

All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Watching the Influence War

It's happening right in front of us and there seems so little we can do about it. Day after day, the influence war is being played out in the private and public spheres as corrupt forces disable the means of disinformation detection and countermeasures. While defenses are being disrupted as the US elections approach, the offensive weapons are brought online with increasing financial backing and positional advantages. But it's not just the US that is at war and effected. I just happen to live here, but global information warfare effects almost all of us.¹

Destroy the defenses

In the last few weeks we have seen the power applied, and it does not look good for those who wish truth and honesty were at the heart of our societies.

- The Stanford Internet Observatory election misinformation detection function was terminated, not that they were all that effective in the first place. But they were well known and considered a bellwether for educational institutions.
- The destruction of the counter-disinformation teams in social media companies has been coming for quite a while. Twitter → now X was among the most obvious and radical examples. But Facebook has always been on this bent and is famously the initial target of Russian intelligence in the 2016 US election cycle. They are particularly easy because they have a long-term bent away from privacy and toward exploitation. LinkedIn has increasingly become a channel for deception delivery and exploitation of other sorts, this really starting with the acquisition by Microsoft.
- The emerging generative AI companies have so-called safety teams but they were never even a little bit effective against any level of bypass attempts, and today they are at the ridiculous point. If you ask them who the US president is, for example, while search engines will produce the expected result, the AI engines seem unable to address the issue. Indeed anything factual is at odds with generative AI... that's just not how they work. But worry not, these teams have largely been reduced, apparently because of the desire to use AI to solve the problem over people.
- The disinformation warnings that were once, briefly, part of the effort of US government agencies to counter election interference efforts have, apparently, largely been destroyed by the political factions wishing to retain freedom of lies... only called speech in this context. Freedom of speech is apparently a license to lie, but fraud is still a crime, as long as you are not a politician... and sometimes even then!
- Presidential immunity in the US now applies in an absolute sense to any act that is within the exclusive scope of the President of the United States. And that means that power to destroy opposition is not enabled. The legal defenses against disinformation for political leadership is now completely gone. The US has historically used disinformation in its intelligence operations, as have most other nation states, but the

¹ About 6.5 Billion of the 8 billion people alive today have Internet access in one for or another, and nobody else can read this. So if you are one of 'us', you are likely affected.

removal of all restraint on Presidential power is clearly problematic given the bent in this direction of the extremes of political parties.

- There are various small efforts to understand and counter disinformation, but the funding sources that you would imagine might be behind seeking the truth have increasingly abandoned that approach in favor of funding their 'side'.

The factions

There are two major nation-state coalitions in today's global game; the autocracies and the democracies.

- On the autocratic side, we have Russia, China, North Korea, Iran, and various despotic leaders around the globe.
- On the democratic side, we have most of the European Union, Canada, Australia, New Zealand, and some other nation states around the world.
- In the middle and possibly transitioning, we have the rest.

There are also two major religions fighting it out; radical Islamists and Christians

- The radical Islamist extremists (not the largely peaceful Muslims)
- The radical Christian nationalists (not the largely peaceful rest of the Christians)
- In the middle we have the rest of us, and for now the Jews as the focus, as usual.

I feel like this is the place for a Tom Lehrer song.²

Build the offense

Of course when Musk bought Twitter and turned it into X, we all knew what we now see was the likely result. But that's just the tip of the iceberg. News media, Art, Film, Radio, ...

- Steve Bannon is widely quoted as being happy when he left government because "I've got my hands back on my weapons".³ He is now in jail, but only for 4 months, and only for refusing to obey a subpoena. His disinformation campaigns are still with us.
- Sinclair radio network has been pushing out hundreds of stories per week to its hundreds of local trusted news affiliates about Biden having cognitive problems, all based on stories created by Republican politicians. But since then, Biden did himself a real disservice by his June debate debacle. At this point, all the preparatory disinformation has been justified, turning it from propaganda into clairvoyance.
- Palestinians are generating floods of false claims about 'Palestine' being a country occupied by Jews, including false images, produced short films showing people dying when they are still alive, false depictions and headlines for images showing Palestinians living where Israel is today for thousands of years. Of course there is no actual historical group called Palestinians, it was invented in the last 75 years and relates to historical facts that did not involve the same people now being pushed as Palestinians.

