in no small part to ...

Narratives

So let's talk about the dominant narratives that you see in the movies today and in the other means of communication are that evil wins most of the time.

Okay, basically crime pays. Occasionally the evil ones lose but then they get reconstituted. and this is also reflected in financial information. Evil turns out to be more valuable. the merchandising prices prove it.

I did a little study 2022-12. That's the starting name of the article at all.net. You can look these things in blue up if you like. And what's the favorite character from Star Wars? The action figure pricing is Boba Fett followed by Darth Vader followed by all the rest together being worth. Another site Java and the Emperor were the big winners. Next site, Camera, a TIE fighter, a blaster, five Stormtrooper helmets, and a Vader helmet. None of the good guys are worth anything in the merchandising market.

And this whole narrative that good wins in the end, whatever that is, or it's actually more like in the middle, it wins in the end for a moment and then lots of good guys die. The bad guys get rich, the good guys get poor, the hero almost dies but A lot of heroes of course die along the way. The hero finally wins. And then the bad guys return. So on average, it turns out bad is better in our current narratives. It's more successful.

Of course, reality is not the movies. Or maybe it is.

There are those that claim that perception is reality. And I'll just share a little story. When I was younger, I said, “maybe that's true." And I decided that I should be able to walk through walls if I truly believed it. So, I tried really hard to convince myself I could walk through walls, but what happened was I kept bumping my nose. So, I become convinced that perception is not reality.

It's all in your mind. That's the perception is reality viewpoint. There's no ground truth. It's just a point of view. And then we believe based on leaps of faith.

But my nose hurts

So perception may be wrong. There is an actual reality. You have to be careful how you interpret the things that you perceive. And don't just trust things, but test them. And so there's a methodology for getting at the truth in reality. It's called science. And here's how it works.

- You observe what you see and compare it to the theories that you currently have.
- If they disagree, you don't ignore what you learned. You propose new testable theories.
- You try to prove your theories wrong by testing them. And you keep doing that until you come up with theories you can't prove wrong by testing for a while.
- And you use the ones that you can't yet prove wrong.

- And continue to observe what you see and compare to the theories. And you keep looping on this.

And the idea is that, it's not that it's ever perfect. It's that things get better.

Errors and disinformation

I want to point out that error is not the same as disinformation.

People make mistakes. There's no getting around that in any future I see. And what science offers is a self-correcting approach. And what you see here are some examples of the common mistakes that people make. There's a great deal of psychological literature on this over many years. And these are just different kinds of mistakes that people make. But that's not the same as intentional lies.

Frauds are people that take advantage of people who believe their lies. And there's also a substantial literature on how to commit frauds. And here are examples of some of the common fraud techniques. And it's really important if you're going to, have a future here to recognize the difference between, frauds and mistakes. and so that's going to be a critical component.

John Henry for mental labor

There's another question here in this transition we're seeing in all these fields. the question is, what are people better at than computers anymore?

And computers are already better at sensing in almost any domain, acting that is things that they can do through automation, communicating almost anything you can name, I can communicate better and faster by a computer than person to person, and deciding well in some circumstances for defined decisions in short time frames computers are better at making decisions. People remain better at non well-defined and group decisions in longer time frames. So, we still have an edge. we're better at understanding situations and making decisions about what to do in time frames slower than a half a second. And some other things like, but not at building pitches or investing.

So this goes down to these fundamentals of the sense act communication and control or observe orient decide and act. These loops about decision making are things that computers now get better data for, in shorter time frames, and make and enact better decisions in shorter time frames for most cases.

So what we get as a result is cheaper influence. Computers are far faster at spreading information, including good or bad, just information. They're far cheaper at spreading information and they're better at many or most influence things. And you can see a picture here. This is a picture of how this works. It's a recent patent and earlier patent on automated influence. So, we have this capacity now and emerging to automate influence. and it's a two-edged sword.

So, let's talk about automated influence today

- We have psychometrics on individuals and there's theory about groups that you can also apply. And the technical details aside, essentially you can take information on people or information from people, do psychometrics, turn them into an analysis of different factors in their decision-making processes and their behaviors, and from that create a set of prompts for AI to do things.

- There are direct lines of communication, social media, email, text messages, voice and so forth that allow you to automate a lot of the communications.
- Psychological manipulation is pretty well understood which means that we can now take automated mechanisms for figuring out things about human psychology in the context of something we're trying to convince them of, produce a pitch on that, and then we can take these AI generated prompts on psychometrics and customize the pitch to the individual.

> *So automated convincing generation which takes cognitive computation and produces individualized minim manipulation in real time.*

So we basically automated cognitive attack, but of course it's a two-edged sword.

So what's the situation with cognitive automated defense today?

- For defending things we're really not allowed to use psychometrics on individuals. They won't let the cyber security folks use these techniques.
- There's little interference in direct lines of communications. You can put some interference on, some sensors and so forth in the way at corporate levels, but really social media, email, text messages, voice, and so forth are uninhibited.
- There's no psychological manipulation allowed for defense for the most part. So, you can get rid of that part of the automation.

So, what that means is there is no automated counter disinformation. so we don't have any automated counter measures.

In other words, cognitive defense sucks because it's blocked. We're basically decided not to do it.

It not it's that we can't. It's that we don't

And by the way, there's a lot of money in tricking people, especially when the legal blockades are gone. Many of the legal blockades that existed over time just aren't there anymore. So the question is, where's the money in honesty?

