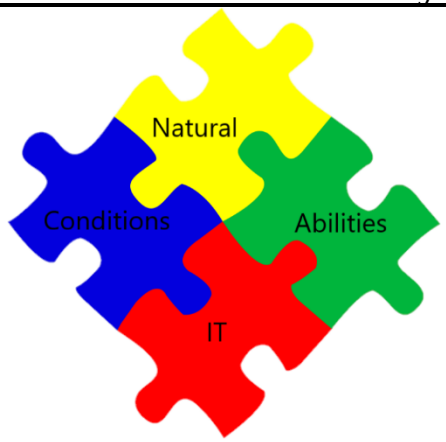
Natural abilities & conditions that can heavily impact the IT field



Introduction

This section discusses the *Ethical Issues in Hacking* devices and people via natural abilities and conditions as applied to the IT field. When we think of hacking, we think of people using machines or digital assets to hack the machines or digital assets of other humans. This is comparable to a person playing Chess and thinking that they are playing the game (chess), instead of playing their opponent. This section discusses the ethical issues of hackers playing their opponents (the hackers) and the game (hacking) (ethical issues in hacking (devices & people)) simultaneously. Playing the game and the player simultaneously can be advantageous as noted by *Madeinthemind* and *nimzo5* in addition to multiple other users at chess.com.

While people as a variable are accounted for in security auditing, limited consideration is given to their abilities. Most, if not all, security audits assume all people to be "same, same" in terms of abilities and threat capabilities. While people can pose threats with shoulder surfing, eavesdropping, fence-scaling, lock-picking, password cracking, and social engineering, not much else consideration is given. This section details why and how more consideration should be given.

This section discusses how natural abilities and conditions hack people and devices using reverse logic of how the internet works. Internet search engines work using algorithms that try to return the most relevant search results for users. Search results at the top of the list tend to be the most relevant or most visited sites if not a labeled paid advertisement. The more links, mentions, and visits a site has, the larger its node in the IoT web is. The more abundant larger nodes become, the more forgotten smaller nodes become. The more forgotten smaller nodes become, the more of a security risk or vulnerability they become. Machines may co-exist with humans and nature, but they are often built mimicking humans and or nature. The more advanced and inclusive technology becomes, the more humans forget about what exactly the device is mimicking or replacing. The camera and photographic memories are a great example. Many places with sensitive areas post signs warning that the use of photography or other electronic devices in that area are strictly prohibited. Yet people often forget cameras mimic the natural ability of a photographic memory. Before the camera, photographic memories were a larger node in the information web. After the introduction of the

camera, photographic memories became a smaller node in the information web, or at least cameras became a much larger node.

There isn't a lot known about some of or all the areas listed in this section, which in part makes research on those topics hard in addition to research that links them to a specific niche, such as Information Technology. Relative research, or lack thereof, highlights how smaller nodes can be utilized in hacking.

Three of the five subtopics in this section are related to autism. People with autism tend to be STEM savants as well as underestimated risk factors in network security.

Natural abilities

Since it is probably safe to assume government and military sectors are the largest employers of IT personnel, that means most IT personnel have access to information at an elevated level of sensitivity and confidentiality than most others. A photographic memory would directly sidestep any security measures in an environment prohibiting electronic devices and cameras to reduce theft of intellectual property or distribution of imagery.

Charisma

Definition

The Lexico dictionary powered by Oxford defines charisma as "n*oun: [mass noun] Compelling attractiveness or charm that can inspire devotion in others.*" *'The charisma of people who are smooth talkers and good listeners with positive personalities tends to attract, charm, and captivate broad audiences.'*

About it

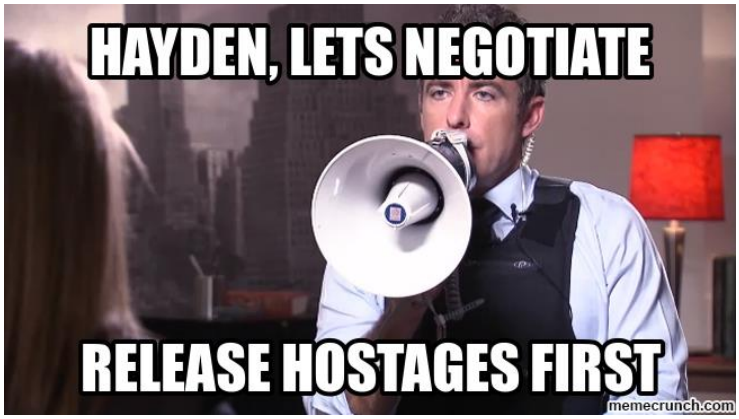
People who are familiar with role-playing video games know that a character trait can be "charisma" which usually allows a player access to certain content in the game based on social engineering, such as, cheaper prices at markets, access to secret rooms and items, and less susceptible to being attacked. While it does not physically make your character stronger, it does make the character stronger overall without the dependency on physical attributes. While physically handicapped people may or may not be

able to choose whether their video game character is physically disabled or not, they do not have that option in real life. Charisma is an ability that a physically abled person or a handicapped person can utilize with extraordinary results. Charisma is also universally relatable, which makes it more powerful than any physical ability.

The ethical issues in using it to hack

Charisma is a very powerful persona trait that is often underestimated. The effectiveness of charisma can be likened to the phrase about getting more bees with honey than vinegar. There is a lot to be said about smooth-talking criminals, as they have the ability to charm their way through security by saying they're new and left their security badge at home while flashing a smile and striking a quick conversation in passing. The hacker knows their charisma is overwhelming and some targets know it's just a ploy, but sometimes the magic of charisma as used in a negative light is more effective when directed towards lesser socialized people. The charismatic person knows they are utilizing social weaknesses in people with their charm to get what they want, but the ethical issue in using charisma to hack people is that when charisma is used in a negative way, it can be done carelessly, like most other things in life. Using charisma to hack people can gain a hacker access to something of value while instilling temporary false hope or unrealistic expectations, subsequently damaging them.

The ethical issues in using it to prevent a hack



The ethical issue in using charisma to prevent an attack are almost the same as the issues in using it to assist a hack. This can be exemplified by the coercion techniques of hostage negotiators. A hostage negotiator is willing to say almost anything that gets a criminal to release a hostage starting with trying to deescalate the issue by relating to the criminal before trying to convince the criminal the situation isn't worth it to them, before promising anything reasonable under the sun in return for the release of the hostage(s).