² <https://www.youtube.com/watch?v=allJ8ZCs4jY>

³ <https://www.theguardian.com/us-news/2017/aug/18/steve-bannon-returns-breitbart-donald-trump>

- Fox News, the Wall Street Journal, and other outlets owned by Rupert Murdoch are pushing out false narratives, even after Fox News settled a law suit about the same behaviors for somewhere just over \$787M.
- Russia is pushing narratives asserting it will use nuclear weapons if (name the event), and while repetition in this case causes a loss of credibility, nobody in a responsible position can truly ignore such threats. But Russian internal and external disinformation is one of their longest standing strong areas of military/political operations.
- The disinformation of Wikipedia has again emerged as the social encyclopedia suffering from the tragedy of the commons. Garbage history was always an issue, but the disinformation campaigns underway today replace what is often considered an initial basis for encyclopedic information with pure propaganda. Of particular focus is the attack on history related to the conflict in the Middle East.
- Generative AI has long been the subject of speculation and experimentation producing demonstration samples and theoretical calculations, but it has recently reached the point where it is a viable offensive weapon in the disinformation world. Left to its own devices, it is a powerful tool for misinformation. But when directed toward intentional deception, it becomes automation to support customization of disinformation to each of us, backups up by other deceptions and written in prose that makes it all the more believable. Or to restate it using AI (ChatGPT in this case):

Generative AI, once a topic of speculation and experimentation generating demo samples and theoretical calculations, has now advanced to the stage where it functions as a practical offensive weapon in the realm of disinformation. When operating independently, it serves as a potent tool for spreading misinformation. However, when purposefully directed towards deliberate deception, it automates the process of tailoring disinformation to individual targets, reinforced by additional falsehoods and presented in prose that enhances its credibility.

Follow the money

Notice where the money is being put and pulled from. It's offense all the way. And a lie can go half way around the world (in all directions) before the truth can get its pants on.⁴ So there is a natural advantage to the well constructed lie over the truth, and the money is behind the lies over the truth. One of the suggested strategies is to merely flood the field with as much on your side as you can come up with, and don't worry about the truth.

Nowhere to hide, nowhere to go

Which leaves the rest of us SOL⁵ Us individuals can only read and hear what comes to us in written, video, and audio forms. And the domination of the offense means that we cannot get at the truth unless we try very hard to seek it out. The artificial amplification produces errors of omission cause by focus of attention, and the media companies amplify this by their algorithms which generate more money from following (and creating) popularity.

4 Winston Churchill "A lie gets halfway around the world before the truth has a chance to get its pants on." but also, historically from as far back as 1787 sermons by Thomas Francklin, has also been attributed to Mark Twain, also 1821, 1834, 1835, etc. per <https://quoteinvestigator.com/2014/07/13/truth/>

5 Sh*t Out of Luck

A classic example is conflicts around the world wrecking havoc, killing people, starving people, enslaving people, destroying all manner of resources and infrastructure, all largely ignored over concerns about less than a quarter of a tenth of a percent of the World population, and actual deaths of less than 1% of the deaths generated over the same period by other conflicts.

Which brings me to another Tom Lehrer song...⁶

What do we need?

More transparency in less time, more information better filtered, and less control by the few. Sure – these things will help. But as we enter the high intensity part of the information war, an underground will need to be created in order to ever return from the brink.

Why is that?

