HOW DOES RHETORICAL THREAT INFLATION IMPACT AMERICANS' PERCEPTION OF NATIONAL CYBER SECURITY THREATS?

by

LUCILLE A. SCHILLER NOVELLO

A THESIS

Presented to the Department of Journalism and Communication
and the Robert D. Clark Honors College
in partial fulfillment of the requirements for the degree of
Bachelor of Arts

June 2022

An Abstract of the Thesis of

Lucille Schiller Novello for the degree of Bachelor of Arts
in the Department of Journalism and Communication to be taken June 2022

Title: How Does Rhetorical Threat Inflation Impact Americans' Perception of National Cyber Security Threats?

Approved: *Jane Cramer, PhD*
Primary Thesis Advisor

This research project studies how three linguistic shifts, experiencer deletion; deleted agent of the passive; and nominal compounds, impacts a sample of Americans' perceptions of three cybersecurity issues, hacking; privacy; and cyber war, when framed in the national security context. The purpose is to assess how successful these techniques would be if used as rhetorical threat inflation. While this study is not focused on proving whether or not threat inflation is happening with cybersecurity, it uses the fact that there have been few major cybersecurity attacks on US soil that could have severely impacted preconceived notions of the threat. Through a survey composed of three different sets of prompts randomly distributed to 94 participants, there were various combinations that elicited positive shifts in perception. However, there was no single linguistic technique that consistently caused positive impacts. Rather, the most consistency was within cyber war; it was the only topic where all three linguistic techniques had a positive impact.

Acknowledgements

I would like to thank Dr. Jane Cramer, Dr. Melissa Baese-Berk, and Dr. Angela Rovak for their support throughout this thesis process. I feel so privileged to have these three incredible women on my thesis committee. I was fascinated by the concept of "threat marketing" from the moment I first learned of it during a seminar by Susan Eisenhower, American consultant and President Dwight D. Eisenhower's granddaughter. When I learned that this concept is also known as threat inflation and has been researched by Dr. Cramer here at the University of Oregon, I was inspired to pursue my own research about it. Dr. Cramer, thank you for sharing your brilliance with me as both my professor and my primary thesis advisor. I'm very grateful for you. I'd also like to acknowledge Dr. Baese-Berk and the Speech Perception and Production Lab at the University of Oregon for their support and resources that allowed me to conduct this survey. I would not have known where to start with creating, distributing, and analyzing this survey if not for Dr. Baese-Berk's guidance; this thesis would not have been possible without you, Melissa, and I'm so lucky to have you as the second reader. Dr. Rovak, thank you for your assistance with all aspects of the Clark Honors College (CHC) thesis. I appreciate you joining my committee as the CHC representative and for your help with coordinating and planning. I would also like to thank my parents and friends for their constant support and encouragement throughout this entire process (as well as all four years of college). I would not be here without you all, and words could never express how grateful I am to be surrounded by such uplifting, intelligent, and all-around delightful people. You all inspire me to keep moving forward each day. Finally,

I’d like to thank Miriam Alexis Castellón Jordan, the Academic and Thesis Programs Manager, for her help throughout this process with scheduling, coordinating, and formatting.

Table of Contents

List of Tables

Introduction

All day, every day Americans are consuming messages, some of which are being strategically marketed with the intention of getting the public to believe a certain narrative. This subtle manipulation of messaging is accepted and understood on a commercial level; however, it can also be employed by American leaders to promulgate a tainted narrative (Mueller). One tactic is to market an inflated version of a threat through amplified statements, rhetoric, or other linguistic tools, which can create unnecessarily exaggerated fears. Threat inflation, whether intentional or not, does not give the public the chance to make a true assessment on a situation, which means public opinion on an issue will be based on a misleading or manipulated narrative. This sort of misinformation is harmful to a functional democracy since the public can't properly hold the government accountable when there is a false understanding of why the government is acting as they are. Therefore, it is crucial to understand how this phenomenon works in order to acknowledge and account for it in policy and national security discussions.