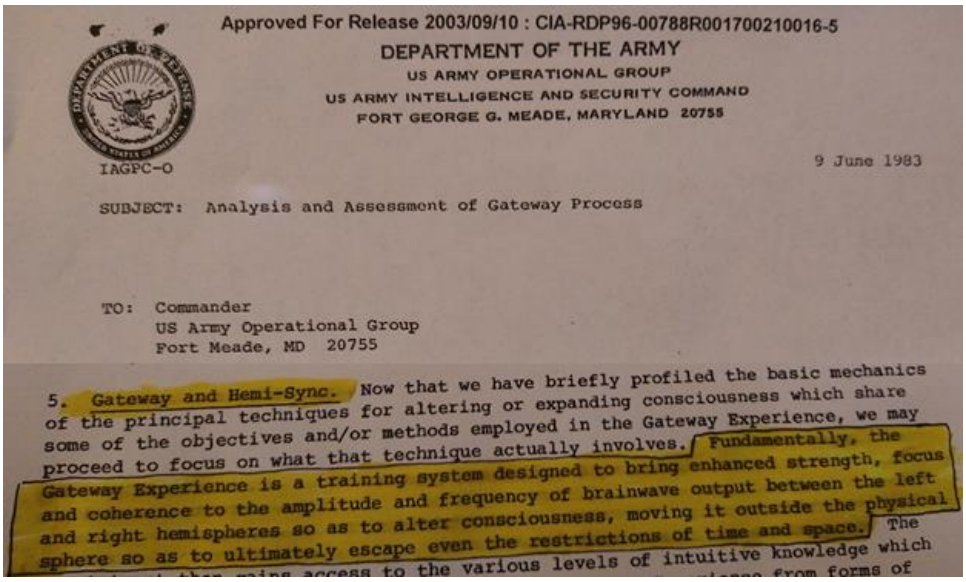
Gateway Process

!!! Disclaimer !!!

!!! 100% OF ALL INFORMATION IN THIS SECTION IS 100% FACTUAL AND SITED FROM A CIA DECLASSIFIED ARMY OPERATIONAL GROUP WHITEPAPER FROM 1983 !!!

This section draws source from a single CIA-declassified Army Operational Group report from 1983 titled "Analysis and Assessment of Gateway Process" as reported by Lieutenant Colonel Wayne M. McDonnell to Commander of The Marine Corps Special Operations Command Detachment One (Det O). The document itself is a 29-page report with a 2-page pre-report disclaimer due to the life-altering material in the report.

Definition



Approved For Release 2003/09/10 : CIA-RDP96-00788R001700210016-5

DEPARTMENT OF THE ARMY
US ARMY OPERATIONAL GROUP
US ARMY INTELLIGENCE AND SECURITY COMMAND
FORT GEORGE G. MEADE, MARYLAND 20755

IAGPC-O

9 June 1983

SUBJECT: Analysis and Assessment of Gateway Process

TO: Commander
US Army Operational Group
Fort Meade, MD 20755

5. Gateway and Hemi-Sync. Now that we have briefly profiled the basic mechanics of the principal techniques for altering or expanding consciousness which share some of the objectives and/or methods employed in the Gateway Experience, we may proceed to focus on what that technique actually involves. Fundamentally, the Gateway Experience is a training system designed to bring enhanced strength, focus and coherence to the amplitude and frequency of brainwave output between the left and right hemispheres so as to alter consciousness, moving it outside the physical sphere so as to ultimately escape even the restrictions of time and space. The ... to the various levels of intuitive knowledge which ... from forms of

The *Analysis and Assessment of Gateway Process* defines the Gateway Experience as a "*training system designed to enhance strength....of brainwave output....to alter consciousness, moving it outside the physical sphere....to ultimately escape even the restrictions of time and space.*"

About it

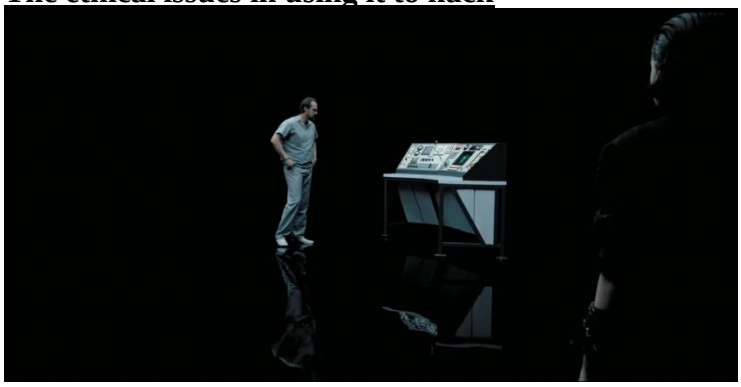
It's a whitepaper written by Lt. Col. Wayne M. McDonnell in June of 1983. The document is the government's exploration into the mechanics and functions of the human brain and consciousness. In the research of it all, the government realized that the Universe is nothing more than a complex hologram. The Gateway Process allows a person to hack and manipulate the fabric of space and time.

Sections of the document include....

1. Introduction
2. Hypnosis
3. Transcendental Meditation
4. Biofeedback
5. Gateway and Hemi-Sync
6. Lamp vs Laser
7. Frequency Following Response
8. Role of Resonance
9. Brain Stimulation
10. Energy Entrainment
11. Consciousness and Energy
12. ***Holograms***
13. The Part Encodes the Whole
14. ***The Consciousness Matrix***
15. Brain in phase
16. Evaluation

17. Self Cognition
18. Time-Space Dimension
19. Intervening Dimensions
20. Subatomic Particles
21. Dimensions In-between
22. Special Status, Out-of-Body Experience
23. Absolute in Perspective
24. From Big Bang to Torus
25. Our Place in Time
26. Quality of Consciousness
27. Consciousness in Perspective
28. Gateway Method
29. Hemi-Sync Introduced
30. Advanced Techniques
    - ***A. Problem Solving***
    - ***B. Patterning***
    - ***C. Color Breathing***
    - ***D. Energy Bar Tool***
    - ***E. Remote Viewing***
    - ***F. Living Body Map***
    - ***G. Focus 15: Travel into the Past***
    - ***H. Focus 21: The Future***
31. The Out-of-Body Movement
32. Role of REM Sleep
33. Information Collection Potential
34. Belief System Considerations
35. Redacted
36. Redacted
37. Motivational Aspect
38. Conclusion

The ethical issues in using it to hack

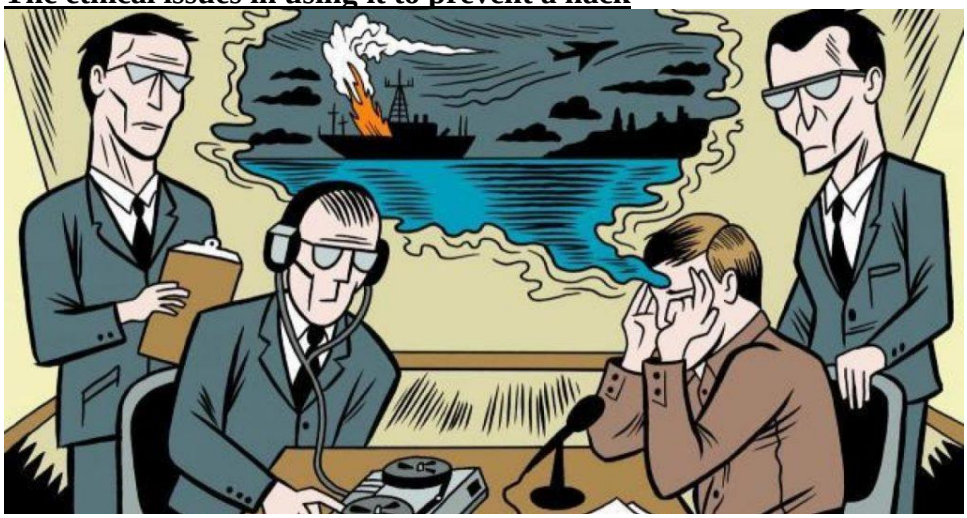


The ethical issue in using it to hack is that you are hacking the fabric of space and time as well as people which completely erodes the illusion of free will. The character 'Eleven' in the Netflix original series, Stranger Things, is able to remote view

targets of her desire. I myself am able to do this. The ethical issue is highly alarming as it is akin to Harry Potter with the cloak of invisibility and a time machine. This is credential harvesting and shoulder surfing at its peak glory. Hackers would be able to harvest all the credentials they needed without detection. Being able to remote view might also even negate the need for a hacker to initiate a hack if what they were seeking was access to a camera since they could just remote view the target themselves.

