

## All.Net Analyst Report and Newsletter

### Welcome to our Analyst Report and Newsletter

#### **Programs we should not allow**

It has become increasingly clear to me that legal restraints are going to be required to stop the research, development, production, and use of abusive algorithms. Like global treaties on nuclear, biological, and chemical (NBC) weapons, we need to do something to stem the tide of informational weapons or the human race will face catastrophic consequences.

#### **INBC**

Informational, Nuclear, Biological, and Chemical weapons are all capable and all have killed people. Arguably, informational weapons have been the root causes of the other three. How else do we get people to travel to foreign lands, meet new and interesting people, and kill them?

Of course informational weapons also work at home, arguably the reason that the right wing of the world (the haters – might makes right – love it or leave it – stop the foreign invasion – they look and smell different – they are the other – responsible for the bad things that happen to me and you) is thriving, is because of the increase development and deployment of informational weapons by the leadership of large nation-states and their minions, loyalists, and most importantly, their backers who prosper from the death and destruction it will yield.

#### **But free speech!**

Bull...oney. Frauds are illegal. Hate speech is illegal in many places. Inciting to riot. Conspiracy. Lots of ways you can commit crimes using only your speech – in person or online. But it's not just the pure shoving of bad ideas in repetition into the public discourse that creates this social havoc. It's also the abuse of technology to amplify and put flame to the fire.

Of course those who have spent the time to seek and understand what is going on in terms of social influence and political process, understand that the real change has been micro-targeting of large populations based on psychographics.

In some sense, it is completely reasonable that I should be able to sell one thing to you and something else to someone else. There is nothing inherently wrong about using technology for efficiency. Being efficient about convincing large numbers of people is also seemingly reasonable, even convincing each one of something different based on whatever information I may have about them. If it becomes extortion that is something else entirely, and if it is a fraud, again that's a crime regardless of how I communicate about it.

Eating a little bit of poppy seeds is fine. Eating a lot can kill you. The same is true of drinking water. No kidding – people have died from it – and I don't mean from drowning. The big question is: "When does it become poison vs. food?"

We want to feed our population lots of good healthy truthful information, but we don't want to poison them. Poison can come from unhealthy deceptive information, but also from too much selectively fed (or unbalanced) truthful, otherwise healthy information. It seems we need healthy information guidelines and a program of mental nutrition. It used to be called "school", but that was one of the first things attacked in the current cyberwar.

## The Radical [Religion] Terrorists

- There are no radical Islamic terrorists.
- There are no radical Christian terrorists.
- There are no radical [Religion] terrorists.

If you believe in the Koran or the Bible or any of their related religions or other major religions, you are almost certainly not a radical or a terrorist. If you harm other people under these guise, you are more likely one of these:

- A person taking advantage of other people for your personal gain.
- A person being taken advantage of for someone else's personal gain.

Religion is the mechanism of influence used to trick other people into ceding power to the leader(s). It's not that religion is bad. That's a different question and issue. It's that people who take advantage of religion for power and influence are bad. Because they don't believe – they cynically exploit others by using the belief system for personal gain.

- A supposed Christian leader who claims it is immoral for a Democrat to do something then tolerates it from a Republican is not a Christian and should not be given a tax exemption. And people of faith should not follow their teachings. Especially the teaching that says you should forgive them for leading you astray. Perhaps they should practice their religion rather than misleading it.
- A supposed Islamic leader who claims you will go to heaven by killing people is not Islamic and should not be tolerated as an Imam. People of faith should not follow their teachings. Especially the teachings that say you will be rewarded for killing other people or that you are doing Allah's work by carrying out a Fatwa. Perhaps they should practice their religion rather than misleading it.
- The same goes for any so-called religious leader who teaches hatred, killing, or that you should bend to their will (under the guise of calling it God's will). People of faith should not follow their teachings. People of faith should teach them the true faith.

But people do follow their teachings. Because people are fed information that supports that narrative and denied or taught to dispute and deny information that refutes it. In the language of deception...

## Induction and suppression of signals to produce desired behaviors in targets

The mechanisms of influence are and have long been clear and well known. They have been studied at length and in detail and we know how to exploit them. We now have the technology in place and being used by a sufficient portion of the World population to:

- Identify who is able to be convinced of a particular narrative
- Identify how to convince them as a function of information provided and prevented
- Create the information to present and implement means to prevent (focus of attention)
- Deliver the information to convince and suppress belief in and attention to alternatives
- Get feedback on the deception by observing behaviors and loop

## What is being done today

The big money is in sales and marketing.

