SOCIAL ENGINEERING IMPACTS ON GOVERNMENT ACQUISITION

Kathleen Hyatt, Zachary Levenson

The MITRE Corporation

October 2022

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

TABLE OF CONTENTS

1. Executive Summary 1
2. Definitions 2
3. Introduction 2
4. Background 2
4.1. Lifecycle of a Social Engineering Attack 4
5. Social Engineering Attacks 6
5.1 Cognitive Exploitation 6
5.2 Principles of Influence 6
5.3 Operational Social Engineering Attacks 7
5.4 Emerging Technology Integration and Autonomous Execution 12
5.5 Implications of Human Error in the Context of Emerging Technology 12
6. Impacts on Procurement from Social Engineering Attacks 13
7. Indirect Losses to the Government 14
8. Recommendations 14
8.1 Defensive Factors and Vulnerabilities 15
8.2 Active Defense Measures and a Proactive Approach 17
9. Conclusion 19
Appendix A: Acronyms 20

Special thank you to our editors Patrick Staresina and Adam Bouffard.

1. Executive Summary

Information is valuable. Knowledge is power. Because of the utility of information, those with ill intent work with steadfast discipline to extract data from those with privileged access through a variety of means. Sensitive information that is collected can be used as intelligence by nation state adversaries, it can enable fraudulent financial activity, and it can be deployed to interfere, influence, and disrupt sovereign national activities. Privileged access can also be leveraged—even without theft of information—as an avenue through which actors can travel to attack computer systems in kinetic ways (e.g., overspinning a centrifuge in a nuclear facility causing them to self-destruct) to disrupt U.S. government (USG) operations, damage equipment, or even harm personnel. Therefore, information security is vital to prevent an adversarial advantage on multiple fronts and to ensure the security of U.S. and allied personnel and assets. Government employees can be unknowingly manipulated to provide valuable information and access to harmful actors which can cause varying degrees of damage in multiple areas. This paper highlights ways in which social engineering attacks can be used to manipulate the government acquisition ecosystem to detrimental effect.

Social engineering activities are prevalent within the government acquisition community because so much of the labor is not automated, and therefore relies on human actors. For instance, as a part of most government acquisition operations, there is an individual Contracting Officer (CO), an industry official, and additional unsuspecting support staff who can potentially be manipulated to facilitate unauthorized access and/or fraudulent activity. This can happen to anyone and can vary in severity. The purpose of this paper is to educate practitioners and provide threat mitigation recommendations to the government acquisition community.

Note that many elements of social engineering as a discipline of adversary activity overlap with traditional Human Intelligence (HUMINT) and Cyber-HUMINT tactics, techniques, and procedures (TTPs); however, for the purposes of this paper and audience, prospective distinctions and similarities between these various categories of operations will not be called out. Additionally, for the sake of clarity and consistency of lexical terms used, this paper will focus on the concept of social engineering in the context of information security.

There are central themes to many social engineering attacks, and many attacks are conducted using a hybrid approach combining one or more of the types of attacks outlined in section 5.3. Knowing that anyone can become a victim, this paper recommends both proactive offensive approaches and defensive approaches to counteract the attempt at manipulation in the hopes of minimizing vulnerabilities in government acquisition and preventing the loss of information and millions of dollars.

.

2. Definitions

For the purposes of understanding this document, the following terms are defined to clarify intent and scope.

Social Engineering: The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.[1]

Government Acquisition: The act of acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the federal government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated.[2]

3. Introduction

Social engineering is increasingly becoming a problem for the USG. Even as there are advances in technology that create more secure online and offline operating environments, a significant vulnerability continues to be the human factor. Social engineering is the activity of attempting to manipulate users or employees to either reveal sensitive data, obtain unauthorized access, or unknowingly perform fraudulent activity. The USG is not immune to this issue and has lost hundreds of millions of dollars over the last decade due to social engineering attacks as detailed below.

This paper addresses the impacts that social engineering can specifically have on USG contracting and acquisition such as threats to the supply chain and deepfakes. Recommendations will also be made for how agencies can both recognize and prevent social engineering attacks from occurring, thus preventing damage, disruption, compromise, and the loss of resources.

4. Background

Adversary-directed threats to U.S. systems, information, and personnel—including HUMINT operations, cyber attacks, signals intelligence collection, and cyber-enabled espionage—have long plagued the Western national security enterprise. However, as the overarching rise of technology in society widens the attack surface on which adversaries can conduct operations, social engineering as a threat has also evolved in conjunction with these larger changes. In today's operational context, social engineering can manipulate a plethora of individuals and technical access points to facilitate the fraudulent provision of information, the success of a network intrusion, and/or the execution of an influence, interference, or kinetic operation. Where cyber attacks center on infrastructures and networks, social engineering attacks focus on the actors who control and access those networks.

Humans remain an unpredictable variable in maintaining cybersecurity, and therefore, are a common target for attackers. Technical attacks are typically easier for information security and counterintelligence (CI) entities to plan for given that these processes are often repeatable and predictable. However, it is much more difficult for human activities to be seen as reliably consistent in terms of TTPs because where computers and infrastructures might be the same, no two humans behave, react, or think in precisely similar ways. Where one person might be able to anticipate and recognize a social engineering attack, a different person might perceive an attacker's intrusion attempt to be an innocuous or friendly act and thereby unknowingly allow the attacker to access the information they seek.

[1] National Institute of Standards and Technology (NIST) Digital Identity Guidelines. Special Publication 800-63-3

[2] Federal Acquisition Regulation (FAR) Part 2.101

"SOCIAL ENGINEERING ATTACKS ARE TYPICALLY MORE PSYCHOLOGICAL THAN THEY ARE TECHNOLOGICAL. INSTEAD OF USING SOPHISTICATED HACKING TECHNIQUES OR IN-DEPTH KNOWLEDGE OF COMPUTERS, THEY RELY ON TRICKING PEOPLE INTO GIVING AWAY INFORMATION. CYBERCRIMINALS THAT ENGAGE IN SOCIAL ENGINEERING ARE DIGITAL CON ARTISTS, GAINING VULNERABLE PEOPLE'S TRUST TO STEAL MONEY OR DATA EASILY."[3]

Another reason that social engineering TTPs are growing[4] in popularity with attackers is that they are generally perceived by users to be low-cost, high reward tools within the larger kit of computer exploitation options. For example, it might unnecessarily burden a given Advanced Persistent Threat (APT) group to design a complex, highly surreptitious, and deeply intrusive malware delivery package when a simplified socially engineered mass malware spam campaign can achieve the same objective of initial network access. Additionally, using social engineering techniques to gather information about a user could make it much easier and faster for that attacker to ascertain a user's password to access the system. In these cases, it often doesn't matter how sophisticated the security guarding the network is, if the attacker is able to target the user and manipulate them into giving away credentials without realizing what they're doing.