This paper looks specifically at how threat inflation impacts Americans' perceptions of cybersecurity issues that could threaten the US' national security. As the US has become more interconnected with and reliant on the cyberspace, cybersecurity has quickly become a prominent issue on the national security agenda. Major investments have been made, policy introduced, and conversations had in order to protect the US from what is being framed as the future of warfare. The world has not yet experienced a cyber war, and therefore there are no major events that prescribe a collective understanding of cybersecurity as a threat. Additionally, cybersecurity is

technical by nature, making it hard for the average American to understand. These two factors leave room for political rhetoric to be a primary influence on Americans' interpretation of what cybersecurity means for the future of America.

There are two conflicting arguments: cyber threat theory and cyber threat inflation theory (Mok). The first believes cyber threats are as severe as conventional military tactics through their ability to incapacitate government capabilities, bolster more traditional attacks, and threaten critical infrastructure. The second argues cyber threat inflation mimics threat inflation of the past; it is being used by government leaders, agencies, and contractors to create a cyber-industrial complex focused on profit, despite cyber threats being nothing more than an inconvenience. Those who predict a cyber-industrial complex equate it to the military-industrial complex and blame the close-knit, revolving-door system between government agencies and defense contractors (Mok). Some of the incentives for the political leaders who want to overinvest in defense include a personal political agenda or their relationship with contractors. There is also an issue with how threat inflation can fail to be corrected in the marketplace of ideas due to it dominating the rhetoric seen on the media or by other political leaders (Brito and Watkins). The media often does not fact check claims about cybersecurity but rather reports on the exact rhetoric being used by politicians. Similarly, Congressional representatives tend to hesitate to oppose the rhetoric to avoid looking foolish if the threats do come to fruition. These failures represent a failure in democracy, which makes it that much more important to break down how the inflation becomes widespread.

Perception is reality, and if perception is being manipulated to further a political agenda or to create a disconnect between public understanding and reality, that is crucial to acknowledge. This research intends to understand how thought-leaders could use various rhetorical devices within their cybersecurity communication strategies, and what those rhetorical devices could do to Americans' perceptions of the issues. It is extremely difficult to prove the existence of threat inflation prior to seeing the full impact of the threat at hand. It requires proving the threat is being intentionally packaged by influential people to be worse than they know it to be true. Therefore, this paper is not focused on saying definitively whether or not cybersecurity is being inflated in America up to the date of defense; rather, its intention is to highlight some of the ways it could occur with cybersecurity and to find out whether or not those ways would be effective in increasing perception.

As mentioned, the world has not yet seen the full-scale of some countries' cyber capabilities. Therefore, cybersecurity is a national security risk that is likely less tangible for most Americans compared to national security risks America has already experienced either directly or indirectly. This makes it more of a blank slate in terms of prior conceptions about cybersecurity, cyber war, privacy, and hacking. The core research question is to what degree is there a shift in how individuals perceive various cybersecurity issues after being exposed to manipulated rhetoric designed to inflate the threat?

Answering this research question could help in identifying successful and unsuccessful mechanisms for manipulating perception. It will be especially helpful if in retrospect the threat of cybersecurity turns out to have been inflated. It will offer a better

understanding of how much linguistics matter in national security conversations. There is a myriad of ways of saying the same thing, however, are there certain structures of those messages that create a subconscious, implicit meaning? Equally as important, are there patterns to those structures that could help us break down implied meanings in political rhetoric? Answers to these questions will allow us to uncover the cause-and-effect mechanism of threat inflation that occurs initially on a 1:1 basis but can ultimately lead to mass persuasion of public opinion. I hypothesize there will be rhetorical patterns occurring that use association, personal connection, and intentional vagueness to manipulate how individuals interpret a presented cyber threat.

Literature Review

American government leaders should be expected to provide honest communication, especially when it comes to an issue as vital as national security. However, there is historical evidence of politicians employing rhetoric that inflates threats to be disproportionately alarming and in turn manipulating the public perception of an issue. Threat inflation was evident leading up to both the Cold War (Cramer) and the Iraq War (Brito and Watkins)– two conflicts that did not require the response that the US employed. Scholars have studied these conflicts in retrospect and found threat inflation occurred within them both. This was done in part with the help of information coming to light that highlighted discrepancies regarding how the threat was portrayed as compared to the actual threat America faced.