- Advertisements in existing cell phones are designed to user personal information gleaned over time to identify people who can be convinced (to buy something)
- They use psychological and behavioral histories to identify how to convince people to make decisions (buy things).
- They create information designed to get mindshare – specifically by getting focus of attention and time of the user (to entertain and reward them via discounts).
- They deliver information to convince and suppress opportunities for alternatives (by signaling hunger when near an advertising restaurant and offering discounts).
- They get feedback on the deception by observing behaviors and looping (they watch eye movement, motion, location, button pushes, sounds, and other things sensed and use these to association micro-behaviors with macro-behaviors (buying)).

But of course it can be applied to bring about all sorts of changes. Like political views, hatred, love, fear, action, inaction, obesity, fitness, and on and on.

This is existing technology being used systematically in large scale to influence buying decisions and other behaviors.

It is being exploited to an increasing degree for political change and influence operations designed to break up national political cohesion – picking apart the body politic.

### I think it's a question of quality – and persistence – and stopping it before it grows

The slippery slope we are currently sliding down at a blistering pace is rapidly coming to be a torrent of deception (and psychological / sociological influence) going over a waterfall carrying society with it. A little bit of anarchy is probably good for the soul, but there comes a point when people get killed for sitting in the park because some idiot decided they are “other”.

There are plenty of lies in the world, and I am not suggesting we make them all illegal. I am in favor of humor, and I sometimes tell people positive things about themselves when I don't feel it deep inside. That is not the problem. The main problems are:

- High fidelity, individually targeted, high volume, amplification, and strong feedback on the use of instantiations of memes.
- The inability of targeted individuals and, at larger scale, institutions of democracy, to rapidly and easily discern authentic reliable information from deception.
- The exploitation of the collection and analysis of detailed information from many people for one purpose (e.g., helping them in some way) for different purposes (exploiting them).

### An example of the tradeoff I just encountered

Here's a great example I just encountered. What looks like an outstanding program for checking and improving grammar in my writings (and yours) installs in your Web browser and other applications, and helps you improve in real time. It would probably have made this article 25% smaller and far easier to read.

The problem is that in order for this to work, they send everything I type into my browser to their cloud-based system for the analysis. I don't know if they are really fine people doing a great thing for all of us, and I tend to believe that they are sincere. They have a policy that I haven't read, but it probably says they will never share anything of mine with anyone unless they need to do it to make the service work. And they may be sincere indeed. They may even have a system that immediately throws everything they collect out as soon as they do the analysis of it (although I doubt it because that would not likely be as good for the quality of their service). They may anonymize it, but countering this is likely trivial as soon as my texts appear on the Internet and can be correlated to the anonymized versions. All those technical solutions will ultimately fail under serious threat actor attacks.

But the technical limitations are not likely the big problem here. The bigger problem is that if I want to get access to this data (when they grow large enough to make it worth exploiting), all I need to do is help them succeed by buying them. These fantastic startups that are making the world a better place get bought or taken over or an insider or two are bribed or extorted, or the same happens to their service providers, and without any computer break-ins, the great company helping the world can be turned into a weapon of cyber warfare. Something about the road to hell being paved with good intentions should go here...

### **It's about control over content**

Do I want my inner thoughts as expressed in my initial draft writings sent out to 3<sup>rd</sup> parties over which I have no control? What if I had control? How do I get control back into the hands of the owners?

The easy technical way to change all of this is to not allow "personal data" (bad name for it) out of the local environment. Instead of me sending you my data, you send me your program. The program does analysis here and produces the answers here that help me and you don't get any of my data. But then the service will not be able to improve as well over time and the business model of them selling my data or the use of it to 3<sup>rd</sup> parties goes away. They could charge me for the use of their software or even have a freemium or recurring revenue model, but then I would actually have to pay for what I get directly instead of indirectly, and the "free" part of the Internet would go away, increasing the friction on transactions, and reducing the economic utility of the Internet.

There is a middle ground, where the research uses test subjects who know exactly what is going on, or uses published works for analysis rather than watching the users as they type. The published work analysis could be used to inform and update the software on the end-user platform and keep it improving. Wow – seems like it could work! But will the folks doing this be willing to tolerate this approach, will the end users actually pay for it, and will the competitors using the more exploitative approach win in the marketplace?

### **Quick observation**

Not to break the flow here, but the solution to a marketplace forcing the players who want to do it in the best interest of the public and individual freedom to lose, is regulation. I am not a fan of regulation, but at the end of the day, bad people seeking money can really only be countered by legal restrictions and punishments. Unless of course we could get benevolent people to buy all these companies and assure over time that they stay good. But of course, that would depend on people being good, and we know that cannot be assured reliably.

## Deception is the heart of the issue

At the heart of the matter is the issue of deception. Not the little deceptions of saying you would be happy to have anything for dinner when you probably would prefer one thing or another. It's the big deceptions that affect society as a whole.