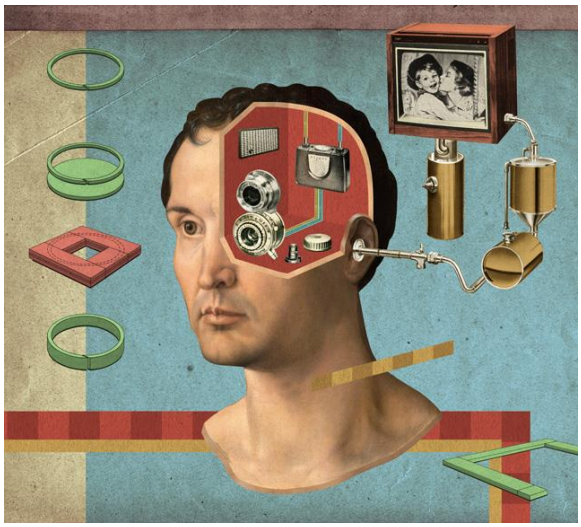
Another ethical issue in using the Gateway Process to hack is that it's so powerful and effective that even while including topics about The Big Bang, time travel, hypnosis, and sleep

The ethical issues in using it to prevent a hack



The ethical issue in using it to hack is that you are hacking the fabric of space and time as well as people which completely erodes the illusion of free will. The character 'Eleven' in the Netflix original series, Stranger Things, is able to remote view targets of her desire. I myself am able to do this. The ethical issue is highly alarming as it is akin to Harry Potter with the cloak of invisibility and a time machine. This is credential harvesting and shoulder surfing at its peak glory. Government officials could remote view a suspected criminal's house for clues that would determine if the suspicions were true. Police could then raid the hacker hideout if enough evidence were seen during a remote viewing to warrant a raid. The obvious ethical issue is explaining in court how you essential entered a home without permission or a warrant to specifically look for evidence that would directly support a warrant to go retrieve said evidence.

Photographic memory



Definition

The Lexico dictionary powered by Oxford defines *photographic memory* as *"noun: The ability to remember information or visual images in great detail."* *'I have a photographic memory and can remember things I see with great detail.'*

About it

While people are aware that some people have photographic memories, not everyone remembers, and not everyone who remembers realizes the extent of photographic memory capabilities. People take photographs because their brain lacks the ability to accurately photographically remember everything it sees, similar to a video camera that's always on record. Most people can buy a large hard drive at their local electronics store that will hold more pictures and videos than they could ever produce with a point and shoot camera. It won't be until people understand how lossless quantum data compression relates to the human brain that people get rid of cameras. While it's inconceivable for a human brain to remember everything it sees since it's inconceivable that the brain has the storage capacity for it, if humans could understand how the brain stores and compresses information on a machine scale, they might have the brain capacity to store everything they ever saw. Most machines designed with storage capacity tend to be designed with adequate storage capacity for the expected life duration of the product.

The ethical issues in using it to hack

People with photographic memories have the ability to see remember, and sometimes reproduce things they saw and weren't allowed to record that they sometimes shouldn't have seen in the first place. Back in the 1950s, the government wasn't as worried about people seeing things they didn't want them to see if they didn't have a camera to record it. In most courts, evidence is needed to substantiate a crime. As such, a camera was seen as needed to substantiate a data leak.

I used to work for a small, family-owned, government-contracted machine shop that produce parts that were not for public eyes. The company regularly gave tours to customers and prospective customers. Possibly for proof of business capability. I pointed out that if the production line and subsequent produced parts were not for public eyes, then they shouldn't be seen. After a while the company put signs up saying no cameras or other digital recording devices were allowed on the property and use of them inside the buildings was strictly prohibited.

The problem is that someone with a photographic memory will be allowed on the tour with no electrical devices, will see everything, and if they have any artistic talent, will be able to reproduce on paper what they saw in person. The saying is true that "there is more than one way to skin a cat". There are multiple ways to obtain a copy of top-secret blueprints although we won't discuss all of them, especially as some are outside the scope of this project.

One way to obtain a copy of top-secret blueprints is to hack a network that contains a data store where the desired blueprint is stored. This method could leave a digital footprint leading to you, which will raise alarms and detection. The machine shop I worked for saved all of their confidential and top-secret documents in paper form in filing cabinets and in digital form on hard drives stored on a network accessible by the WiFi-capable machines in the production line.

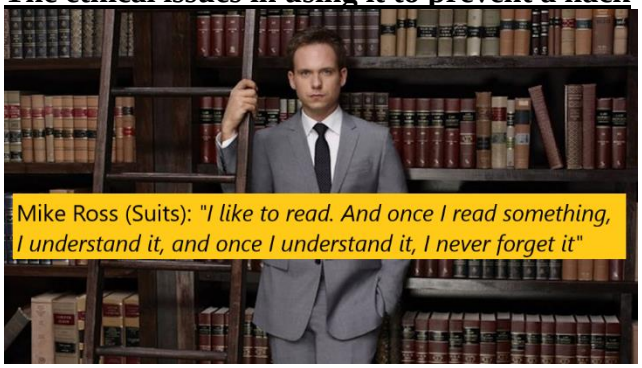
Another way to obtain a copy of desired blueprints is to physically steal them off a desk or from a filing cabinet. This method will raise alarms and detection.

A third way to obtain a copy of desired blueprints is to see them physically or by *remote viewing* via the Gateway Process (which is outside the scope of this project), photographically remember them, and then physically reproduce them on paper.

There is a short video on YouTube of an autistic artist named Stephen Wiltshire who is capable of taking a brief helicopter ride over a city and then completely reproducing it on paper with incredible detail. If the city were a military base and he had a camera, he might not have been offered the helicopter ride. Since Stephen has a photographic memory and doesn't need a camera, he wouldn't have had one, and the military would have let him fly over the base.

While Stephen knows the full extent of his capabilities, while maybe at the same time thinking that people underestimate him for being autistic, he is technically taking advantage of military personnel who allow him to see classified content that shouldn't be recorded knowing that he doesn't need a camera or other electronic device to record and reproce what he sees. Since most people don't have great photographic memories or abilities at all, it's one of the last things on a CSO's security checklist, if at all. Nobody ever stops to think about "what if someone with a really good photographic memory comes into my classified facility? How will I recognize them? How will I know if they're using it? Or how will I know what their intentions are?".