While social engineering operations can result in gathered reconnaissance information that can then feed and shape the design of a network intrusion set, there is a prospective cyclical nature to many of these operations where the data gathered from a network intrusion can then feed additional tailored social engineering manipulations should the adversary wish to gain access to other hardened networks. That said, the sheer depth and breadth of publicly available online information sometimes eliminates the need for any intrusion set to precede a social engineering operation; this is because attackers can take commonly accessed information and twist it in a way that is advantageous for them. Simply put, social engineering attacks can take many forms depending on the context and needs of the attackers. This threat is especially present in the government acquisition arena. For example,

[3] D. Partida, "Social Engineering Cyberattacks and How They're Affecting Businesses." Security Infowatch (December 2020) https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses

[4] L. O'Reilly, Social Engineering Threats Rose 270% in 2021 – Indicating a Shift to Multi-Channel Phishing Attacks as Apps and Browsers Move to the Cloud." Slashnext. (October 2021). https://www.slashnext.com/blog/social-engineering-threats-rose-270-in-2021-indicating-a-shift-to-multi-channel-phishing-attacks-as-apps-and-browsers-move-to-the-cloud/

> "…the fact that GovCon Co. is a prime contractor on a certain Government contract is generally available to the public; a press release, website news item, social media profile, or other public information may show that Subcontractor Co. is a subcontractor to GovCon Co. on that prime contract; and a simple LinkedIn or Facebook search may reveal that John Smith is a contracts manager or billing representative for Subcontractor Co. A fraudster need only create a domain and email address such as 'jsmith@subocntractorco.com' to facilitate his or her scheme. Many individuals, when processing invoices, may not notice the misspelling in the domain name. They simply changed the bank account information and issued payment. The result? Hundreds of thousands of dollars in losses, and limited recourse to recover what was lost."[5]

In fact, there are many examples of acquisition social engineering attacks that do not involve cyber intrusions at all. An example occurred in North Carolina in 2019 when the state government lost over $1.7M to a social engineering scheme. The government office was approached by what appeared to be a legitimate contracting business hired for the construction of a school. They possessed allegedly valid licenses and all the required paperwork needed to establish an account and have funds transferred. The fraudulent actors were able to create such accurately forged papers because of publicly available information gathered on similar legitimate businesses. Possessing this convincing cover, the threat actors were then able to gather privileged information that enabled the theft of funds. The county in which this social engineering attack occurred was very clear to state that this was not a cyberattack, and the loss of funding was the direct result of an unintentional information leak. "The county was not hacked. It was not a cybersecurity [incident]. This is a case of a spoofed identity in which somebody posed as a vendor, provided seemingly valid documentation and signed approvals."[6]

4.1 Lifecycle of a Social Engineering Attack

Social engineering has continued to grow as a persistent threat to U.S. businesses and government entities over the past decade. As the attacks have grown in frequency[7], so has the understanding of how these attacks typically arise and evolve over time. As seen in Figure 1, researchers now depict and organize social engineering attack techniques into four phases of adversary execution:

1. **Investigation** – The initial stage in which the attacker already has an intended goal in mind and selects their victim(s). Once they know their target, they begin gathering background information (oftentimes information that the target has already released willingly through open channels) and decides on their preferred attack method (discussed further in section 5.3).
2. **Hook** – The stage where the initial interaction with the target occurs in the effort to gather the needed information. This includes preparing a cover story if needed and knowing how to maintain control of the interaction to ensure the needed information is successfully obtained.

[5] P. Mazza & M. Feinberg, "Social Engineering Fraud: 4 Steps Every Company Needs to Take Right Now." (May 2020) Social Engineering Fraud: 4 Steps Every Company Needs to Take Right Now | PilieroMazza PLLC - JDSupra

[6] L. Ropek, "Social Engineering Attack Nets $1.7M in Government Funds" Government Technology (August 2019) Social Engineering Attack Nets $1.7M in Government Funds (govtech.com)

[7] O'Reilly, 2021

Figure 1: Lifecycle of a Social Engineering Attack

3. **Play** – The stage in which execution and continuation of the socially engineered manipulation occurs; this is where humans are influenced, coaxed, pressured, or unwittingly fooled into provide sensitive information or access. The duration of this stage can be long or short, depending on the type of social engineering attack used, but implies that the attacker will have the patience to play the long game and will engage with the target multiple times if needed. In some cases, the attacker might even use multiple techniques to gather as much valuable information from the target as possible.
4. **Exit** – The final stage in which the attacker generally ends the interaction with the victim in a natural way so as not to arouse any suspicion.

This social engineering framework allows for the threat actor to cycle back into stage one for further investigation and manipulation should the adversary require additional information not gathered during the previous engagement(s).

Using the steps in the social engineering attack lifecycle, the attacker is able to retrieve all of the information they need without the target being aware that they have divulged valuable information. The target's lack of awareness about their own inadvertent support is what makes these targeting techniques so dangerous.

5. Social Engineering Attacks

5.1. Cognitive Exploitation

Procurement and acquisition play an essential role in a majority of government projects, and it should not be overlooked that social engineering activities can negatively affect this foundational element of the defense enterprise. Social engineering attacks are uniquely targeted at the human decision-making process. As Sherman and Arampatzis discuss in their article "Social Engineering as a Threat to Society," the biggest challenge that makes humans (and therefore government employees) susceptible to social engineering attacks are cognitive biases.[9] Cognitive biases refer to the ways that humans process information and how decisions are affected. Not everyone interprets information in the same way, and therefore it can be difficult to predict how humans will react in a given situation. Social engineering attackers capture this reality and use it to their advantage when collecting information from targets.

