Social Engineering and Psychological Warfare Are Becoming the Most Dangerous Weapon in Cyberwarfare.

Alexander Abou Khir

Old Dominion University

CYSE426 Cyber War

Professor Alex Korb

April 4th, 2025

For most of humanities history we have fought in wars with physical weapons and are face to face with military force. Humanity growing with new advances in technology to the rate where everyone relies on the internet and a device to interact with others instead of physical ways of communication like letters and word of mouth. With our globe becoming more interconnected with technology, physical wars are becoming less of a pursued way of combating an enemy, as of now cyberwarfare has become the new way of war. Even though cyberwar is still a relatively new way of fighting, there have been rapid involvement of improving technological defenses that keep evolving with new tactics. However, there has been one category of offensive strategy that has been the most reliable which is psychological manipulation. Digital manipulation includes using social engineering, phishing. Deepfakes from AI, misinformation and disinformation; These methods exploit human behaviors instead of codes and digital infrastructure, humans tend to be easier to manipulate than digital failsafe's, a threat actor doesn't always need to code, sometimes its just a convincing email that can give them unauthorized access to a digital infrastructure.

Psychological warfare has always been around, however back then it historically was propaganda to influence, intimidate and or manipulate a population or specific target. In present modern era with the digital age becoming the new world, this concept has evolved dramatically and has become part of cyberspace where influence can be weaponized through exploitation of trust, and misinformation in social media for instance. In the digital aspect, psychological warfare essentially means any attempt to exploit human emotions, behaviors and thought process to achieve a goal, usually without having to use code, its to create confusion, compliance and fear (Chamika Hiruni, 2024). Psychological manipulation through the cyberspace is different from traditional cyber attacks because what cyber attacks tend to target are devices, codes, networks; those individuals need technical skills to be able to avoid detection systems and firewalls to exploit

system vulnerabilities. Psychological cyber attacks are the most dangerous because of the flaw of human nature in itself. Human error is the highest cybersecurity risk, according to IBM from 2023's Data Breach Investigations Report that was published by Verizon, human error has caused 74% of the breaches which also points out that phishing scams are responsible for 41% of the incidents (Labs, 2024)**.** This shows how easily a threat actor could take advantage and be emboldened by this statistic and really cause damage to individuals and organizations and cost millions of dollars. Even though malware can sometimes be traced back to whoever developed it or what state actor caused the attack, with social engineering like attacks, attackers use proxies, fake names, botnets, and sometimes deepfakes on others to make them untraceable. These behavioral focused type attacks can be scalable and cheap, already being weaponized by Russia China, Northern Korea and Iran through non-state actors to create an overall distrust within Americas own countries politics with the bots they send out for disinformation purposes through the social engineering they commit in mass. For example, the "Russiagate" is the Russians interfering in the presidential election by using social engineering to influence the presidential election. Russian intelligence agencies, specifically the GRU, used phishing attacks targeting individuals within the democratic party that granted attackers access to many emails within the democratic party. During the DNC the attackers sent malicious links to staff members that also exposed sensitive information. Russia also assisted in the large amount of influx of information across the social media platforms at the time, which has created the term 'fake news', and which that could have influenced voting behavior, targeting specific demographics that would help bolster support for Trump (Boyd-Barrett, 2018). Overall, this was a great example of how social engineering can sway or incentivize certain events to take place for a threat actors' agenda or to create chaos.

Social engineering are very broad types of behavioral attacks that often use emotions like abusing trust by impersonation of contacts or organizations, another is fear where you threaten someone as a high authority to suspend someone's account, curiosity like free rewards if you click a link. Sometimes abusing these emotional cues override rational thinking and create victims to act in a way that can help the threat actor achieve their goals. Social engineering doesn't need as much technical skill but better understanding of human behavior. The type of attacks that are used digitally are phishing which is sending email or messages to induce individuals to reveal personal sensitive information, another is baiting false promises, and pretexts of false scenarios to make victim perform certain actions (Labs, 2024). Physically there are ones called tailgating where you exploit your surrounding environment to gain physical access to a restricted area through someone who has legitimate access, and another example is dumpster diving to find sensitive information to gain access to an infrastructure or gain personal sensitive information for the threat actor to use to their advantage. One major example that happened in 2020 was the major Twitter hack in July. The hacker took over a hundred high profile twitter accounts like government officials and CEOs of massive companies. He used these accounts to post bitcoin scams where the hacker wrote manipulative messages where the high-profile accounts would give back to the community if people sent their bitcoin to the address under their tweet (Witman & Mackelprang, 2022). The hacker got their way because he social engineered the employees by posing as coworkers and calling twitter at help desk, once he privileges escalated, he used the admin tools to reset the two-factor authentication, and reset email addresses to take over the accounts, all because of human error (Witman & Mackelprang, 2022). This caused a major lock down within twitter and this brought congressional hearing about concerns on serious insider threats, access controls and weaponization of social engineering that caused this mess in the first place. While ransomware is