The ethical issues in using it to prevent a hack



The USA Network television series *Suits* stars a lawyer named Mike Ross who was quoted in season one, episode one as saying "*I told you. I like to read. And once I read something, I understand it, and once I understand it, I never forget it*" (Bray). The ethical issue here is that Mike Ross never took the bar exam, but is an acting attorney. A short conversation between Mike Ross and the legal office's lead attorney, Harvey Spectre, reveals the

nature of the ethical issue involved. A transcript of the brief conversation as it appears in the episode follows.

"**Harvey:** Unfortunately, we only hire from *Harvard*. And you not only did not go to Harvard law school, you haven't even gone to any law school.
Mike: What if I told you that I consume knowledge like no one you've ever met and I've actually passed the bar?
Harvey: ***I'd say you're full of crap.***
Mike: That's a Barbri Legal Handbook right there, right? Open it up, read me something, anything.
Harvey: Civil liability associated with agency is based on several factors including—
Mike: —including the deviation of the agent from his path, the reasonable inference of agency on behalf of the plaintiff, and the nature of the damages themselves.
Harvey: ***How did you know that?***
Mike: I learned it. When I studied. For the bar.
Harvey: Okay, hotshot. Fire up this laptop. I'm gonna show you what a Harvard attorney can do. Pick a topic.
Mike: Stock option backdating.
Harvey: Although backdating options is legal, violations arise related to disclosures under IRC Section 409A.
Mike: You forgot about Sarbanes-Oxley.
Harvey: The statute of limitations render Sarbanes-Oxley moot post-2007.
Mike: Well, not if you can find actions to cover up the violations as established in the Sixth Circuit May 2008.
Harvey: ***That's impressive*** but you're sitting at a computer.
Mike: Playing Hearts. Sorry, if you wanna beat me, you're gonna have to do it at something else.
Harvey: ***How can you know all that?***
Mike: ***I told you, I like to read. And once I read something, I understand it. And once I understand it, I never forget it.***
Harvey: Why take the bar?
Mike: This dickhead bet me I couldn't pass it without going to law school.
Harvey: Okay look, this is all pretty fascinating stuff but I'm afraid I gotta get back to work. I'll make sure that Serpico isn't around waiting for you."

An ethical hacker with a photographic memory could more easily remember more of their IT knowledge at a quicker rate than someone without a photographic memory. This can be useful during a live hack in remembering command line functions and commands much quicker and more completely. It would also allow

an ethical hacker to more completely remember the man pages of a command line function which would greatly improve their ability in using the command line to mitigate hacks.

Natural conditions

Auditory Hyperesthesia

Definition

Hyperesthesia is defined by the International Association for the Study of Pain as being "*increased sensitivity to stimulation, excluding the special senses*", with *special senses* according to Wikipedia as being "*vision, hearing, balance, smell, and taste*".

Auditory hyperesthesia is defined by vocabulary.com as being "*noun: abnormal acuteness of hearing due to increased irritability of the sensory neural mechanism; characterized by intolerance for ordinary sound levels*"

About it

Hyperesthesia is defined as being an increased sensitivity to senses, and not in a pleasant way, while auditory hyperesthesia is defined as having exceptionally-good hearing.

The ethical issues in using it to hack

The ethical issue in using auditory hyperesthesia to hack is that you are subconsciously absorbing what might otherwise be considered private, exclusive, or confidential information. If you are not interested in everyone's conversations, you could tune them

out easily enough. At the same time, if you are trying to absorb as much intelligence as possible from your environment via audible information, then tuning in would be of best interest. When tuning in to all the chatter and noise going on in the environment around the hacker, they are able to cherry pick the most valuable information and aggregate it into information that can be used to hack network or perimeter securities.

I'm told that my hearing is more exceptional than people realize when I divulge information I subconsciously or intentionally eavesdropped on from a seemingly impossible distance. Then I tell people that I hear everything but at the same time "ignorance is bliss". From what I hear, people talk too much about personally identifiable information that can be used in credential harvesting.

The ethical issues in using it to prevent a hack

The ethical issue in using auditory hyperesthesia to prevent hacks, is that it strips people of their sense of privacy and perhaps security. When he's not busy being Superman, Clark Kent works at a newspaper publisher. Newspaper journalists often have confidential informants that they work with who would rather not be named or identified. This creates an information web with very specific nodes (journalists) that interact specially with other specific nodes (confidential informants). As such, information tends to be node specific and can be traced back to sources. For example, if Bob is having a word-of-mouth party and tells five friends, five separate party themes, Bob is able to assess the network size of each of his five friends based on how many people show up and which of the five party themes their outfits reflect.

An office environment may not provide specific designated privacy zones for employees, other than perhaps the bathrooms. Although employees usually expect their personal offices to be personal and private spaces. However, if Bob has auditory hyperesthesia, chances are he can hear a lot more than most other people realize. While Superman's auditory hyperesthesia could be used as the peak performance point of auditory hyperesthesia, the intensity exists on a sliding scale of inconsistency

among afflicted people. I myself hear more than most people would like me to be able to hear. While I don't think anything extraordinary of my hearing, I apparently hear things others don't and from distances they can't. As such, Bob might be able to hear everything that occurs on the entire office floor, through walls and closed doors, but nothing outside the office floor. If that were true, then Bob would be able to hear conversations that occur in offices even with doors closed. If Bob is working late with another employee who works on the other side of the office floor, and overhears that employee tell someone on the phone that they are staying late to hack the company's computers, Bob will be able to stop the hack. The ethical issue that the other employee's office is presumed to be a safe and private space. While the other employee would have to assume their hack was prevented by Bob, they would have no idea how Bob would have ever known unless he overheard the conversation. Even then, the other employee would wonder how Bob could have possibly ever heard the conversation from across the office floor and through at least two closed doors. While this example alone is hard to believe, that's what poses the ethical issue. Is it ethical to foster a work environment with no privacy where all conversations are heard and possibly recorded? While it isn't out of the question of possibility, especially when considering places like military bases, intelligence headquarters, security firms, banks, and prisons.

There isn't a single species on Earth that enjoys being watched. People like watching people, but don't like being watched themselves. Being watched, or even the feeling or suspicion of being watched can put someone in a constant state of angst and paranoia. How auditory hyperesthesia in the office space differs from being in an office with strict security is that the strict security is seen and mutually acknowledged by both the viewer and the viewed. Auditory hyperesthesia is unseen and unknown. Someone being watched by a camera all day is less apt to be stressed out as they know the camera is there and watching and that everything they do is recorded. However, if there is no camera, but an office memo has been emailed to all employees saying that one of the employees in the office has auditory hyperesthesia and to please be mindful of all conversations. Since laws prohibit the employer from naming or firing the employee, the unnamed employee now causes stress to every other employee as mass paranoia would sweep through the office like wild fire. Everyone would be wondering who the employee is and if their conversations are really private. Employees might start leaving the company as a result causing a company to lose some of its best employees.

Synesthesia

Definition

A brief definition of Synesthesia follows five times. Once as it appears to most people, including myself, and four ways that appears to someone with synesthesia.

The first definition is of how the definition would appear to most people, including myself.

The second definition is how the definition would appear to a person with synesthesia on a white background, with white-colored 'I's and 'O's highlighted black so people can more easily read the text.