An example of this this cognitive bias is the tendency for the human brain to group similar memories or repetitive actions together, to the point where the brain almost goes into autopilot. If you read the previous sentence again, you may notice that an additional "this" has intentionally been included as a display of this bias in action. For many, the brain has self-corrected the error without registering that an additional word was present. Biases like this could impact contract and acquisition activities because it is a field where similar processes are repeated over and over, and it becomes possible for smaller and inaccurate details to go unnoticed. As previously mentioned above, attackers can emulate domain names, email addresses, and other information easily based on information that is gathered electronically. An example could be processing invoices in a system, which Contracting Officer Representatives (CORs) must do quite often. The repeatable process begins to put the COR on autopilot and the COR could easily overlook pertinent information and submit payment to an attacker through human error. The social engineers who are looking to conduct attacks are aware of this and are prepared to take advantage as best they can. As discussed later in Section 8, this is one area where advanced technological aids (particularly those relating to artificial intelligence-enabled "suspicious activity" detection) can be of particular use in terms of threat mitigation.

5.2 Principles of Influence

Social engineering attacks tend to focus on the exploitable elements of human cognition and behavior in an attempt to manipulate workers. Robert Cialdini identified several of these characteristics in his work, Influence: The Psychology of Persuasion, which he refers to as the six principles of influence. These include:

1. **Reciprocity** – This refers to the tendency of people to return a favor when something is done for them. An example of this can be seen in marketing when businesses offer free samples or trial runs before requesting commitment to buy. An acquisition-salient example of this could manifest as a CO awarding a contract to an industry partner in return for monetary, professional, and/or personal benefits.
2. **Commitment and Consistency** – Commitment can be a powerful motivator and refers to the fact that once people say they are going to do

[9] J. Sherman and A. Arampatzis. "Social Engineering as a Threat to Society". (July 2018) https://www.realcleardefense.com/articles/2018/07/18/social_engineering_as_a_threat_to_societies_the_cambridge_analytica_case_113620.html

something, they feel personally obligated to ensure it is completed. Sometimes they will continue with an activity even if the original intent has changed, or if its completion will no longer have an impact. Given that acquisition professionals are, as described later in this paper, often hyper-cognizant of their professional reputation, an example of this principle in action might include a CO prioritizing essential contract actions over good security practices.

3. **Social Proof** – This principle states that humans are more likely to conduct activities that they see others doing. This includes people who avoid being the first person to do something in case it results in failure or issues. An example of this might include the disincentive that a CO has to be the first (and possibly only) individual to identify and call out contract fraud.
4. **Authority** – Most people have a natural respect for authority and those in positions of power, and often reflexively comply instead of questioning the orders given to them by those types of figures. An example of this might include a CO receiving a call from a higher echelon of authority—a Department of Justice official or that CO's supervisor—whereby orders are given to provide sensitive source selection information.
5. **Liking** – This refers to the tendency for people to be more likely to listen to commands and follow directions that come from people that they like. It is easier for people to want to please those they have a higher opinion of; a desire to do one's best to ensure that the other person likes them in return is a related effect. An example of this might include a bad actor impersonating an individual known to be close friends with an influential contract manager in order to sway the requirements and outcomes of given contract awards.
6. **Scarcity** – Lastly, if people perceive that something is scarce, they believe it to be more valuable, and naturally will make more of an effort to obtain it even if that is not true. Scarcity might lead to people buying more items than they actually need or spending more than is necessary to obtain the items. An example of this might include a commercial organization being manipulated to believe that they are likely to win a valuable and highly competitive contract if they provide extensive PII.

All six of the principles of influence create opportunities for staff to be exploited by social engineering attackers. According to the Association of Government Accountants (AGA), there are many ways in which those principles can be exploited, and that staff can be targeted.[10]

5.3 Operational Social Engineering Attacks

Table 1 below shows many types of social engineering attacks and examples of how they can manifest in the operational environment.

[10] AGA, "Social Engineering (accessed December 2021) https://www.agacgfm.org/Intergov/Fraud-Prevention/Fraud-Awareness-Mitigation/Social-Engineering.aspx

Table 1: Social Engineering Techniques and Examples

Social Engineering Technique	Definition	Example
Phishing	As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity, or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.	Ubiquiti Networks, a manufacturer of technology for networking, lost almost $40 million dollars in 2015 after a phishing attack. It is believed that an employee email account was compromised in Hong Kong. Then, hackers used the technique of employee impersonation to request fraudulent payments, which were made by the accounting department.[11] From an acquisition perspective, an example may look like email response to an Request for Information (RFI) that contains a corrupted word document therefore installing malware on to the CO's computer.
Elicitation	A subtle approach used to gather information from users through basic social interactions and research into a user's online and social media presence.	Hackers stole millions of Social Security numbers and thousands of credit and debit card numbers from the South Carolina Department of Revenue in 2012. Employees fell into scams by sharing their usernames and passwords with criminals. After that, with credentials in hands, the hackers gained access to the state agency's network.[12] From an acquisition perspective, an example may look like a CO who is talking to co-workers in a public place, and inadvertently discloses sensitive contract information to a person listening in on their conversation.
Pharming	Redirecting web traffic from legitimate sites to malicious clones/fraudulent IP addresses. This ploy can be leveraged to create fake sites, upload content, monitor traffic, or hack official corporate systems.[13] For example, an attacker can use malicious code to monitor user web activity to trigger a redirect to a spoofed banking site. When a user enters their bank domain into the browser address bar, the pharming code hijacks the user's activity and redirects the browser to an attacker-controlled website with the same look and feel as the official bank account. Users rarely look at the domain in the browser's address bar, so it's an effective attack to steal user financial data, including their credentials.[14]	"A number of news stories have emerged in recent years of corporations being attacked in this way, including instances of official corporate subdomains being hijacked to re-direct to content including malware, pornography, and gambling-related material. Subdomains of the Xerox website, for example, were used in 2020 to drive traffic to sites selling fake goods, taking advantage of the trusted reputation of the official corporate domain to boost the search-engine ranking of the malicious content. In another case in 2019, GoDaddy® shut down 15,000 abused subdomains that drove a massive spam campaign geared towards the sale of counterfeits."[15] From an acquisition perspective, an example may look like a website masking the Wide Area Workflow, the DoD's invoicing, payment, reporting, and contract information portal, would allow an unsuspecting contractor or government official to give proprietary, sensitive, and financial information to a bad actor.
Framing	The tactic used to frame a situation by asking leading questions or phrasing statements in such a way that they focus on the target's unique biological and cultural influences to create a level of comfort and familiarity. That familiarity is then leveraged to manipulate targets into sharing sensitive information or otherwise enabling access to systems.	If an attacker wants to obtain information on a certain type of security device they might ask, "Where can I get some info on security devices?" or, "What resources are there available to help me find information on security devices that can handle XYZ protocols?" If trying to obtain personal information from a secretary who has a family photo out an attacker can ask, "What is your child's name?" That direct question may close the door quickly. The secretary may answer it, but it may not allow for additional inquiry. Whereas "Is this your oldest child?" may elicit not only a positive response, but a plethora of information about other children she may have.[16] From an acquisition perspective, an example may look like a bad actor or curious industry contractor could solicit information from a CO such as source selection information, future acquisitions, or vendor performance to influence stock trading or investment opportunities to enrich themselves.

