

Linguistic/Behavioural/Sentiment/ Astro-Psychological Analysis and Its Attribution To (Cyber/Insider) Attacks: There Is a Story/Meaning (To Be Analysed In 3D View) Behind Every Action, Reaction, Creation, And Destruction...

Kavinmuhil S.K.

Senior Cyber security consultant, EY, Astro-psychology enthusiast.

Abstract:

Negative sentiments, words to express negative emotions, linguistic analysis, behaviour, planetary positions reckoned on a day, all these factors establish a correlation with each other and follow some patterns, which could be used in creating warnings or alerts to organization or could be applied in digital forensic cyber analysis and cybercrime investigations, enhance the existing behaviour analysis pattern in digital forensic analysis through improved machine learning where monitoring the employee or insiders communications closely with the captured email and chat logs and situations beforehand, which would reduce the risk of some unplanned or unexpected (insider) cyber-attacks. Malicious insider, an angry employee is often overlooked when it comes to organization cyber security planning which is highlighted in this article.

Keywords: Negative sentiments | Sentiment analysis | Linguistic analysis | Cyber threats | Organization cyber-security planning | Astro-psychology | Negative Sentiment scale | Email/chat monitoring | Negative emotions | Insider threat | Digital forensics

Introduction:

Psychology has been considered a part to be unified into digital forensics because of the need to look closely into the motivations of cybercriminals. With psychology and digital forensics, businesses could gain insight into how, why, and where cybercriminals hack their systems. Furthermore, a business can better protect its resources through the psychological understanding of its people, learning where the internal vulnerabilities are present (Insider threat). Digital forensics deals with the collection, examination, and analysis of the evidence of cybercrime and the presentation of that evidence in the court of law. Cyber forensics aims to the collection, well chain documentation of the pieces of evidence that is collected. Digital forensic analysts follow a protocol to collect evidence. They physically seclude the affected device and make a digital copy of that device. After copying the device, the analyst will seal the entire device for further analysis. Using different Forensic tools analyst will check the device and recovered files.

Planetary position and impact on human thinking:

Planetary positions, especially moon, mercury and nodes of moon and its placement, movement has deeper impact in human psychology. Hence in digital forensics field, analysts should consider including the planetary position analysis to confirm if the person, on that day would have committed the mistake. The level of accuracy in deriving the outcome of investigation is high when including the Astro-psychological analysis. Therefore, in addition to considering the linguistic, behaviour analysis of cybercriminal case investigation, adding Astro-psychological intuitions to it gives more precision in analysis. We make reckless, bad decisions when planetary natural moon and mercury positions are afflicted, moon in natural 3,6,8, in the house of Gemini, Scorpio, Virgo and mostly conjunct or aspect by Moon's north node, Rahu. Our communications and actions are attuned with negativity and our excogitation is affected during this stretch of time, where moon and mercury are troubled and is not comfortable and this pattern could be utilized in analysing the sentiments of employees in an organization as is important in an organization to monitor the negative sentiments, especially these days, that could otherwise lead to potential insider threats.

Negative emotions in Linguistic analysis:

Some of the common ways that human being tries to manage or express the negative emotions include:

Denial/Suppression: When people deny that they have problematic feelings, that ends up some day exploding or acting out in harmful ways. The Negative Sentiment Scale (NSS) in expressing the emotions through language and by the average level of normal human speech or language perception is initially low in Denial but could be 'Very-high' in the long run. Example: 'I'm not sad', 'It's okay, I will take care'

Sounding tired/ bored/ uninterested: When people at work get too tired/ exhausted/ drained/ burned-out/ worn-out, they express that by sounding very low. The NSS is mostly low in this case.

Example: 'Can't work anymore'

Feeling embarrassed/Ashamed/ guilty/ remorseful: NSS is High to Very High in this case.

Example: 'I'm feeling embarrassed to show my face at work'

Jealous/ envious: NSS is Medium to High in this case.

Example: 'He has that', 'I want it'

Sad/down/depressed/unhappy/Sullen: NSS could be from Medium to High in this case.

Example: 'Feeling sulky', 'I'm not in good mood today', 'I'm feeling depressed', 'feeling down', 'I'm feeling lonely these days'

Anxious/ Nervous/ Stressed/ Scared/ Unsettled/ Apprehensive: NSS is Low in this case. It can be easily handled by dealing over the phone.