Note I used the term affect in that last sentence. I almost always prefer talking about effects because that's what causes produce through mechanisms. But in the case of deception in the large, it's more about affect. Affect is about the feelings people have. It's about influence, not about the directly provable easy stuff of hard science. Rather, it's about the hard stuff of soft science. People who have felt the affect of excessively nationalistic influence are unable or unlikely to change their minds based on fact. At least not a few facts spread among the many lies they see daily. They are influenced by their friends and family, their lives and history, the way people talk to them or at them or over them, and their pre-loaded beliefs.

A far more subtle form of deception lies in telling the truth selectively. Of course if you go to lies, that is over the line, but what about focus of attention? The way people think is limited by their focus of attention. When paying attention to one thing, they miss something else. By controlling attention, even if you only make truthful statements, you can dramatically influence others.

- For example, if we focus on Trump's asserted criminality, even without the actual evidence in front of people, they will come to the conclusion he is a criminal. But in fact, such a determination is normally made by courts of law based on evidence.

Of course this is not perfect in any way shape or form, among other reasons because lawyers study the psychology of jurors and seek to influence them. But there are two sides who get to play that game against each other, in the American system. In other systems it is done differently...

- On the other hand, if we focus on Hillary's asserted criminality, and the claim that the criminals are accusing us (the good guys) of what she did and making it all up, even without any actual evidence in front of people, they will come to the conclusion she is a criminal. Again, ignoring the normal process.

The court of public opinion influence causes beliefs that are often false, and years later, people who held these beliefs realize they were fooled, but may still not admit it. That is what happened in Nazi Germany and there is plenty of social science to back that up.

History is written by the victors. And as new victors come they tend to rewrite the rewriting.

## Come the archives and records managers

One of the reasons I like folks in the archives and records management business is that they focus on identifying, collecting, preserving, and making available, records. Their focus is on reliable and authentic records. The general idea is that these records reflect a reality supported by contemporary evidence accurately recorded and properly preserved so as to be usable in context at a later date.

They long have been, are, and will continue to work on ways in which accurate and reliable records of what took place can be transmitted over time and space so as to be received and perceived as reflective of that original meaning that created them. Which brings us to their role in the process and the legal (a.k.a., juridical) issues and context of their existence.

The ARM profession exists in every country, every state, many businesses, and is generally mandated for every legal entity that exists. This has long been true and will hopefully long continue to be true. The custodians of records exist de-facto even if not specifically defined, and the profession of diplomatics, whether physical or digital, is a means by which analysis of records may be performed to determine their reliability and accuracy. But these institutions and notions are being challenged today as never before. Strangely, it is the very neutrality of their position and desire for reliable accurate records that is creating these challenges, along with the race to take advantage of the new digital age.

### The research solution

You might imagine that research into counter-deception would be a high priority, done at a high volume, and of great academic interest. It's not.

The vast majority of research in this area is focused on how to achieve deception, the error modes in human cognition, how to exploit them, and how to make money or gain power by exploiting these things.

This is unlikely to change for the foreseeable future. Why?

### So what should be illegal?

My view is pretty simple to say, but not that simple to do. I think it should be illegal to use computer systems to artificially amplify your influence, to lie using technical means in a way that makes it very hard or infeasible to discern the lie of what you express, or to perpetrate the various crimes that are already illegal using technology as an instrument of the crime in such a way to avoid some legal limitation.

- **Amplify your influence artificially:** Amplification I have written about before. In essence, the use of technology to artificially create more accounts, more apparent identities, more messages, larger or better connected groups, higher ratings, or anything else that increases your influence other than through your personal direct effort (obviously using computers as the mechanism, but expressing your own thoughts and views) should be prohibited and made illegal. Yes – illegal. And to be clear, money is not speech and companies are not people.
- **Technical deceptions hard to detect:** Detection of deception is often easier than you might think, and that's a good thing. But if the research and development folks spend enough time making it harder and harder to tell the difference, they provide no benefit to the legitimate (honest) use for humor, satire, political commentary, or anything else. Making deceptions hard to detect serves only one purpose. Taking advantage of others. It should be stopped by legitimate researchers, not accepted by internal review boards, not funded by governments... Except of course that governments view this is a potentially necessary element of information warfare. Disinformation. Which means we need a global treaty on information armaments that includes the use of deception.
- **Avoid other laws via technology:** I don't know of many cases where this is done, but I am against it anyway. Technology has long been used to avoid laws, for example, by crossing jurisdictional lines to commit crimes. Laws are catching up, for example, in California, anything that potentially harms a California resident is subject to some of their laws. If they can catch you and get you extradited. In general, a law should be

passed that makes it a worse crime to commit any other crime through the use of technology. This also goes to changes in the laws regarding statutes of limitations.