[11] "Ten Real and Famous Cases of Social Engineering Attacks", Gateby (June 2021) https://gatefy.com/blog/real-and-famous-cases-social-engineering-attacks/

[12] *Gateby*, 2021

[13] D. Barnett, "The World of the Subdomain", Circleid.com (accessed June 2022) https://circleid.com/posts/20220504-the-world-of-the-subdomain#fn5

[14] "What is Pharming?", Proofpoint.com (accessed March 2022) https://www.proofpoint.com/us/threat-reference/pharming

[15] D. Barnett

[16] "Framing", Security Through Education, LLC (accessed March 2022) https://www.social-engineer.org/framework/influencing-others/framing/

Table 1: Social Engineering Techniques and Examples (Cont.)

Social Engineering Technique	Definition	Example
Pretexting	A premeditated attack in which a person constructs an elaborate story to place a user in a tense and urgent situation in which they might disclose information they normally would not disclose. Pretexters can impersonate co-workers, police officers, bankers, tax authorities, clergy, insurance investigators, etc. Impersonating a person of authority or someone with a right-to-know lays the groundwork for applying pressure onto targets which thereby provide needed information. The pretexter must typically prepare answers to questions that might be asked by the victim. Sometimes, an authoritative voice, an earnest tone, and an ability to think on one's feet are all that is needed to create a pretextual scenario.	The most common example of a pretexting attack is when someone calls an employee and pretends to be an individual in a position of power, such as the Chief Executive Officer (CEO) or a staff member on the information technology (IT) team. The attacker convinces the victim that the scenario is true and collects the information that is sought.[17] From an acquisition perspective, an example may look like a CO receiving a call from a person posing as an FBI agent requesting small bits of information on a specific program's vendors to aid in an investigation, which the CO complies with. If the program is sensitive, this information on which vendors are working the program can be used by adversaries to target and attempt to exploit these unsuspecting businesses.
Cold calling/ Vishing	This is the simple act of gathering information by making unsolicited phone calls, sending voice messages, and leaving voicemails as a means to make contact; these acts are conducted in ways that initially seem to amount to insignificant interactions, but small pieces of information about a person gathered separately over time are often combined to form a valuable profile to be used by attackers.	Social engineers can mimic recognizable phone numbers and caller ID names to gain trust. Voicemail recordings, automatic "out of office" replies, and other volunteered information can also be leveraged to collect PII. As a hypothetical example, a social engineer could leverage an "out of office" reply to form the following elicitation email: *Hi Dan, I hope Erica is enjoying her vacation in the Bahamas. Since she won't be back until July 31st, she directed me to you to answer my questions.* A confident opening is all a social engineer needs to appear as a credible source.[18] From an acquisition perspective, an example may look like a CO who is targeted of specific "new" business pitches and their products/solutions where a CO reveals slowly what is interesting to them one product at a time, framing a picture of what the agency may be procuring in the future.
Gaslighting	This technique involves psychologically manipulating a target to the extent that they begin to question their own logic, opinions, and/ or sanity. This is an aggressive technique where attackers will do their best to lie, misdirect, and confuse people into providing information unwittingly in support of a social engineer's operation.	One example involves asking questions with unimportant answers to create the opportunity for the attacker to get aggressive and fluster the employee to the point that they will offer any information they can to attempt to calm down the attacker and end the confrontation. Criminals and foreign actors can use gaslighting to change perceptions, behaviors, and actions. Gaslighting also stifles discussion and dissent because it attacks conviction and surety of a person's knowledge and beliefs. Gaslighting must tear down an individual in order to manipulate and control them.[19] From an acquisition perspective, an example may look like a CO receiving a call from a person posing as a vendor who is requesting confirmation of financial data. The CO may reply that the information has already been sent, but the fake vendor insists that they never received the information and threatens to call their supervisor. This immediately makes the CO question their past actions and resend the requested financial data, giving it directly to the fake vendor.

[17] Nadeem, M.S.,"Social Engineering: What is Pretexting?" Malifence.com (February 2022) https://blog.mailfence.com/pretexting/

[18] "The Top Ten Social Engineering Tactics you Need to Know", Access Systems (October 2019) https://www.accesssystems.com/blog/the-top-10-social-engineering-tactics-you-need-to-know

[19] McGuinness, T. "What is the Purpose of Gaslighting?" LinkedIn (October 2020) https://www.linkedin.com/pulse/what-purpose-gaslighting-tim-mcguinness-ph-d-

Table 1: Social Engineering Techniques and Examples (Cont.)

Social Engineering Technique	Definition	Example
Client/Vendor Impersonation Fraud	This technique involves a social engineer posing as a client or vendor in order to gain sensitive information through a conduit of trust; phishing and other techniques can be used to collect information to build a more sophisticated cover-for-action and cover-for-status.	"An employee receives a phone call from an individual who he believes to be a genuine supplier. The fake supplier advises that his bank details have changed, and payment is to be made to a new account. Going through procedure, the employee advises that the request must be received in writing via email or on company letterhead. The employee later receives an email from what appears to be the legitimate supplier complete with the supplier's signature at the foot of the email. The employee proceeds to change the bank details and a payment is issued. Sometime later, the genuine supplier requests payment, indicating that the original payment was never received. Further investigation will identify that the earlier request was fraudulent." Due to a social engineering and Business Email Compromise (BEC) scam, Cabarrus County, in the United States, suffered a loss of USD 1.7 million in 2018. Using malicious emails, hackers impersonated county suppliers and requested payments to a new bank account. According to the investigation, after the money was transferred, it was diverted to several accounts. In the emails, the scammers presented apparently legitimate documentation.[20] From an acquisition perspective, the above example demonstrates how a bad actor can pose as a legitimate company and target a less seasoned acquisition professional.
Fake Office Fraud	An attack in which the perpetrator will pose as a staff member from an office—usually one of authority—to threaten repercussions; this activity is often combined with a sense of urgency so as to not give the victim time to consider their actions.	"A mid-level finance employee is the only person remaining in the office on a Friday evening when she receives a phone call from an individual who identifies himself as the company's CEO. He explains that a major acquisition is about to take place, but it must close tonight, and he can't get in touch with anyone else on the finance team to process the payments. The employee explains that she only has authority to transfer funds of up to $50,000 and that no one else is in the office to countersign the transfer. The CEO grows increasingly irate with the employee for refusing to transfer the funds because she does not have the authority. He repeatedly tells her that he's granting her the authority. Eventually the CEO persuades her to circumvent the established procedure by issuing multiple $50,000 transfers totaling $500,000."[21] From an acquisition perspective, an example may look like a CO receiving a call from someone posing as the Office of the Inspector General, suddenly forcing them to reveal source selection material or proprietary information.
Funds Transfer Fraud (FTF)	A type of social engineering attack in which government agencies think they are doing business with a legitimate company, when in actuality they are sending funds directly to attackers.	FTF (aka BEC) has become a very popular form of social engineering attack given that if the targeted business does not have the proper protocols in place to verify the legitimacy of the vendor, they can potentially send large payments, once or even several times, resulting in significant losses. "According to the Federal Bureau of Investigation (FBI)'s 2019 Internet Crime Report, complaints revealed an uptick in BEC scams by a considerable margin. The FBI found BEC to be the most damaging type of cybercrime in 2019. BEC losses averaged $75,000 per complaint, phishing, smishing, and vishing accounted for $500 per complaint, and ransomware averaged $4,400 per complaint."[22] From an acquisition perspective, an example may look like a CO receives an unsolicited bid from someone posing as a vendor advertising a scare resource. Due to the need for services during an urgent and compelling situation, the CO fails to verify the legitimacy of the vendor.