usually seen as just a technique-based attack, but the most successful attacks are when it relies on social engineering for initial access, which makes it a hybrid of using both technique and social engineering techniques. Ransomware was used when Vegas was attacked by a group called scattered spider, an affiliate of ALPHAV, who destroyed massive amounts of precious data and slowed down the casino's websites causing millions of dollars of damages and damaged their reputation as a company as they also paid ransom for these hackers too (Weisman, 2025). If these attacks are happening to these big corporations, imagine the attacks that are being inflicted to nation's governments everyday that try to be successful.

AI has been a big proponent to support psychological warfare to be the most dangerous weapon as its capabilities are vast and terrifying. Threat actors use ai to generate media using AI to upload all across every type of social media that exists to create an audience or group that does not exist or is not that widely supported (Taddeo & Floridi, 2018). With AI creating these false pretenses it can make people believe that there is something there is not, creating a wide paranoia and distrust. This issue only deepens when AI deepfakes became much easier to create where it has been used to create false narratives or to incite violence, this tactic could be sed to create infighting, so it gives either state actors or threat actors time to commit their agendas. Another way for deepfakes to cause massive destruction is to use deepfakes to cause wars by using audio of a leader speaking for such acts, there are so many potential threats to what it can be used for that could cause chaos. Social engineering attacks are being militarized by state-sponsored hackers to collect personal data to build psychological profiles, with these it's used to blackmail, and manipulate key individuals in powerful branches of military, intelligence and political positions. For example, The U.S faced breach within Office of personnel management which is the agency responsible for managing government employee records. This attack was caused by a hacker group

that is affiliated with the Chinese government that carried out a major cyber-attack, stealing millions of people's sensitive data within the government of all formal current and future employees, taking biometric data with each individual's background checks which is extremely invasive (Gootman, 2016). This is prime evidence of psychological warfare to use the personnel of others to manipulate with coercion for the state-actors to get their way, in this instance, China's agenda fulfilled.

Humanity being flawed makes psychological manipulation effective. It works because of how threat actors use established principles from psychology to get their way. Cognitive bias are shortcuts within the mind to decide fast, threat actors use this to exploit victims. Abusing confirmation bias which essentially is to lead individuals to seek out and accept information that they already believe in (Cialdini & Goldstein, 2002). Authority bias is also abused where it makes people follow instructions from a perceived figure of authority, for example threat actors impersonating CEO's and IT admins (Duygu Güner Gültekin, 2024). With the scarcity principle as well when it comes to panicking the user like a time limit before losing your account. Sometimes threat actors use emotional cues with these cognitive biases to manipulate someone like fear, shame, and curiosity, these emotions usually pass by logical thinking and causes an individual not fully think through their decision that is decided to be made especially when there's a perceived idea or fact set in place that others have done the same thing as well (Montañez et al., 2020). Social engineering works not because its technical, it's because of how it uses human behavior against itself, supporting why this tactic of cyberwarfare is becoming more popular, and has shown an abundance of results in the digital age. No matter how strong technical defenses can be, even though they're essential, the issue is that all that can be passed through from just human error. As threat actors keep improving at crafting convincing narratives to exploit individuals, there need to

be improvement in training for being more aware of emotional states, behavioral training and policy literacy.