Throughout the Cold War, there was an inflated fear of Soviet nuclear capabilities. This rhetoric created an arms race that was not based in reality and increased the defense spending budget, specifically on weapons of mass destruction (WMD), and grew the military-industrial complex. These fears were part of what led the US to the Cuban Missile Crisis. However, information about the actual threat Soviet WMDs were to the US proved the threat to be negligible, and the US' actions against this so-called threat to be unnecessary. Dean Acheson, President Truman's Secretary of State during the start of the Cold War, admitted this years later. It fostered an unnecessary fear of an enemy and brought America on the brink of a nuclear war.

Similarly, the path to the war against Iraq had a lot of its justification based on inflated or untrue national security threats. President George W. Bush exaggerated the Iraqi regime's connection to Al Qaeda, and therefore he exaggerated the regime's role

in 9/11. The supposed evidence claiming this alliance ended up being non-existent, which the US leaders who made these claims were aware of (Brito and Watkins). The threat was also framed in the context of nuclear weapons, which was highly unlikely and played on the Cold-War era MWD fear. The less serious, less understood, and more realistic threat from Iraq was biological or chemical warfare. Once again, US leadership was aware of this, but they chose to inflate the threat by framing it in terms of a more lethal, familiar weapon to Americans. To make matters worse, the administration claimed Iraq was making nuclear weapons, leaked this unfounded claim to the media, which went unchecked, and then used this media report as justification for the conflict (Brito and Watkins). The lead up to the Iraq war is an example of how threat inflation can survive in democracy and surpass checks and balances due to the rhetoric being taken at face value.

The theory of Cyber Threat Inflation suggests threat inflation is currently occurring in cybersecurity (Mok), and other scholars have drawn parallels as well (Brito and Watkins; Thierer); however, as previously stated, because America hasn't actually experienced a full caliber cyberattack on US soil, it's difficult to determine how much the rhetoric is exaggerated. That being said, researchers and scholars have drawn parallels between the ways government officials are framing and talking about a looming cybersecurity threat to how threat inflation has been used in the past. The threats being presented in sources such as the CSIS Commission Report or the book *Cyber War* are done so in an alarmist way without evidence that matches the scale of the supposed threats. The evidence provided are things such as DDOS attacks, which can cause servers to shut down; these kinds of attacks are widely defined by the

cybersecurity community as being nothing more than an inconvenience that is easily reversible. Another is that the Department of Defense computers are probed "hundreds of thousands" times per day (Brito and Watkins); however, they don't explain that this is something even the most novice coder can accomplish, as it is the computer equivalent to trying a doorknob to see if it's open. While there is the obvious issue of government confidentiality, these sources are still asking Americans to use blind faith in accepting these threats as legitimate, while providing minimal evidence. This same blind faith was used in the Cold War and the Iraq War.

Although there is research on threat inflation as a concept and its applications to historical events through a big picture lens, there has been little to no research breaking down the process of this kind of political rhetoric. This is the gap this study intends to start filling. It takes this threat inflation rhetoric that is known to exist through history, and its implications for cybersecurity, which has been posited to be currently occurring, and see how it unfolds on the individual level. There has been research conducted regarding the power of linguistics on perception and the ways political rhetoric can affect psychological responses (Bakker), but nothing yet connecting rhetorical threat inflation to individuals' acknowledged understanding.

Methodology

Background

This thesis is working within multiple subfields. It includes political theory, linguistics, and perceptions of threat. Typical research methods in the cross-sections of these fields include applying theories to behaviors, looking at how individuals interact with the world, and surveying data. Researchers analyze both qualitative and quantitative data; this specific study focuses primarily on quantitative data but contextualizes it with some qualitative data. A lot of what is analyzed in political science are theories in tandem with behaviors. Therefore, it is mostly qualitative identifications of behavior and trying to find meaning in them. Researchers analyze patterns in political actions and can connect those to polling results or other forms of surveys. Linguistics find patterns in how word usage, grammar, and subtle changes alter a meaning. This is also conducted through qualitative analysis of sentence structures and how those that offer the same literal truth differ in interpretation. Some psychology research includes capturing subconscious physiological reactions someone has to a stimulus (i.e. affective responses). However, the specific subfield of understanding how someone perceives or understands something must be analyzed through how they respond to prompts in surveys. Since perception is an internal process, we can only analyze what the individual chooses to share about their understanding, which is why strategically targeted survey questions are so important.