[20] *Gateby*, 2021

[21] Arthur J. Gallagher & Co. "Social Engineering Fraud" (accessed December 2021) https://www.wasb.org/wp-content/uploads/2017/04/20161219_ajgallagher_social_engineering_fraud.pdf

[22] Cyber Armada, "Social Engineering Threats to the Supply Chain During COVID-19." (accessed December 2021) https://blog.cyber-armada.com/articles-and-resources/social-engineering-threats-to-the-supply-chain-during-covid-19

Table 1: Social Engineering Techniques and Examples (Cont.)

Social Engineering Technique	Definition	Example
Lawyer Impersonation	This technique involves a social engineer posing as an attorney or legal figure in order to gain sensitive information through a conduit of trust and often urgency; phishing and other techniques can be used to collect information to build a more sophisticated cover-for-action and cover-for-status.	"An employee receives a phone call from someone posing as an attorney and claiming to be handling confidential or time-sensitive information. These scammers typically initiate contact at the end of the business day or work week to coincide with the close of business of international financial institutions."[23] From an acquisition perspective, an example may look like receiving a fake data request from the agency legal office or the Government Accountability Office, and fulfilling the data call, which gives away trade secrets, proprietary information, or source selection information.
Deepfake Deceptions	The use of "synthetic media" enabled by artificial intelligence to simulate a specific person's appearance and/or voice via video or audio recording; this can be used to deceive victims into divulging information or performing an action.	In 2019, a fake recording of a CEO's voice was used to instruct an employee to transfer money to an international account. "The recording was left as a voicemail to the subordinate, who obeyed the fraudulent instructions and sent $243,000 to the attackers."[24] From an acquisition perspective, an example may look like a CO receives a phone call from a bad actor using a synthetic voice manipulator to pose as the director of their department, requesting the immediate purchase of a specific item that can only be found on one website. Due to the low value of the product, which is below the micro-purchase threshold, no approvals and little documentation is needed, handing the money directly to the criminal.
Browser Notification Hijack	A technique whereby social engineers insert notification script, malware, and/or influential messaging into web browser or website notifications; this requires that the target be convinced or manipulated into "allowing" notifications (e.g., engineers can disguise subscription consent as another action, they can switch the "accept" and "decline" buttons on subscription alerts, etc.).	According to a Review Geek publication in March 2022, an affiliate of the website outlined what was perceived to be a pop-up computer virus pretending to be anti-virus software; however, these messages were actually malicious browser notifications from a website and as such, could not be removed with legitimate anti-virus software.[25] From an acquisition perspective, an example may look like a CO's weekly check of the file transfer where status reports are uploaded by contractors suddenly offers to push notification when a new file is submitted. When the CO clicks yes to save time, malicious code is downloaded onto their computer.
Additional social engineering techniques not mentioned in detail include: Spear phishing, Vishing, Whaling, Smishing, Baiting, Piggybacking/Tailgating, Quid Pro Quo (i.e., tech support scams), Honeytraps (deceptive and/or false romance scams), Scareware, and Watering Hole attacks. The FBI's 2021 Internet Crimes Report showed that "phishing (scams via email to induce recipients to share sensitive information) vishing (voicemail phishing), smishing (SMS text phishing) and pharming (using malicious code on the victim's device to redirect to an attacker-controlled website) were the top forms of cybercrime in 2021."[26]		

[23] Gallagher & Co. (December 2021)

[24] D. Slater. "7 New Social Engineering Tactics Threat Actors are Using now" csoonline.com (accessed June 2022) https://www.csoonline.com/article/3613937/7-new-social-engineering-tactics-threat-actors-are-using-now.html

[25] A.Heinzman " That computer Virus you can't Remove might be a Browser Notification" reviewgeek.com (accessed August 2022) https://www.reviewgeek.com/111106/that-computer-virus-you-cant-remove-might-be-a-browser-notification/

[26] R. Watson. "Cyberattacks are Gaining Momentum" Grand Rapids Business Journal (accessed June 2022) https://grbj.com/news/technology/cyberattacks-are-gaining-momentum/

5.4 Emerging Technology Integration and Autonomous Execution

With the advancement of artificial intelligence (AI), machine learning (ML), and Internet of Things technology, many emerging and aforementioned social engineering techniques have the power to be partially or fully automated from end-to-end giving rise to a compounding threat of "social engineering at scale" with significantly fewer human resources burdened to execute operations. Examples include attackers training AI and its algorithms to target specific types of files so that they can hone in on the metadata of these files. Reporting on how ML can be leveraged to bolster the toolkit of cyber-criminals notes:

> **"As in the case of phishing or infection preparation, hackers may use the [machine learning] classifying algorithms to characterize a potential victim as belonging to a relevant group. This means that after having collected thousands of emails, a hacker sends malware only to those who would click on the link. Thus, the attacker reduces the chances of early detection of the planned attack. Numerous factors may assist here. For example, the hacker can separate the users of social networking sites who write about IT from those focused on "food-and-cats" topics. The latter group might be unaware of threats. Various clustering and classification methods from K-means and random forests to neural networks can be used in this case on top of the [natural language processing] (NLP) analysis, which should be applied to victim's posts on social networks."[27]**