If Germany in WW2 had the intelligence capability of unlimited video, audio, and written communication surveillance, the underground that was so critical to the Allies defeating the Axis would never have been able to persist. Rather than the paper system of record-keeping and manual processes with the ability to hide from surveillance and search, today we have the technical ability to listen to nearly everything, see through walls, listen at distance and through almost all barriers, detect digging, heat signatures, power usage, signaling, air usage, and on and on and on. These are all small enough to readily hide, deliverable by unmanned vehicles in near silence, long-term recording and rebroadcast when desired, and we now have the ability to fuse and analyze all of this data in near real time.

The new underground

The new technical underground capacity required to defend against autocratic governments and effectively operate the criminal enterprise which is a resistance against the autocrats in power cannot likely be developed after the autocrats have solidified their mechanisms. Rather it should be thought up in advance and prepared for. So what is the starting point? Here are some parameters:

- We need ‘clean hardware’ that lacks embedded surveillance and tracking, and it has to be reasonably portable and covert.
 - *This starts with old tech. Buy older laptops that don't have the embedded ‘security’ capabilities or the new complex chips with the newer embedded Trojan horses. Buy radios and learn how to use them. Short wave is pretty good, but very important is the ability to create ad-hoc infrastructure that takes many hops and can be readily placed and left to be wherever it is. Place them never to return, locally powered, no writable storage, remotely turned on and self turned off. With detection and self disablement. Cheap, simple, and easy to place covertly. Multiple channels that change rapidly with time in hard-to-predict patterns.*
- We need reasonably safe operating environments that can reasonably defend themselves against remote assault.
 - *That means some of the older cleaner versions of Minix, Linux, and similar open source versions built with limited capabilities, booted from ROMs to run from RAM.*

⁶ <https://www.youtube.com/watch?v=TloBrob3bjI>

- We need the ability to conceal these capabilities from surveillance during limited periods of time when they are used for covert communications.
 - *We need to use strong steganography based on reasonably strong encryption algorithms and embedded into widespread and publicly usable communications, hopefully planted as Trojan horses within all manner of code.*

Or alternatively, we could learn to operate safely over new technology using non-connected technology to translate, encode, encrypt, etc. and connected technology to transmit and receive covertly using mass communications channels. Think mass volume AI-generated content infused with steganographic content that itself is compressed then encrypted prior to insertion.

Anonymous networks

Of course the problem with any such system is that it relies on a trust architecture that doesn't really exist. How do people get into these groups, how do these groups protect themselves while still growing, how do they reform when disrupted, how do they disburse when detected, and how do they do this when the participants are naive? Don't imagine that this was done successfully with Q. Plenty of folks knew who Q was and this has been widely revealed. But Q was not operating with a government using heavy surveillance to defeat it. Forget about the notions of free speech, law enforcement limits on surveillance, search, and censure, torture, extortion, kidnapping, and all the niceties. The network must be self-healing, self-generating, self-anonymizing, and so forth.

Ready, set, go... Ah... we don't really have a way to do this yet... Better get started.

Where do we look to get started?

Where we have always looked for breakthroughs in this arena... Pornography and Crime.

Yes, if you look at history, pornography has persisted despite all attempts to disrupt it. It has advanced with technology, always a step ahead of those who try to stop it. One reason is that lots of folks want it even when they say they don't. So they do it as do the corrupt government officials and the religious leaders and so on and so forth.

Crime has always had to evolve to get away with things when law enforcement chases them, and law enforcement is always behind crime, among other reasons because things aren't made illegal till they are discovered and made illegal. But the other reason is that law enforcement tends to be underfunded and ill-prepared for large distributed crime networks where they don't care to follow the rules of societies. Autocracies and similar forms of government are often inherently criminal in that insiders take advantage of privilege based on who they are. In helping them take advantage, they are easily taken advantage of, because when they get caught they get killed like the rest of us, not for the crimes, but for disloyalty.

Conclusions

The war that started in the early 2000s⁷ is near the end of the beginning. To defend against the coming capabilities of nefarious governments we need to act today to defend the new resistance. It's too late to wait and soon it will be too late to hide. Be prepared! Start your pornographic and criminal enterprises today and become well established with elites!

⁷ <http://all.net/books/lwar.pdf>