Example: 'you don't know why', 'I can't, I'm scared', 'I'm nervous'

- **Implied criticism/ negativity:** NSS could be unpredictable here Example: 'I have given my best', 'Wow! Good try!', 'Better luck next time'

- **Provocations:** NSS could be high Example: 'I dare you'

- **Objectifying, sexual, religious, racial content/ using curse, foul language:** NSS could be very high
- **Personal appeal/ plea:** NSS is low here in most case

Example: ‘Please’, ‘Listen to me’

- **Angry/ Furious/ Pissed/ Annoyed:** NSS could be high in this case.

Example: ‘I’m at wit’s end’, ‘I’m going to be very cross with you’, ‘Grrrr’

Correlation #1:

Consider **Hansen Evan’s case**, that happened on 13th July 2011, ‘Manning-Lamo Chat logs revealed’. From Hansen’s email communication excerpt taken during the period he was accused of leaking materials to Wikileaks,

‘i can’t believe what I’m confessing to you :’(I’ve been so isolated so long... I just wanted to be nice, and live a normal life... but events kept forcing me to figure out ways to survive... smart enough to know what’s going on, but helpless to do anything...’ - shows words of a desolate soul, showing a very high level of NSS.

Position of moon(mind, thoughts, cognition) calculated on 13th July 2011 was debilitated in Scorpio- 29 degrees at Jyeshtha nakshatra conjunct North node rahu(28 degrees in Jyeshtha nakshatra), mercury in cancer(Moon- Mercury’s natural enemy) in Ashlesha nakshatra, displays high level of depression. Sun and Venus in the house of Gemini, the natural house of communication that revealed the secret.

BASIC	LAGNA	NAVAMSHA	MOON	C
Ur*	Ju	Ke* Ma	Ve^ La Su	
Ne*			Me	
Pl*	Ra* Mo		Sa	

* Retrograde ^ Combust

La 02°50'14"	Su 26°21'30"	Mo 29°04'50"
Ma 21°26'52"	Me 22°00'57"	Ju 12°44'15"
Ve 16°53'48"	Sa 17°07'52"	Ra 28°03'19"
Ke 28°03'19"	Ur 10°38'06"	Ne 06°25'35"
Pl 11°40'08"		

Therefore, the idea is to configure an alert in emails, chat data monitoring tool of an organization when an employee is expressing emotions with high NSS, provide immediate counselling and trying to handle the case internally, within the organization, to avoid any risk that would happen in future.

Correlation #2:

Anthrax attack:

According to a linguistic and behavioural analysis report of the FBI, on anthrax letters dated 18th September 2001 and 9th October 2001, all the three letters were authored by the same person. The anthrax used in the letters was disbursed differently in each letter, showing inconsistency. He tried to identify the correct target address of the victims and used sufficient postage to ensure proper delivery. Other characteristic traits of an attacker include- Secretive, non-confronting in public, prefers being lonely, comfortable to travel only in his locale, organized, rational, Knowledgeable, withdrawn, less confident. The NSSL was very high noticeably. Capitalized letters throughout shows the author is wanting attention, a level of attention deficiency is seen.

There are ways of expressing anger, negative sentiments, discontentment through writing. Some will express in a regular, even toned manner, at times frequently and will be able to verbalize their emotions well. The risk level of this sentiment is less when compared to anger or negative sentiment expressed through carefully planned and articulated, less expressive toned communication.

This is an example of the latter way of expressing anger and negative sentiment.

'YOU CAN NOT STOP US, YOU DIE NOW, ARE YOU AFRAID? DEATH TO AMERICA, DEATH TO ISRAEL, ALLAH IS GREAT' - Shows aggression and anger, and the NSS level is Very-high.

Natal chart of the person should have resemblance to the astrological chart that is reckoned at the time of the attack, 18th Sep 2001, the date when the letter was posted and death of first anthrax victim noticed.

Position of the moon, mercury, and sun(1 degree, showing less confidence level to confront or act in public) is in Virgo, the natural 6th house, house of science, medicines, medical science, details, organized and rational thinking, and communication. Mercury in Chitra nakshatra, whose ruler is mars, and which is mercury's natural enemy, exhibits harshness in communication. Jupiter and Rahu in Gemini, Arda nakshatra.