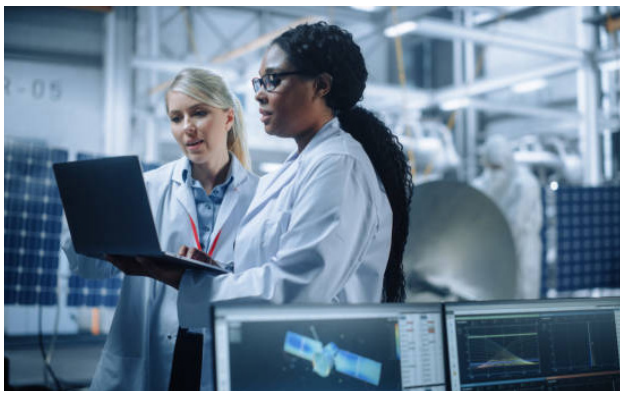
AI-enabled chatbots—often leveraged by IT help desks—can also be turned around by social engineers to seek out and extract sensitive PII from customers in need of technical assistance; in this way, an illegitimate chatbot posing as one tied to a legitimate business could be deployed at a target to extract data, but it is also possible that social engineers could pose as the very target they seek to extract data about when speaking to legitimate chatbots and use collected PII to access account information through the authentic automated help desk. In so many ways, bad actors' opportunity for operational growth in this area is dangerously promising.

5.5 Implications of Human Error in the Context of Emerging Technology

Social engineering techniques center around the unpredictable (e.g., difficult for bureaucracies to systematically mitigate) and malleable (e.g., exploitable) actions of humans, and one unavoidable fact is that humans tend to make mistakes. It does not matter if the mistakes are large or small, it only matters that social engineering attackers know that if they can create the right circumstances, they can increase likelihoods that humans will make the kinds of mistakes that will benefit their agenda. This likelihood expands sufficiently when social engineers attack in numbers (all it takes is one human's error to open the network's flood gates) and those numbers expand dramatically when enabled by advanced technology that pushes the social engineering operational tempo to an exponential scale. Spoken more bluntly, if 50,000 targets are attacked within one government agency every day (a scale potentially to be enabled by AI/ML tools) with social engineering techniques that are programmed to change and enhance themselves as neural networks learn more about the targets' interests, habits, and behaviors (purposed to exploit the varying possible weak

[27] A. Polyakov "Machine Learning for Cybercriminals 101" towardsdatascience.com (accessed June 2022) https://towardsdatascience.com/machine-learning-for-cybercriminals-a46798a8c268

points among human cognition within the target population), the likelihood that at least one attack will succeed is not just high, it is oftentimes all that is needed for operational success and security disaster. For example, an employee can be trained to recognize a fraudulent email and phishing attempt that instructs them to "click this link for more information." However, under the right situation where the employee is pressed for time due to multiple deadlines and when emails stress the urgency with wording such as "this must be done immediately," the employee is more likely to make the mistake of clicking the link and opening a connection for the attacker. This is especially prevalent in acquisition as contracting professionals always have more work than time and are often working under extremely tight deadlines and heavy amounts of stress. Prognostic horizon analyses—and even diagnostic assessments of the more current threat—would not be sensational if they articulated that the threat was compounded by the prospect that new technologies are significantly increasing the quantity of human targets that can be hit (and the rate at which they can be attacked) therefore raising the threat level in unprecedented ways.



6. Impacts on Procurement from Social Engineering Attacks

Another unique impact to businesses and government agencies that affects procurement activities is the loss of reputation. In procurement, reputation and past performance play a critical role in how many other businesses will want to engage in partnerships and relationships with a given entity. If a business entity is consistently unable to defend against social engineering attacks, it could cause them to lose future contract awards. "Perhaps the most damaging side effect of any data breach is a tarnished reputation. A Ponemon Institute study found that 65% of surveyed consumers lose trust in a business after a data breach. Furthermore, 27% ended their relationship with a company, and stock prices fall an average of 5% after a breach."[28] Social engineering attacks are dangerous because even if the monetary damage done to the business is small, the impact to a damaged reputation and future business lost can be severe. Since government agencies frequently rely on contractors to achieve their missions, contractors who have access to secure government assets are consistently vulnerable. If a contractor is impacted by a social engineering attack, it may have an adverse effect on the future government acquisitions and procurement process as well as put the mission in jeopardy. Additionally, disruptions to existing business relationships with contractors add to the overhead acquisition cost and make for a less efficient and more costly acquisition ecosystem. For example, losing a contract relationship due to social engineering attacks necessitates remedial market research to identify and select a new contractor, as well as follow-on contractor vetting, contractor surveillance, and training of new contractor staff.

[27] Partida, (December 2020)

7. Indirect Losses to the Government

In addition to the threat of losses from direct social engineering attacks, indirect effects can be seen in supply chain disruptions which can have sizable downstream impacts on government operations. Mainly, due to the sheer number of contracts and operations that large businesses and government agencies interact with to purchase services and supplies, there is an increased likelihood of feeling the effects of social engineering attacks either by direct intrusion or by second- and third-order proxy. Because there are so many variables, there is a greater chance that somewhere down the supply chain, there is a vulnerability that can be exploited. Once one company in the supply chain is impacted, those effects can be seen by all other companies who do business with the exposed entity.

8. Recommendations

Awareness is a primary challenge in social engineering attacks. However, so is the need to defend personnel, networks, and assets with techniques that match or outgun the sophistication of emerging social engineering attacks; to do so would be to act on the advice of counterintelligence/cybersecurity professionals and leaders that have historically been tasked with defending against tier-one threats to the U.S. defense enterprise. In order for acquisition staff to make efforts to prevent these social engineering attacks, they need to first be made aware of the threat and the ways in which they might be vulnerable.

As mentioned above, the biggest challenge with addressing social engineering prevention is the vast differences in staff, i.e., a static set of techniques for making staff understand and prevent these attacks will not work for everyone. Some factors that must be included when developing different training processes include the employees' skill level, time in the work force, and internet usage[29]; managers can go further to include factors such as trending attack techniques, promotion incentives or rewards for thwarted attacks, creative engaging "war game" exercises, and/or more flexibility provided to staff for detecting threats despite project deadlines. These are all factors that can impact someone's understanding, concern, and applicability of social engineering prevention measures. These factors have been broken into two categories, defensive/vulnerabilities and offensive/proactive.