The third definition is how the definition would appear to a person with synesthesia on a white background, with white-colored 'I's and 'O's not highlighted. This shows most accurately how alphabetical text appears to people with synesthesia as text is most often on a white background do to default text colors predominantly being black and white offering the best neutral contrast.

The fourth definition of synesthesia is on a light grey background to show how the definition would look to someone with synesthesia reading it on a light grey background, allowing them to more readily see and or determine the placement of 'I' and 'O' letters. It also allows people to see a more accurate representation of what text looks like to someone with synesthesia as white-colored letters do not appear with black highlight to aid in the visual detection.

The fifth definition of synesthesia is on a light grey background with non-alphabetical characters removed since I'm not entirely sure what colors non-alphabetical characters are as I was only able to find research on what colors the letters were determined to be. That's how fresh this area of research is and why it's so critical to conduct more research in this area.

"Synesthesia is a neurological condition in which stimulation of one sensory or cognitive pathway (for example, hearing) leads to automatic, involuntary

experiences in a second sensory or cognitive pathway (such as vision). Simply put, when one sense is activated, another unrelated sense is activated at the same time. This may, for instance, take the form of hearing music and simultaneously sensing the sound as swirls or patterns of color." **(Psychology Today)**

"*Synesthesia is a neurological condition in which stimulation of one sensory or cognitive pathway (for example, hearing) leads to automatic, involuntary experiences in a second sensory or cognitive pathway (such as vision). Simply put, when one sense is activated, another unrelated sense is activated at the same time. This may, for instance, take the form of hearing music and simultaneously sensing the sound as swirls or patterns of color.*" **(Psychology Today)**

"*Synesthes a s a neur l g cal c nd t n n wh ch st mulat n f ne sens ry r c gn t ve pathway (f r example, hear ng) leads t aut mat c, nv luntary exper ences n a sec nd sens ry r c gn t ve pathway (such as v s n). S mply put, when ne sense s act vated, an ther unrelated sense s act vated at the same t me. Th s may, f r nstance, take the f rm*

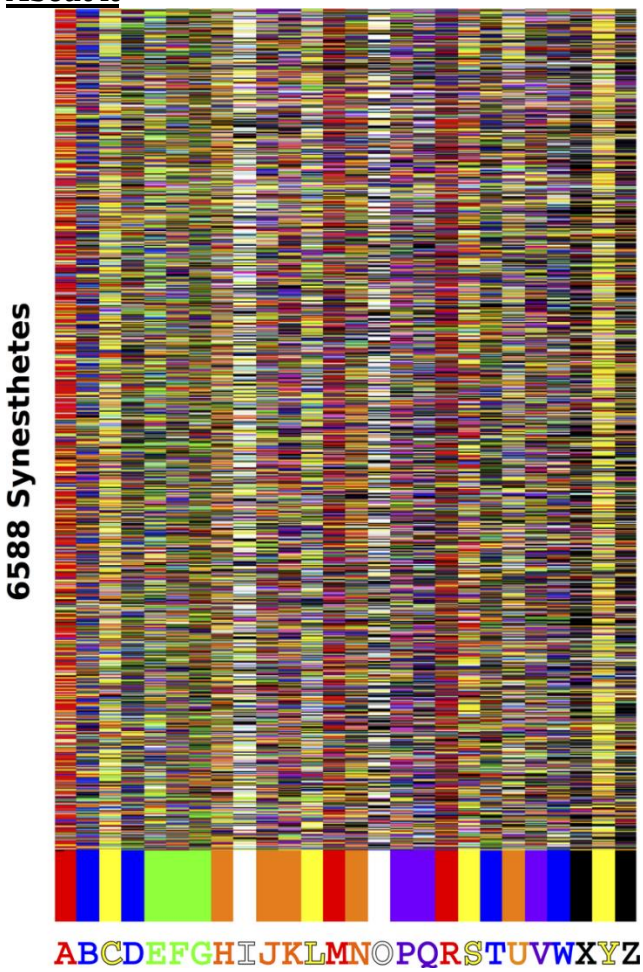
f hear ng mus c and s multane usly sens ng the s und as sw rls r patterns f c l r." (Psych l gy T day)

"Synesthesia is a neurological condition in which stimulation of one sensory or cognitive pathway (for example, hearing) leads to automatic, involuntary experiences in a second sensory or cognitive pathway (such as vision). Simply put, when one sense is activated, another unrelated sense is activated at the same time. This may, for instance, take the form of hearing music and simultaneously sensing the sound as swirls or patterns of color." (Psychology Today)

Synesthesia is a neurological condition in which stimulation of one sensory or cognitive pathway for example hearing leads to automatic involuntary experiences in a second sensory or cognitive pathway such as vision Simply put when one sense is activated another unrelated sense is activated at the same time This may for instance take the form of hearing music and simultaneously sensing the sound as

swirls or patterns of color Psychology Today

About it



Synesthesia allows people to see text as color, which allows them to see and extract information from a wide range of text-based mediums more effectively including command line outputs and encrypted texts.

While I myself am not afflicted with Synesthesia, my brain does understand colors better than text. My brain has an easier time binding large amounts of information to different colors and then recalling entire information stores by referencing particular colors that pertain to the desired information stores. This is very similar to the associative memory access method used by computers wherein a portion of data is used to retrieve a much larger portion of data. This is proven by the fact that the less content a person needs to absorb, aggregate, and assess, the quicker their brain is able to continue processing and compiling new data.

The word ‘book’ will be used to prove the concept. The word ‘book’ contains four letters, two of which are the same. When coded into synesthesia using the first picture in this section, the word ‘book’ would look like this:  Moving on from text to colors, the word ‘book’ only contains three colors, one of which is used twice. For starters, the letter ‘B’ is a blue letter as indicated by the picture above, and is one of only four blue letters (about 15.38% occurrence). Subsequently the letter ‘O’ is white and is one of only two white letters (about 7.69% occurrence rate) orange and is one of only five orange letters (about 19.23% occurrence rate).

The math of the color binding works statistically. An event that occurs every time is understood to have a 100% occurrence rate. Subsequently an event that occurs 50% of the time is understood to have a 50% occurrence rate. An event that is contingent upon two conditions being met, wherein both conditions are always met, is understood to have a 100% occurrence rate. Subsequently, an event that only occurs if two conditions are met and both conditions are only met 50% of the time, is understood to have an occurrence rate of 25%.

This statistical math is achieved by multiplying percentages. For example....

100% **x** 1 = 100% (100 **x** 1 = 100)
50% **x** 1 = 50% (0.50 **x** 1 = 0.50)
50% **x** 50% = 25% (0.50 **x** 0.50 = 0.25)

As a result,

15.38% **x** 7.69% **x** 19.23% = 0.02274374406% (0.1538 **x** 0.769 **x** 0.1923 = 0.02274374406%)

The subsequent result is a word that has a 2% occurrence rate, which means if it needed to be determined if a 200-page encrypted text contained the whole word ‘book’ or not, having a 2% occurrence rate would mean the word ‘book’ is in the top 2% in terms of word rarity, which will make it stand out amongst other text for being a uniquely visibly more distinct color pattern seen less often.