It turns out, it calls for long-term thinking and building trust relationships.

Fundamentally the money is in trustworthy mechanisms, content, people and entities. That is, building a trust architecture that allows us to figure out what we can reasonably trust, what relationships we have that can work and that we can rely on.

So trust here is both the problem and the solution.

So you have got to ask what it's good for.

Distrust is good for anarchy.

They'll call it democratization, but basically everybody has a so-called equal voice, but some are more equal than others, 1984, for those of you that know the reference, because they can artificially amplify their voices. All it takes is money, which the Supreme Court has decided we call speech.

> The response is more surveillance, of course. there's lots of bad things happening. We're moving towards anarchy, so we're going to increase surveillance to detect the bad things.
>
> > But of course history shows it doesn't do that at all. it does some of that depending on what you call bad but also it gets abused and that abuse ultimately can lead to autocracy.
> >
> > > So there's more surveillance leads to tighter control over what people are doing and what goes on, all in the name of security.
> > >
> > > > but security for whom?

Before AI was in place nobody could really watch it all.

This was, in World War II. the Germans had lots of records that they could do and lots of surveillance they could do of the underground. But, they couldn't really examine it all in real time as hard as they tried to do so. But that's no longer true.

AI is now at the point where basically it can watch all the communications that are going through all the digital media and a lot of personal communications that are under surveillance in one way or another and do the analysis.

So the 2025-03 article on how to destroy security by enhancing it might be interesting here.

So what is trust good for?

It turns out trust is pretty good for demonstrably trustworthy governance and institutions is what we would like to have. And this depends on things like time to transparency, being able to demonstrate honesty, fairness at all levels, and basically allowing the people at large to see and change it.

> And of course that's what is being fought against when you don't want democracy.

It's good for long-term success. You partner with people and mechanisms and content that you can count on so you don't waste your time worrying and planning for things that will not happen or, in other words, you get increased certainty which is to say less risk and more reward out of this trust mechanism if you can build one.

And of course you get happier healthier lives for more of us, advancement of knowledge towards enlightenment, and all the drama and fantasy you want when you want it, but not all the time. Thank you.

So sort of the underlying question is do you want to live in fear or in joy?

S → T + D = BO

So the situation is we have science that produces technology and when we add demand let's see what happens.

- We have cognitive science which is way over the utility threshold. We can use cognitive science for good or ill now and automate it largely.

- AI is yet over another utility threshold. We've constantly improved what was then called AI, which is now called technology, because the new stuff is called AI, until it's just technology. And it's certainly getting over this utility threshold for a lot of functions associated with influence operations.
- The unadressed cyber security demand is high enough to make some value out of it.

So we have the potential for explosive growth and that's here and now.

When you take science leading to technology plus demand that's equal to business opportunity. So the question is how do we take advantage of the opportunity?

I think the issue here is startups and early stage businesses and angel level and early stage investors. That gives us the AI influence confluence.

Did I mention what I do for a living?

I run Management Analytics and Angel to Exit and we do a variety of things. But it really comes down to helping people succeed.

- At management Analytics:
  - We have been trusted advisors since 1977
  - We do cyber-related research and advisory services
  - We do expert witness work
  - We have a patent portfolio in this area
  - We provide SaaS services for investors and startups
- At Angel to Exit:
  - We do advisory boards for equity and partially deferred compensation
  - We have investments in about 35 companies
  - We do metrics and due diligence at scale
  - We provide startup and investor support services

So what are the business opportunities?

There are lots of them. The critical thing is you want scalable ones. So here are some of the areas that are ripe today. It’s an incomplete list, but a good starting point.

- One of them is countering disinformation.
- Another one is trust architecture developing this on a large scale for enterprises and individuals and other organizations.
- Cognitive defense being able to defend against all these cognitive attacks.
- Intrusion detection and response is a cyber security term, but if we talk about influence detection and response that's the next wave of IDR
- Then there is deception for protection.

These are fields that already have technology that already have some companies that are starting, have started, or have been running for a period of time where they're really ready to scale and be successful.

And generally speaking, the confluence of AI and influence and security means we can use:

- AI for Influence
- AI for security
- Influence for security
- Influence for AI,
- Security for influence,
- Security for AI.

Oh My!

So what are my investment strategies here?

Basically I have three things that are at core.

- **One of them is to invest across the rising boats.** So I believe that these things you see above are among the rising boats, and there are other rising boats, and you want to invest across those rising boats and also in the IP that underlies them.
- **You need terms and supervision to reduce losses.** One of the big problems with early stage investment is most of the companies fail. But if you don't have a total loss when they fail, but only a partial loss, that pretty dramatically changes the statistics on success.
- **And then finally, the ability to do due diligence on the investments at scale.** And when I say due diligence, that means the level of diligence has to do with the amount that you're investing and the risk that you're taking relative to your portfolio. Being able to scale that is important to being able to apply this strategy.

I'd be happy to join forces with any of you to advance this, to understand more about it, and I am happy to take any of your questions.

Conclusions:

We are at major inflection points in technology and society, and what we do now will influence the future for a long time to come. The question we each must answer is what we want and how we will go about getting it.

My view is that we need to create opportunities for investments and innovation at the confluence of AI, Influence, and Cybersecurity to lead us way from anarchy and autocracy and toward democracy, honesty, and happier healthier lives.

We need to create the means by which trust can be properly attributed to mechanisms, content, people, and entities, because trust is the problem and the solution we need to succeed.