Study Design

The approach I chose is to conduct a primarily quantitative, cause-and-effect survey to identify whether or not subtle linguistic changes impact perception. Three broad cybersecurity issues – hacking, privacy, and cyber war – were paired with three linguistic manipulations –nominal compounds, deleted agent of the passive, and experiencer deletion. Nominal compounds are two nouns linked together in order to create a phrase with a new meaning; these can be strategically created with words that have associative value in order to foster an emotional connection between the rhetoric and the audience. For this study, it includes the phrases "cyber-9/11", "cyber-Katrina", and "cyber-Pearl Harbor". They associate cybersecurity with catastrophes the average American is familiar with. The linking of these events with "cyber" is intentionally vague; it is intended to determine whether or not such a vague, random connection is effective in eliciting a perceptual understanding of a concept that is not defined through factual prompts. The pairing of each subtopic to a specific nominal compound is designed to be random. A deleted agent of the passive focuses an entire situation on one particular actor; rather than it being "person A did this to person B", the sentence focuses on either what person A is doing or what happened to person B. For the purpose of this study, the receiver statement refers to the structure aligned with what happened to person B while the actor statement refers to the structure aligned with what person A is doing. Finally, experiencer deletion is a way of using vague wording, such as "seem" or "may" to disguise sources and get away with making a statement without significant evidence (Bolinger).

Each issue was paired once with each of the linguistic manipulations, and they were divided into three forms of the survey wherein each form was evenly and randomly assigned to participants. For the first form (red), hacking was paired with experiencer deletion, privacy with deleted agent of the passive, and cyber war with nominal compounds. The second form (green) had hacking with nominal compounds, privacy with experiencer deletion, and cyber war with deleted agent of the passive. The third and final form (purple) paired hacking with deleted agent of the passive, privacy with nominal compounds, and cyber war with experiencer deletion.

Each survey form was comprised of demographic questions, a set of questions to establish the participant's baseline perception of each issue, and nine or ten sets of questions. These sets were comprised of strategically written prompts with subtle linguistic changes followed by a series of questions to collect participants understanding of cybersecurity threats after reading each prompt. The questions asked for the baseline and after each prompt were:

Q0. (Only for baseline set) How much do you think you know about _____? (Answer on scale of 1-10)

Q1. How worried does _____ make you? (Answer on scale of 1-10)

Q2. How imminent of a threat do you see _____ as? (Answer on scale of 1-10)

Q3. How likely do you think you personally could be affected by _____? (Answer on scale of 1-10)

Q4. How does this change your perspective on this concept? What do you

associate with this concept after reading this excerpt? (Text box response)

The three cybersecurity issues had 2-3 designated prompts per survey form. Additionally, the prompts focused on specific scenarios rather than the overarching concept. For hacking, those scenarios were hacking of the US electrical grids, US nuclear technology, and US classified government information. For privacy, it was American's personal privacy being compromised and American companies having their privacy compromised. For cyber war it was a war with another country and a war with a terrorist organization. Each of these subtopics had a dedicated prompt and set of questions. When the issue was paired with deleted agent of the passive, each subtopic had two prompts: one focused on what the actor is doing and one focused on what is happening to the receiver. Although the prompts were focused on a specific subtopic within the broader cybersecurity issue, the questions themselves asked about the participant's perception of the overarching topic to maintain consistency.

The survey concluded with optional demographic questions asking the participant's age, gender, race, general location (city or state), and political affiliation. Although the questions were intentionally vague to prevent participant identification, these were made optional to ensure participants felt comfortable participating, since it is not possible to guarantee confidentiality.