[29] H. Aldawood, T. Alashoor & G. Skinner. "Does Awareness of Social Engineering Make Employees More Secure?" International Journal of Computer Applications" (February 2020) https://www.ijcaonline.org/archives/volume177/number38/aldawood-2020-ijca-919891.pdf

8.1 Defensive Factors and Vulnerabilities

Defensive factors should be implemented to ensure that staff and systems at any business or government agency are well postured to recognize social engineering attacks, know how to prevent them, and know what to do if an information leak should occur. The acquisition community is inherently outward facing because they are the bridge between industry and the government. This makes them a unique target because of their need to interact outside the cyber-security perimeter of the government, their publicly available contact information, and their access to sensitive information. The following factors should be addressed and researched to ensure the best chance of repelling and identifying a social engineering attack:

- **Security Skill Level** – The degree to which the acquisition professional is familiar with common security practices and procedures. When assessing an employee's security skill level, the government or specific agency may tailor training processes after asking:
  - Does the employee have the ability to determine whether something doesn't seem right? If so, do they know how to appropriately respond?
  - Does the employee have a USG security clearance? Those with a clearance are more likely to think twice about engaging in risky behavior due to the additional training related to counterintelligence, manipulation, and risks associated with doing cleared work. Those without a clearance may need more in-depth training.
- **Time in the Work Force** – An employee's level within the company (e.g., entry-level, journeyman, or senior) could also be a factor as they will have different levels of responsibility and familiarity with established policies and procedures. For example, some employees who have been through years and years of training may be less likely to pay attention to new security measures because of the belief that they don't need to learn anything new. Alternatively, some experienced employees may, because of that practical wisdom, be postured to recognize common schemes deployed at acquisition professionals. When developing social engineering training, the government should consider:
  - Does the employee's knowledge of the work/office environment unintentionally cause them to be a target? All employees, no matter age or time in workforce should be required to attend annual training for cyber security and social engineering threats which includes an assessment.
- **Internet Usage** – Internet usage is a part of every acquisition professional's day-to-day activity, but some employees will be more familiar with it than others. That familiarity might be beneficial, but it also might become detrimental depending on how knowledge is applied; for example, experienced internet users who visit many sites and have higher activity levels may be more likely to accidentally click links they should not, or to enter a password to a site that gives an attacker back door access to a system. While the government has some ability to block some undesired websites, attackers are getting smarter and are creating duplicate sites that can be hard to detect. Acquisition employees must be trained on how to navigate the internet, particularly when conducting market research, opening documents from RFI's, or browsing social media. Regarding internet usage, ask:
  - Does the employee confidently use the internet? Users who have become accustomed to routine or repetitive web activity

(e.g., visiting the same sites over and over) might become too comfortable and pay less attention to crucial security measures, or they may fall victim to the aforementioned "autopilot" cognitive bias.

  - Does the employee know how to recognize a legitimate website vs. a duplicated or imitation one? Does the employee know how to properly read a URL and detect a spoofed address?

- **Cybersecurity** – 2021 figures from research firm IDC indicate that the COVID-19 pandemic has coincided with a spike in many forms of network intrusion (many of which can be and have been enabled by social engineering techniques); the same research notes that in response to such phishing, DNS hijacking attacks, and other forms of compromise, many institutions have turned to zero-trust cybersecurity initiatives to mitigate threats. A zero-trust model is a security framework that fortifies the enterprise by removing implicit trust and enforces strict user and device authentication throughout the physical and logical network ecosystem (for example, increased requirements for two-factor authentication); following this model of security and/or asking whether elements of this model could be employed within government and contractor networks is a discussion worth initiating within the many acquisition subcommunities. Other deployable elements of healthy cybersecurity and cyber awareness might include using a trusted, legitimate Internet Service Provider, paying for higher grade antivirus software, making device updates mandatory and monitored, and training employees to verify the legitimacy of website certificates, doublecheck URLs and website spellings, and to look for a locked padlock icon within their browsers when working both in the office and at home.

Increased awareness of acquisition social engineering and training to recognize these attacks is a significant step that government agencies and companies can take toward better whole-of-system security. There are four signs that employees need to be on the lookout for when recognizing a social engineering attack:

1. The attacker will request something of value such as money, account passwords, or financial information. If anyone is asking for information that is known to be sensitive, that should immediately set off red flags that something about the situation is not right.
2. The attacker may imply or state that they wish the interaction to be secret or private. Even when operating in environments where information can be "need-to-know," if the requester asks for the interaction to be private, the employee should ask why. If it's not something that can be told to managers, it is not something the employee should be doing.
3. The attacker will try to rush the interaction so that the employee does not have sufficient time to think through the request or involve others that may detect the malign activity.
4. The attacker may pose as someone from a position of authority or influence. As mentioned above in section 5.2, a deference to authority is one of the six principles of influence and suggests that humans are more likely to agree with something without question if it comes from someone in a higher position than themselves.

8.2 Active Defense Measures and a Proactive Approach

Training of employees is essential to successfully limiting the effects of social engineering attacks, however there are additional avenues that can be explored to assist employees.

U.S. businesses and government agencies should explore emerging technologies (including AI and ML tools) to assist them. For example, AI software can be implemented to flag emails that come to employees from an external address or with misspelled address information. This is sometimes seen by denoting "EXT" (external) at the heading of external emails or by adding a red banner or bold lettering to signal to the employee to take a closer look at the email and the source. Because CO's constantly receive emails originating from external email addresses, they may become saturated with "EXT" which may cause no heightened awareness. In addition, internal emails testing employee knowledge and comprehension with rewards for success should be implemented. All of these measures can be put in place to help prevent social engineering attacks before they can occur.