BASIC	LAGNA	NAVAMSHA	MOON	C
		Sa	Ra* Ju	
Ne* Ur*			Ve	
Ke* Ma	PI	La	Mo^ Su	Me

* Retrograde	^ Combust	
La 13°58'51"	Su 01°31'33"	Mo 13°03'57"
Ma 11°12'42"	Me 27°55'46"	Ju 18°37'56"
Ve 02°40'43"	Sa 21°01'23"	Ra 08°01'24"
Ke 08°01'24"	Ur 27°49'56"	Ne 12°16'52"
PI 18°46'19"		

Correlation #3

In the case, ‘Capital one- Leakage insider attack’, the hacker, Paige Thompson in her twitter and DM had posted,

*‘Ive basically strapped myself with a bomb vest, f***ing dropping capital ones dox and admitting it’ (shows emotional turbulence)*

Some months before the incident, she posted about her emotionally painful experience that she had to go through in her life due to the death of her cat.

‘One of the most painful and emotionally overwhelming experiences of my life’ ...

She also complained about her dating life on both her social media account and some of her work colleague. If that had been check before and handled properly, this should have been prevented.

Planetary positions on the day of event, July 19 2019, having mercury conjunct mars and sun in the house of cancer. As already mentioned, mercury and moon are natural enemies. Rahu, North node of moon is in house of Gemini, aspect by Saturn. Moon is in Capricorn aspect by mars, mercury, and sun. Mars is in Ashlesha nakshatra.

By overall analysis, mercury in moon’s sign of cancer causes emotional turbulence and therefore, analysts should very closely monitor the conversations, behaviour, and mental health of resources during these 30 days, whenever mercury is in cancer.

BASIC	LAGNA	NAVAMSHA	CLOUD
	Ur		Ra* Ve^
Ne*			Ma^ Me* Su
Mo			La
Ke* Sa*	Pl*	Ju*	

* Retrograde	^ Combust	
La 07°22'15"	Su 02°11'35"	Mo 28°17'45"
Ma 16°51'25"	Me 05°54'27"	Ju 21°14'55"
Ve 25°01'50"	Sa 22°22'20"	Ra 22°53'08"
Ke 22°53'08"	Ur 12°20'59"	Ne 24°20'44"
Pl 27°29'11"		

Other Insider threats examples

It is usual that any organization view insider threat warning from someone who may go wrong, on the side of goodness. The reason is companies don't want to accuse somebody without full evidence of crime and so they neglect. Now as per the Insider threat report survey, the average annual cost of insider threats has sky-raised in 2021, 2022.

Insider threats are not viewed as seriously as external threats, like an actual cyberattack. But when companies had an insider threat, in general, they were much more costly than external incidents. This was largely because the insider that is smart has the skills to hide the crime, for months, for years, sometimes forever.

Usually there are three types of insiders that could impact any organizations: Malicious insider who intentionally abuses the access privileges, careless insiders who could unwittingly expose data to outsiders, compromised insiders who use the compromised credentials to pass as an insider. Some types are easier to detect, some are hard to detect, but all of the types can cause serious harm to an organization.

Insider threat	Linguistic analysis	NSS	Planetary positions
Google insider threat, attacker who worked on Waymo self-driving program	Implied criticism, denial	High	Reckoned on the time when Anthony Levandowski transferred the company data to his personal laptop: Moon is debilitated, in Jyeshtha nakshatra conjunct by sun and Saturn. Moon's north node rahu is in Virgo, ruled by mercury conjunct mars
Anthem insurance insider breach	Anger	High	Reckoned when the vendor emailed a file containing information about Anthem's member to his personal id on July 8 2016. Mercury is in Cancer, North node is conjunct moon and Jupiter in Leo and Sun is in mercury. Saturn is in Scorpio aspect Rahu in leo.
Boeing insider who sold the trade secret to Chinese Govt	Suppression, greed	High	Although this was happening for decades, the incident received attention in 2009 July 16, mercury is in cancer, conjunct south node, sun is in Gemini, north node is in Capricorn aspecting mercury.

Calculating NSS and deriving the likeliness of threat:

Total number of words taken for consideration – TW

Number of negative words – NW

Number of Intensifiers(including exclamation, excessive capitalization)- I

$$NSS = (NW+I)/TW * 100$$

Afflicted moon(enemy sign/ in 3,6,8 house, conjunct or aspect by Saturn or North node)- 5

Afflicted mercury(enemy sign/ nakshatra)- 3

Non afflicted moon - 0

Non afflicted mercury - 0

PPC= Moon (emotions)+ Mercury (Language) score.