A decrease in a word’s occurrence rate increases the word’s uniqueness, which makes singling it out of other words and reading it in text much quicker. Where a regular person would be looking for B-O-O-K amongst other words, which is a group of four objects as the double ‘O’ is seen as two separate objects.

Whereas BOOK is technically four letters seen as four objects with one object distinctly visible twice, a closer inspection would reveal that same-colored text placed next to each other may appear as individual letters, but they also appear as simplified color spectrums. Such as the ‘OO’ in ‘BOOK’ appears as one color spectrum while the blue ‘B’ and orange ‘K’ appear as two other separate and narrower color spectrums. The result is BOOK appears as a three-colored rainbow. Considering each of the 26 letters of the alphabet corresponds to one of eight colors, it makes structured text more unique and searchable.

The color groups are as follows....
Red
A, M, R
Blue
B, D, T, W
Yellow
C, L, S, Y
Green
E, F, G
Orange
H, J, K, N, U
White
I, O
Purple
P, Q, V
Black
X, Z

The colors pertaining to vowels are as follows....
Red
A
Green
E
White
I, O
Orange
U
Yellow
Y (interesting that yellow represents y)

In conclusion, only five of the eight colors representing the 26 letters actually represent vowels. That means there are three color groups that do not contain vowels (blue, purple, and black....interesting that the three colors that don’t represent vowels are of similar hue in the sense if they were colored laundry, you’d

probably wash them together separate from the other five colors that represent vowels, even red. So while Synesthesia is caused by a nervous system disorder, there seems to be a much deeper and more scientifically methodical way of how and why it functions and affects people who experience it. It almost appears to function in a way that would suggest it shouldn't necessarily be considered a detrimental affliction or disease as it seems to speed up the brain's data acquisition, aggregation, and query processing ability amongst other functions.

With non-alphabetical characters removed from the definition since we can't agree on what colors represent each punctuation mark, it's easier to remove them than wrongfully assign them arbitrary colors. With that being said, the fourth definition highlights how easily black-colored letters and words with them appear to people with synesthesia.

The ethical issues in using it to hack

While the above picture is of programming code and is not an accurate depiction of what a person with Synesthesia sees, it does offer a rough idea of how colors can easily group and highlight data. This is especially true with program coding wherein each code function is represented by a different color to make it easier to read. Synesthesia is the natural version of that. There is so little known and verified information about the condition, which complicates determining how an individual person has adapted to use their ability and what they are capable of doing with it. As such we will have to work with what is known and verified in order to reach a determination on how it can be used unethically to commit or aid hacks.

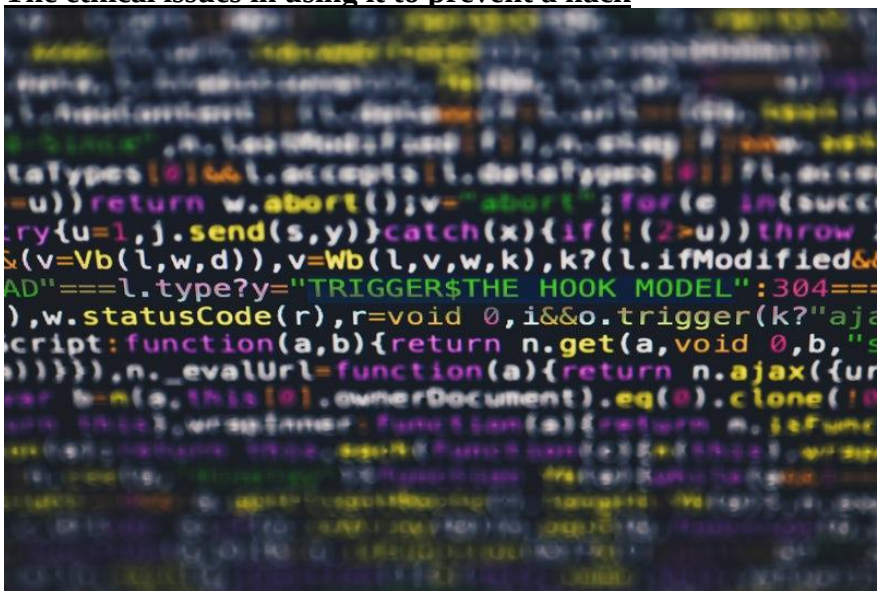
Synesthesia would be used by hackers as an information mining aid as it would allow them to absorb, filter, and aggregate information at a quicker rate.

As it is, in the entire definition of synesthesia, black-colored letters only appear twice and it's the same letter twice in two different words. The other black-colored letter being 'Z'. With that being said, it makes it super easy for a hacker to look for and acquire any needed information containing the letters 'X' and 'Z'. This is especially notable and useful in cases of someone's name being 'Alex'. It's also useful when scanning a document where 'yes' to a question or option is indicated by an 'X', and a hacker is looking for what options or questions a target said 'yes' to. This is especially useful in credential harvesting and data mining.

The next most visible letters are 'A', 'M', and 'R' as red letters. These letters are the next most visible colored-letter group due to the frequent absence of black-colored letters and the high-visibility of the color red.

Since the two black-colored letters are the most visible letters and the three red-colored letters are the next most visible letters, that makes short words containing black and red letters to be highly visible and risky words to use in cybersecurity.

The ethical issues in using it to prevent a hack



The ethical issue in using synesthesia to prevent an hack stems from the unethical issue in using it to aid a hack. Since we understand the word 'Alex' to appear as such to people with synesthesia, what we can also understand is that the word contains four letters. Each of the four letters is a different color. The first ('A') and last ('X') letter are highly visible letters that appear less frequently than others. The middle two letters are 'L' and 'E'. The yellow 'L' is almost invisible on the white background, and the green 'E' is a neutral color not necessarily attracting or repelling to viewers. The green letters being more neutral also allows them to exist almost as the default black font of people without synesthesia. Since red letters (A, M, R) and black letters (X, Z) are the most visible letters and yellow letters (C, L, S, Y) are harder to see on

white backgrounds. Since the letters ‘I’ and ‘O’ are white-colored letters and are more than likely invisible to people with synesthesia when being read on a white background.

With that being said, a CSO might reconsider network user credential requirements. Since there are many methods of credential harvesting, and shoulder surfing is a popular and often forgotten about method for credential harvesting, hackers with synesthesia can use this to their advantage by more quickly absorbing and analyzing data. To mitigate credential harvesting and other hacker techniques, a CSO might now require all network user credentials to be at least 12 characters long, avoid the use of the letters A, M, R, X, and Z, while promoting the use of the letters C, I, L, O, S, and Y. As a result, ‘S C LY’ (‘SICILY’) is hard for a person with synesthesia to read on a white background. Much like ‘live’ is one word that sounds two different ways when used differently.

For example....

People like to live life to its fullest extent.
People like to listen to live music.