The rise in social engineering as enabled by emerging technology also begs for a commensurate rise in sophisticated active defense research and development and execution. As mentioned in further detail below, many experts within the cybersecurity and counterintelligence industry view this goal as one that requires not just a new layer of tools and services, but one that will, over time, be best served by a paradigm shift in culture and organization management. Advancements and emerging methods in this field are more likely to positively impact the threat landscape—and secure assets—when they seek to focus on the multiple stages of manipulation (e.g., investigation, hook, play, exit) and the specific tactics currently employed by adversaries (note that this alludes to a need for threat managers to shift defensive measures in accordance with attack vectors over time and to develop automated and continuously re-tailored defensive tools that can be used against emerging and anticipated threats). Some techniques and elements of a forward-leaning defense posture could include the following:

- Advanced risk measurement and reporting tools – Risk can be measured in various ways (citing a litany of commercial platforms that provide this capability as a service), but sophisticated tools often leverage best practices from deep learning neural networks and combine data points from security awareness, user and group security performance (e.g., following a phishing security test), past breaches, high value and high threat job functions, network security scores, adversary intent scores (based on target asset worth and accessibility), adversary capability scores, recent threat intelligence on known bad actors, and the like.
- Forward leaning network security – This applies to software, firmware, and hardware as standard pillars of defensive systems, but it should include corporate efforts to go beyond standard defensive cybersecurity practices (as those mentioned in section 8.1) by prioritizing the hiring of a capable and engaged IT security department intimately familiar with the latest threats, emerging best practices, and an intent to collaborate with and train the workforce with engaging and exciting training regiments instead of dull and mandatory annual online courses. This IT team should be tasked to ensure that the latest AI- and ML-enabled tools are integrated as force multipliers into the IT infrastructure.
- Advanced and innovative approaches to deflect, defeat, and deter adversary operations Perhaps in partnership with the government

and private industry technology partnerships, acquisition leadership should consider:

1. Embracing experimentation as a test bed of prospective methods defending against social engineering; to date, no one method has proven to provide a fool proof defense against social engineering, thus allowing the acquisition community the time and resources to test new methods that will generate ground-up tools and procedures tailored to that community's needs. An example of this may include running experiments to analyze which security training module leads to a more informed workforce and more secure asset holdings; instead of allowing the leadership to focus on training compliance numbers, run three segregated training methods within three areas of operation, take note of defense successes in the aforementioned "risk measurement" metrics, and employ the leading practice.
2. Reward innovative defense-focused ideas; experienced acquisition practitioners are postured to know their systems and target surface more than outsiders peering in. While the latest tools to be leveraged may rightly source from tech-focused outside organizations (thereby justifying deep collaboration), the specifics of where and how adversaries are targeting acquisition systems is likely to source from two areas: threat intelligence professionals and acquisition professionals on the inside working on the operational floor. Incentivizing (financially, organizationally, and culturally) the internal workforce to begin identifying, reporting, and offering solutions in response to these real-time threats heeds current digital transformation wisdom ("transforming a system requires transforming the system within it"[31]) and would give personnel a sense of empowerment over their own procedures (in the context of many project-burdened staffers being further taxed by mandatory training modules); this would also segue well into the following recommendation.
3. Integrally collaborate with emerging technology-focused organizations working in the area of social engineering and network security solutions; innovators leading the movement toward greater system security are beginning to employ AI- and ML-enabled tools and creative low-cost solutions against many of the threats articulated in this paper, often viewing upfront costs as valuable investment. Examples of such solutions include:
   - Integrating honey trap/Potemkin Village targets within a defending system to lure attackers into areas without sensitive assets (such initiatives work to deflect, defeat, and deter threat actors, while data from collected threat intelligence can be leveraged to identify threats and signatures that may arise again in future operations).
   - Leveraging automated, AI- and ML-enabled threat detection, reporting, and mitigation; this can take the form of funneling attackers to a hollow Potemkin network, a "vulnerable and publicly accessible" chatbot posing as an acquisition officer, or ML-enabled detection software that repurposes data artifacts from threat signatures to search for and block new or recurring threat actors. Providing discovered signatures or bad actors that continue to operate to threat intelligence professionals would also provide the intelligence workforce the opportunity to penetrate these social engineer networks to collect information on their intended

[31] B. Leshchinskiy & A. Bowne. "Digital Transformation is a Cultural Problem, Not a Technological One." War on the Rocks, (May 2022) https://warontherocks.com/2022/05/digital-transformation-is-a-cultural-problem-not-a-technological-one/

future targets and techniques (information that can be cycled back to acquisition practitioners to enable a more intelligent and more tailored defense). This list of active defense tools enabled by emerging technology grows by the day; empowering IT managers to leverage the latest in Commercial Off the Shelf and automated products and services (many of which are provided by leading cybersecurity firms that enjoy preexisting, vetted relationships with the government) will bring the acquisition community into a league of modern defense.

4. Reduce the attack surface, restrict task burdens, and shift organizational focus onto security where possible. Commensurate with the degree that acquisition and defense leadership seeks to increase security against social engineering threats, opportunities exist to limit the number of acquisition compliance activities required to complete an acquisition task; less online activity (where many acts provide many opportunities for threat actors to interact with and compromise acquisition systems) and reduced task burdens (where personnel are less distracted from security duties by the number of perfunctory duties) tend to reduce multiple forms of online threats posed to organizations.

9. Conclusion

Social engineering attacks are an increasing challenge to businesses and government agencies across the U.S. Acquisition professionals have constant interaction with both internal and external stakeholders such as government acquisition and technical teams and industry contractors. This creates a unique situation of prospective exploitation that not only threatens sensitive governmental and commercial data but also funds, personnel, proprietary ideas, and democratic institutions. As social engineering continues to grow as a threat, so must the prevention and mitigation techniques put in place against them. While social engineering attackers continue to layer in more sophisticated tools and tradecraft, the USG and its acquisition community must level up into a forward leaning position ahead of them to outsmart and outgun the threat. With a final spirit of optimism, we remind our readers that the suite of technology and skills that underpins adversary capability advancements is the same toolkit that can enable a well-postured defense of tomorrow.

[31] B. Leshchinskiy & A. Bowne. "Digital Transformation is a Cultural Problem, Not a Technological One." War on the Rocks, (May 2022) https://warontherocks.com/2022/05/digital-transformation-is-a-cultural-problem-not-a-technological-one/

Appendix A: Acronyms

AGA	Association of Government Accountants
AI	Artificial Intelligence
APT	Advanced Persistent Threat
BEC	Business Email Compromise
CEO	Chief Executive Officer
CI	Counterintelligence
CO	Contracting Officer
COR	Contracting Officer's Representative
EXT	External
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FTF	Funds Transfer Fraud
HUMINT	Human Intelligence
IT	Information Technology
ML	Machine Learning
NLP	Natural Language Processing
PII	Personally Identifiable Information
RFI	Request for Information
TTPs	Tactics, Techniques, and Procedures
U.S.	United States
USG	U.S. Government

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

The views, opinions, and/or findings contained herein are those of the author(s) and should not be construed as an official government position, policy, or decision unless designated by other documentation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®