Total score(TS)= NSS+PPC

Consider the sample:

'YOU CAN NOT STOP US, YOU DIE NOW, ARE YOU AFRAID? DEATH TO AMERICA, DEATH TO ISRAEL, ALLAH IS GREAT'

Here,

Total number of words(TW)= 20

Number of negative words(NW)= 6

Intensifiers- 2(one for capitalization, one for great)

NSS= $8/20 * 100 = 40$

Score addition based on Position of moon and mercury:

Afflicted moon(enemy sign/ in 3,6,8 house, conjunct or aspect by Saturn or North node)- 5

Afflicted mercury(enemy sign/ nakshatra)- 3

Non afflicted moon - 0

Non afflicted mercury - 0

PPC= Moon (emotions)+ Mercury (Language) score, which is 8

Based on the position of planets calculated on the first anthrax attack: both moon and mercury are afflicted.

Repeated behaviour(RB)- A person expressing negative sentiments repeatedly, should also be taken into consideration. If the negativity scale is increasing or decreasing in their conversations would also give analysts, the clue on likeliness evaluation of an event. Therefore, a score of 1 for the first occurrence and Number of occurrences plus 1(N+1) as and when the analysts come across the NSS of the same instance taken for consideration.

Total score (TS) = NSS+ PPC+RB = $40+8+1 = 49$

Likeliness of threat/ event (LE):

If the TS value is greater than or equal to 40, the threat is more likely to happen, and immediate action is required- Set (High-Alert)

If the TS value is 25 to 40, the threat is likely to happen, action is required – set (Medium-Alert)

If the TS value is 10 to 25, the threat is less likely to happen, action required is (Warning)

If the TS value is 0 to 10, the threat is unlikely, no action is required.

In the above example, the TS is 49, the Likeliness of the event(LE) is more-likely, which is a High-alert event. Therefore, the personnel assigned from the leadership team to monitor the chat/email logs of employees should be notified immediately with a high-alert notification. The personnel must perform a false positive analysis as some sarcastic or ironical emotions could be understood by human perception only. The algorithm could later be enhanced for reducing false positives through additional irony/sarcasm perception techniques. It is observed that the false positive rate when compared to other linguistic analysis-based monitoring tools is less as the Astro-psychological logic is applied here as additional score booster to confirm the likeliness of the event.

Do leaders play a part in insider organization risk?

Whenever we talk about insider risk detection, we only consider employee behaviour, ignoring the risks that were lobbed by the toxic leadership to employees. To the question ‘Do leaders play a part in Insider-Risk?’- the answer is Yes, majorly. Although leaders are often protected from exposure by executive shielding, their behaviour and leadership skills can pose a very serious threat to an organization.

Some common types of leadership skills that we would have noticed in our work environment are, leaders that are disengaged, going too off from interacting with the entire team and engaging with only a closed set of high performers, paying no regard to workers, workplace, managing employees’ emotions, both negative and positive. Some leaders might think, ‘Is it really my job to manage workers’ negative emotions?’ The answer is Yes, because the emotional wellbeing of each employee is what is mirrored as

organizational health substantially. Leaders with fixation on only high-level assumptions and having a narrow mind when making decisions, those with blinders on. Some leaders will trust only their confidantes without being aware that they have a different, unethical, toxic behaviour towards others. Some leaders usually create that fear so that the employees will obey them easily by lashing out, punishing when some employee is speaking up. Setting out, telling others by making a good and bad examples list and forcing others to follow them. Pride and maintaining a superior perception of themselves and their confined familiar circle are usual that could increase the insider risk in a workplace .

Below are some suggestive measures to promote psychological safety and emotional wellbeing in the work environment:

- Defending and protecting the informants or whistle-blowers, because if leaders don't, it might be blown out and the risk shall be amplified.
- Showing appreciation and responding with enthusiasm when employees speak up.
- Incorporating an open model to analyse facts, honouring differing viewpoints instead of implicit biases to make decisions.
- Listen, acknowledge when an employee is expressing negative emotion with the leader, even if it is not reasonable. The employee loses the trust on leaders when leaders try to suppress the negative emotions or disregard them.
- It is very important that leaders don't step into the blame culture, like a parent-child relation, 'you will face the consequences', 'I told you already'.

Reference:

1. <https://insiderthreat.mitre.org/sentiment-analysis/>
2. <https://surface.syr.edu/cgi/viewcontent.cgi?article=1047&context=istpub>
3. https://www.researchgate.net/publication/326484154_Detecting_Potential_Insider_Threat_Analyzing_Insiders'_Sentiment_Exposed_in_Social_Media