While ‘S L ’ (‘SILO’) and ‘S L ’ (‘SOLO’) may not be spelled the same, sound the same, or even look the same to someone without synesthesia, but to someone with synesthesia, they look the same. Understanding this concept might make a CSO consider requiring network user credentials to contain words where the letters ‘I’ and ‘O’ are interchangeable, such as ‘silo’ and ‘solo’.
On the other hand, if a user’s name or credentials are, or include ‘MARX ARMZA’ (‘MARX ARMZA’), A CSO might flag it as ‘high risk’ since it contains only black and red letters. The ethical issue in using synesthesia to prevent a hack is that it imposes unfair restrictions on network users that don’t fully understand the reasoning or the mechanisms behind it. Restructuring network credentials to account for synesthesia would require a massive overhaul of requirements and would include lengthy requirement documentation at text-entry boxes.

While incorporating new network credential guidelines that account for synesthesia would strengthen network security, it unfairly asks a lot of network users and would probably even deny network users from using certain passwords they already use and have never had a problem with.

Through machine learning, it would be possible to learn which network users and hackers have synesthesia based on their keystrokes and mouse activity. A mouse with a lot of recorded highlighting activity might belong to a person with synesthesia and the excessive highlighting activity is due to them constantly highlighting text looking for white-colored letters (‘I’s and ‘O’s).

My father is red/black color blind, wherein red and black appear similar to him. Having to read red text on a black background is his least favorite reading setup. While this section may be on synesthesia and color blindness is more or less the opposite in the sense that it involves people seeing less color, whereas synesthesia causes people to see more color, it does involve the same methods and techniques as synesthesia. As such, if a small security company only hired red/black color blind people for security reasons, all computers display text could

be configured to only display red text on black backgrounds to mitigate the effectiveness of credential harvesting via shoulder surfing in the office.

Effects of Passive Learning on Cybersecurity

Security of data and information in computer network systems depends on the strength of cybersecurity. Cybersecurity needs to be upheld to enforce secure internet access and usage. Every individual needs privacy and security in access to personally owned property. All private and confidential data need to be protected from intruders. Internet-connected systems pose a great danger of insecurity over information that circulates on social media. Private information should be inaccessible by unauthorized people at all levels. Passive learning and attacks are significant threats to the information posted on the internet. Cybersecurity protects information on the internet from passive learning and attacks. Also, it prevents unauthorized access to information circulating on the internet. This article discusses the effects of passive learning and passive attacks on cybersecurity.

Passive learning is a method of learning where students receive information from the instructor and internalize it. A few examples are seminars, lectures, and textbooks where communication is mostly one-way. Passive learning helps improve certain skills, such as writing skills, listening skills, and organization skills. The learner is responsible for paying attention and understanding the material that is being told by the instructor.

Cybersecurity refers to the protection offered on systems connected to the internet from cyber threats and attacks. Organizations and individuals use cybersecurity to prevent unauthorized access to computer systems and data hubs. Passive attacks refer to security attacks in which the information is not modified. Passive attacks include traffic analyzes and the release of the message in the content. The attacker observes the information, copies it and may use it for malicious intentions.

In most cases, the target does not realize the occurrence of the attack. Wireless broadband technology has features that make it vulnerable to passive attacks. Passive attackers take advantage of the large scale of the network. The large scale of the network makes it easily accessible by intruders.

Passive learning allows the learners to acquire and store the information without getting feedback from the instructor. Passive learning among computer science and related fields might be harmful to cybersecurity because the knowledge acquired by the students is unutilized. Therefore, such students become computer experts, but they do not incorporate the skills in their entire life (Bendale & Prasad 2018). They might have been tempted to use the information illegally to benefit themselves through hacking computer systems. The internalized information is not applied anywhere by the learner. Passive learning is a threat to computer network systems since the learners can try to apply the stored knowledge wrongly.

Currently, passive learning is one of the primary sources of cybersecurity inconveniences and limitations. Passive learners in computer science and related studies are likely to engage in passive attacking of connected computer systems. Passive learning affects cybersecurity when its victims apply their computer knowledge to modify

computer programs without permission (Riley & Ward 2017). Passive learners are always anxious to attempt what they learned in their field of study. This anxiety can direct them to evaluate and copy information without modification illegally. Such illegal attempts endanger cybersecurity because private information can get accessed illegally. Passive learning affects cybersecurity when the learners get access to information on the internet without the information originator's concert.

Passive learning and attack affect cybersecurity in the following ways. First, in passive attacks, the attacker may use the information maliciously since the message is not modified. The information acquired through passive attacks is directly linked to the original website; the attacker may use it to tarnish the name of the website. Passive attackers get their way to the private information in the attacked network systems and interfere with the information therein. The attacked system might be malfunctioned by the attackers. Multifunctioning computer systems interfere with the overall working of the system (Surya & Magrica 2017). Once the attacker can manipulate the computer networks, they may interrupt sensitive data such as medical data. In medical fields. Passive attacks make the information unsecured and unavailable unsecured for use. When passive attackers access the information, they misuse it. Attacked information cannot be used for the intended purpose by the originator. A passive attack usually aims at getting access to open and vulnerable ports of the computer's network system. If the open and vulnerable ports contain valuable and confidential information, the attack takes advantage and can damage the whole system.

Passive attacks interfere with cybersecurity in organizations leading to robbery and theft in organizations. Inadequate cybersecurity due to passive attacks private information of the organization can be accessed by thieves and robbers. Thieves and robbers get to know the essential information about the organization. This makes it easier for thieves to plan an attack using the leaked information. Leaked information enables the thieves to know places vulnerable to an attack. Interference of an organization's cybersecurity poses a significant threat to the organization because all of its confidential information can be accessed by intruders. Intruders access the organization's private information, intending to manipulate the organization's activities that rely on computer systems. Passive attackers are not easily detected; thus, they can modify the entire information without the computer system owner's concert.

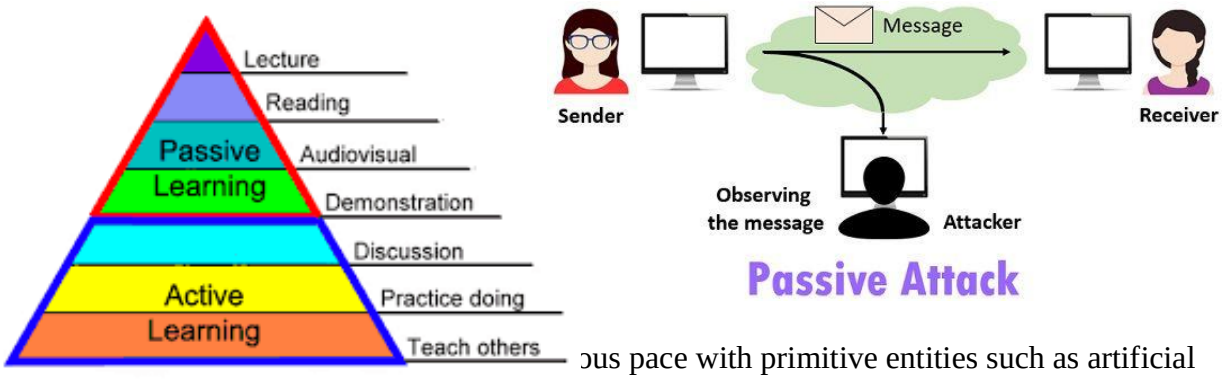
Cybersecurity serves to secure the information that circulates in the connected computer systems. Exposing the information to unintended users makes the information unsafe to be used for the intended purpose. Information stored under the computer network systems becomes useless once the passive attackers get access to it. They can use the information to modify the whole network system (Surya & Magrica 2017). The owner cannot use the modified network due to inadequate cybersecurity. Passive attacks reduce the effectiveness of the computer system network as attacked systems are unreliable. A reliable computer system must have sustainable and robust cybersecurity to guarantee the security of the information and communication that can be made through it. Once passive attacks can access and get private information from the computer network system, it poses a threat to any other information.