These statutes were originally put in place because evidence reliability decreased with time. But digital evidence may not have this same property. As a result, a change that allows older crimes to be prosecuted based on older evidence with the requirement that the evidence be shown to be reliable to the same standard as current evidence (which is inherent in the current standard anyway), would prevent the use of delay tactics and obfuscation from holding off information “long enough” to escape the law by these methods.

- **Use of psychological factors:** Of course we all interact with each other, and some smart folks know how to take advantage of the psychological factors they encounter in others. They were historically called con artists, but increasingly they are called data scientists. Some con artists and data scientists are very fine people, I assume. But as we move toward finer grain and real-time detection of micro facial movement and sound detection and analysis, we really need to make it illegal to do this level of analysis in a feedback loop to cause people to do what we will. It starts with advertising, and the claim it is for good (help you find just what you are looking for). But in reality, it is being used to cause you to buy something that you would not otherwise have bought, pay more for less, what have you, eventually, by some and then more, and then many of the users. And the politicians will rig your phone so they detect the feedback in real time from your accesses to information and provide you with the right feeds to cause you to vote for them. And 1984 will be here in 2024 (or so).
- **Anything disrupting proper archival and management or reliable authentic records:** Of course public records and records of legal transactions of all sorts should be a very high priority in protection. Clearly it should be illegal to forge or otherwise alter public records... Actually not. Records ultimately have to be transferred from system to system and lose some aspects of their utility unless reworked to the new systems and mechanisms of use. Crumbling paper is not identically copied when scanned or reprinted or copied. Archival science addresses this, and thus its the reliability and authenticity of these records that must be retained, and it must be illegal to do anything that knowingly or intentionally causes these records to lose or reduce reliability or authenticity.

### But what if we cannot get the laws to change?

Extra-legal means are things I do not generally support. But on the other hand, “When in the Course of human events, it becomes necessary ...”<sup>1</sup> and of course “self defense may be used to argue that the defendant’s use of violence or deadly force were necessary to protect himself or others from harm. The rationale behind this criminal defense is that people should have the right to protect themselves, their loved ones, and their fellow citizens from physical harm.”<sup>2</sup> The so called “2nd amendment remedies” we hear about from the right wing of the US. Of course these remedies are available to all who feel that it has come to that point.

The history of this arena includes some pretty disgusting attempts at remedies.

---

1 The US Declaration of Independence

2 <https://www.upcounsel.com/lectl-self-defense-in-criminal-law-criminal-defense>

- The sorts of folks who bring the “information needs to be free” thing to bear in defense of Julian Assange,
  - They don’t even understand that they are under or part of an influence campaign to exploit the information for private gain against their own interests and beliefs.
- The anarchists who have never lived in anarchy and imagine it as freedom rather than oppression,
  - They don’t understand that anarchy means people killing each other with no recourse other than more violence and destruction.
- The communist idealists who fail to recognize the tendency for all such forms to become autocracies,
  - They don’t get it that the ideal commune only works with ideal people, and not even they are such ideal people.
- The pure democracy folks who do not fear the tyranny of the majority until they are in the minority,
  - They somehow think that instant decisions by millions of ignorant people are better than what they have now, and further imagine that these millions of people will somehow become educated in the pure democracy.
- The capitalists who imagine that if the rich folks go to an island the rest of us will have a failed society,
  - Ayn Rand told a good story, but who really believes that the rich elite will do the maintenance on their own toilets while the great unwashed masses with their engineers and scientists will not be able to make their way in the world?
- The assassination politics folks who suggest that they are not responsible for the death of the people they put on the target list,
  - So if I list the Republican leadership and you go kill them, and someone else lists the democratic leadership and someone else goes and kills them, do you really believe we will all be better off?
- The peace at any price folks who say violence is never the answer.
  - Gandhi was a great man, but he was fighting an information war against the British who prided themselves on being ethical and moral and following a legal system. Does anyone believe this would have worked against Stalin? Hitler?

If we want to change this and the normal methods do not work, we must work within and along side the systems that exist to make change, using methods like protests, laws from other venues, civil actions, and similar sorts of methods, until public sentiment gets to the point where politicians are compelled to act.

## Conclusions

There are things that laws can address, and there are things that they cannot. But without the force of law, we will continue toward anarchy and likely worsen the problem until the very fabric of governance disappears. We need international treaties for control of information weapons just as we need them for nuclear, chemical, and biological weapons. But of course we need to balance these against the freedom of expression and political advocacy. We are still at the beginning of the cyber age, and have a ways to go. But we best start working on this issue or we will find ourselves enslaved by the prison of our minds, secured by the bars of the very technology that could set us free.