With digital psychological warfare in the cyberspace becoming more prominent, there needs to be more effective countermeasures that can solve both technological vulnerabilities and the human cognition. The most promising defense would be both strong education, AI helping to detect social engineering attempts and cooperation with other countries to prevent these attacks from happening. The first that needs to be focused on is decreasing the possibility of human error with engaging and fulfilling training modules that are adaptive to the evolving offensive strategies that threat actors are using in present day, including examples of these attacks would give employees better judgement on how to react when dealing with one of these attacks. Having detection systems like UBA systems in place when a person becomes the human error can help nip the bud of any threat actor from privilege escalating to control a digital infrastructure of a organization (Ghafir et al., 2018). If threat actors are using AI to commit these social engineering attacks, it is best that defenders use AI as well to defend against phishing through their machine learning algorithms (Montañez et al., 2020). AI is also being used to detect deepfake software, essentially what is happening with AI is an arms race of who can use the better version of what to get their agenda accomplished, and there needs to be constant refining to prevent threat actors from breaking down defenses (Taddeo & Floridi, 2018). Having stronger policies within governance and better policies in place can really help create guidelines for companies to figure out how to train their employees. Policies is a foundation that helps induce innovation for better defense mechanisms and creates incentives since it helps prevents companies and organizations from losing millions from attacks and vulnerabilities. Disinformation is becoming a dangerous cancer that needs AI detection to be able to debunk them immediately, so it does not create a fog where

infighting is created within and creates an opening for attacks to be taken place (Ghafir et al., 2018). Combating cyber warfare requires a multi-layered strategy of defense. Even though software solutions are important, humans are still the greatest vulnerability and are also the most powerful line of defense, creating digital literacy with strong emotional resilience, and with great policies will make these intimidating social engineering threat actor attacks to become measly distractions.

Even with all of our technology becoming sufficient with the many safeguards in place and advanced detection, threat actors and state actors overall are more focused on mastering psychological warfare as it focuses on the weakest link which is humanity's tendency of human error. From phishing emails and ransomware attacks to massive disinformation propaganda and campaigning through deepfakes, shows that culturally we have tunnel visioned on the intricacies of software vulnerabilities instead of human improvement on being able to detect and preventing to be victims to social engineering. Psychological warfare has been around for centuries, it is just in a new form of the digital era, and with its trajectory of growth, cybersecurity has to evolve to keep up with the offense that the attackers keep pushing towards nations and organizations by realizing that psychology is more integral to cybersecurity than most would perceive. If these attackers keep being underestimated, its not just society at risk from losing data to breaches, it is going to be breaches of trust, stability of civilization and integrity in democracies across the globe. The future is not just defending devices and networks, but its also improving humanities psyche against manipulation.

References

Boyd-Barrett, O. (2018). Fake news and “RussiaGate” discourses: Propaganda in the post-truth era. *Journalism*, *20*(1), 87–91. https://doi.org/10.1177/1464884918806735

Chamika Hiruni. (2024, November 2). *Psychological Warfare in the Digital Age: The Role of Cyber Operations in Modern PsyOps*. ResearchGate. https://doi.org/10.13140/RG.2.2.34079.37283

Cialdini, R., & Goldstein, N. (2002). The science and practice of persuasion. *The Cornell Hotel and Restaurant Administration Quarterly*, *43*(2), 40–50. https://doi.org/10.1016/s0010-8804(02)80030-1

Duygu Güner Gültekin. (2024). Understanding and Mitigating Authority Bias in Business and Beyond. *Advances in Human Resources Management and Organizational Development Book Series*, 57–72. https://doi.org/10.4018/979-8-3693-1766-2.ch004

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*, *74*(10), 4986–5002. https://doi.org/10.1007/s11227-018-2337-2

Gootman, S. (2016). OPM Hack: The Most Dangerous Threat to the Federal Government Today. *Journal of Applied Security Research*, *11*(4), 517–525. https://doi.org/10.1080/19361610.2016.1211876

Labs, K. (2024, October 14). *Top 40 Phishing Statistics and Trends You Must Know in 2025*. Keepnet Labs. https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know

Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, *11*(1). https://doi.org/10.3389/fpsyg.2020.01755

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature*, *556*(7701), 296–298. https://doi.org/10.1038/d41586-018-04602-6

Weisman, S. (2025, March 12). *MGM Ransomware Attack Settlement Is Reached*. Forbes. https://www.forbes.com/sites/steveweisman/2025/03/12/mgm-ransomware--attack-update/

Witman, P., & Mackelprang, S. (2022). The 2020 Twitter Hack -So Many Lessons to Be Learned. *Research and Practice Journal of Cybersecurity Education, Research and Practice*, *2021*(2). https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1089&context=jcerp