Passive attacks weaken the cybersecurity of attacked computer network systems. This predisposes the computer system to active attacks that modify the information obtained from the attack. Weak cybersecurity cannot detect and protect the network system from any other types of attacks. Active attacks modify the information acquired after attacking, and as a result, the information loses meaning. Active attacks threaten the strength of the connected computer systems. Through passive attacks, cybersecurity loses the ability to protect the information stored in the computer network system. Computer network systems contain information for personal use among authorized users of the system; thus, any interruption interferes with their activity. Passive attack lowers the cybersecurity of security systems leading to terrorist attacks. The security of a country depends on cybersecurity to ensure that security data information is inaccessible by the enemy. When cybersecurity is insufficient, terrorists might access confidential security information about a country leading to an attack. External and internal terrorist attacks are linked to weak cybersecurity that enhances passive attacks of the security systems (Tajdinian & Mohammadi-Ivatloo 2020). Passive attacks weaken the cybersecurity of secure computer systems, making it easier for the enemies to locate a suitable place for launching the attack. Weak cybersecurity resulting from passive attacks also exposes the plans and movements of security organs, enabling the enemy to escape security operations. Because the enemy already knows when the operation was planned and the expected time to launch the operation. Also, the enemy can hack the military equipment leading to failure in operation.

Cyber-attacks such as passive attacks lead to significant losses in businesses and enterprises. Passive attack damages the cybersecurity of a business firm, exposing the private information of the firm. This predisposed the business firm to theft, which leads to significant losses. Since communication in large business firms depends on electronic data stored in the computer network, any damage such as a cyberattack leads to inconveniences in communication. When the electronic system fails in business firms, online marketing is hindered, leading to diverse losses. Cybersecurity is a pillar to all processes in the business; hence, factors that affect cybersecurity induce losses in business (Tajdinian & Mohammadi-Ivatloo 2020). Passive attacks might interfere with essential business records such as sales records and payment records stored in electronic means. The interference in the payment records leads to mistrust between the employees and the management. Loss of sales records lowers the firm's reputation because customers might lose trust due to the inconveniences.

In conclusion, cybersecurity is a backbone to data privacy and information stored in computer network systems. Cybersecurity secures the information and data from intruders. However, cybersecurity is endangered from cyberattacks and threats. The main threats related to cybersecurity are active and passive attacks. The passive attack does not involve modification of the information. Besides, passive learning also affects the cybersecurity of the information stored in computer systems. Passive learning allows the learners to acquire and store the information without getting feedback from the instructor. Passive learning affects cybersecurity when the learners try to apply what they learned in the field illegally. Passive learning threatens cybersecurity because the learners might get

access to and modify information on the internet unlawfully. Passive attacks pose a danger to the security of information on the internet because of the attackers' access information on the internet without the permission of the originator. When cybersecurity is compromised, the absolute privacy of the message content circulating in the computer system is also compromised. Passive attackers copy the information on the internet, and they might use it maliciously to tarnish the name of the original website. Weak cybersecurity gives way for the attacks to modify the computer network system. Passive attacks also breach active attacks that modify the information on the computer network system. Besides, passive attack weakens the cybersecurity of military computer systems leading to insecurity. Inadequate cybersecurity in business firms leads to losses and loss of essential business records. Insufficient cybersecurity also predisposes organizations to robbery and theft. It is important to remember, security of data and information in computer network systems depends on the strength of cybersecurity.



ɔus pace with primitive entities such as artificial intelligence and machine learning charging for stability. Technology change has changed the way of operations by providing manageable and easier ways of information distribution. With advances in technology, information breaches have become rampant, and specific data might not meet the predefined standards. Information is shared among entities that find it important for their operations, but the acquisition and distribution process submit such information to scrutiny for ethical considerations. The ethicality of data has been compromised with the increased expansion of the data economy, where companies and people collect and sell information for profits or other reasons that might be malicious. The big question that arises is whether information that is acquired through ethical means can be used for ethical distribution and vice versa (Shetty, Shehan & Kshitij 6). Data has categories of characteristics that make it dependable. These traits include confidentiality, integrity, and authenticity. This paper explores whether ethically/unethically hacked information justifies ethical/unethical distribution by assessing the issues and consequences of any of the practices mentioned above.

To promote data security, ethical principles must be defined to cater to all necessary requirements for any data exchange process. Ethical hacking has its advantages, and it is principally associated with the ethical handling of information acquired during the process. According to the Association of Computing Machinery (ACM), data must be preserved with professionalism

(para. 3). This includes the observation of fundamental principles guiding and handling of data for a specific purpose. ACM also notes that respect for privacy and being honest, trustworthy, and avoiding harm are basic principles associated with data storage and distribution (ACM para 11). The justifications for the legitimacy of hacked information are refuted by authors who claim that once data acquisition methods have been compromised, the data itself and its applications lose legitimacy. ACM also points out that data handling must be devised in a manner that "*contribute to society and human well-being, acknowledging that all people are stakeholders in computing*" (ACM para 5). Therefore, justified use of hacked data might be challenging to defends since it should be handled with specified state provided by its stakeholders

Security breaches and exposure of confidential data are frequent phenomena around the world. These exposed data from security breaches present an ethical dilemma on what can be done to it or how it should be handled to maintain a high level of ethics and codes related to information handling. Depending on the area of application, some laws and norms prohibit the use of unethically obtained data in research. In some other instances, information holders must come to terms with the fact that the data in their holding was unethically obtained and must be used in ways that observe the required mandates. According to David Douglas, there are exceptions to the use of data in law, whether it was illegally and unethically obtained, which induces disparities and raises the question of justification and use of such information in different instances (Douglas 23). The unethical distribution of information is expensive for the entities whose data are jeopardized and exposed to the ruthless would of exploitation.

The two segments of analysis in this paper are categorized into ethical and unethical prospects, and each is independent of the other. When data is unethically obtained, then it cannot be used for ethical distribution since all that is born of it is naturally unethical. On the contrary, ethically obtain information has two chances, and one might be an ethical distribution while the other constitutes malicious intentions that are deleterious. In some cases, unethically obtained data is might be used for ethical distribution and research that is beneficial for cases. However, any outcome from the use of unethical data is tainted by the fact that it lacks authenticity and trust. On the contrary, environments such as the legal entity call for unethical data use in a process that is ethical, and justifications exist for such scenarios. However, unethically obtained data cannot be justified with simplicity if its use is for unethical distribution. The distribution of ethical or unethical data is essentially limited to the ethical consequences that an organization or individual will endure. Unethical use of data for unethical distribution is expensive and costly to the owner as numerous factors are loosened, which might lead to damages.