Distribution

The survey was hosted through Qualtrics and distributed through Prolific. Qualtrics' randomizer feature ensured each participant received a random form of the

survey, and that each form was distributed evenly. Additionally, each of the questions within each form were organized randomly for every survey taker. Prolific recruited participants. The only parameters for participation were to be over 18 years old, located in the United States of America, and fluent in English. Ninety participants were recruited through the platform and compensated for their time. There were 4 additional participants who took the survey through distribution from the Speech Perception and Production Lab at the University of Oregon.

Process of Analyzation

The primary focus when analyzing the data was on how much the participants' perception shifted rather than how high the ratings were numerically. If someone's perception started at "4" and changed to "5", that is equal to someone's perception starting at "9" and changing to "10" in this research. A "1" on the scales provided to participants signified the lowest degree of worriedness, imminence, or personal affect, and a "10" on the scales signified the highest degree. The higher the number reported by the participant, the scarier the threat is. Therefore, a positive shift refers to the participant viewing the topic as more threatening after the prompt since the numerical shift is positive. Comparatively, a negative shift refers to the topic being perceived as less threatening. Since this research focuses on the shift, it is difficult to account for those who reported a baseline number of "1" or "10" as they could not decrease or increase their perception respectively.

As discussed in the study design, each cybersecurity topic had subtopics that were used in prompts. Analyzation focused on changes in perception within each subtopic/linguistic change pairing as well as coupling the subtopics together to look at

the broader topic/linguistic change pairing. For the subtopic pairings, the three key values that will be discussed are:

1) The shift from the baseline question average across all participants to the prompted question average across all participants
2) The percent of participants whose perception increased versus the percent that decreased or stayed the same
3) The average increase (among participants whose numbers went up), and the average decrease (among participants whose numbers went down) to see the degree of change in each direction

For the broader topic pairings, the two primary values are:

1) The average shift from baseline to prompt answers per question for a topic/linguistic change pairing (across all of the subtopics)
2) The average shift from baseline to prompt answers across all three questions (to identify general affect per broad topic/linguistic change).

In addition to these averages and calculations of shifts, the reported baseline knowledge score was also analyzed. This question was not re-asked after each prompt since the prompts were not informative, nor were they meant to be. However, the reported baseline numbers were averaged to identify the general knowledge participants self-identified prior to taking the survey.

Results: Focused on Linguistic Difference

I. Perception Shift with Experiencer Deletion

Table 1: Experiencer Deletion Effectiveness Across Subtopics

	More Worried	Less / Equally Worried	More Imminent	Less / Equally Imminent	More Personal Affect	Less / Equally Personal Affect
HACKING	- Elec. grids - Nuclear tech	- Classified Info	NONE	- Elec. grids - Nuclear Tech - Classified info	NONE	- Elec. grids - Nuclear tech - Classified info
PRIVACY	- Personal Info - Amer. companies	NONE	NONE	- Personal info - Amer. companies	- Personal Info - Amer. companies	NONE
CYBER WAR	- Country	- Terrorism	-Terrorism	- Country	- Country - Terrorism	NONE

Overview

Experiencer deletion (ED) had very split effects; Q1 was effective for all but two subtopics, Q2 was ineffective for all but one subtopic, and Q3 was split with two broad topics seeing positive changes and one broad topic seeing a negative change. Across the three broad topics and the three questions, ED's total effect was marginal (+0.004). Q1 (+0.218) and Q3 (+0.293) both had positive average shifts across the three topics, and Q2's shift was negative (-0.507); therefore, although the total effect was minimal, the individual questions did witness some movement. There was not a single broad topic where ED consistently increased or decreased the participants' average shift across questions. This section outlines a lot of data, but please refer to the appendix for more details and tables outlining the findings.

Hacking

When analyzing hacking and ED broadly, it was ineffective for bolstering the threat. For Q1, the average change across all three subtopics' answers was +0.213, however both Q2 (-0.417) and Q3 (-0.767) had a negative effect. This brings a negative total shift of -0.324 across the three questions when ED and hacking were packaged together. Each of the three subtopics also saw a decrease in perception when asked about imminence (Q2) or personal affect (Q3). When asked about how worried the prompt made them (Q1), participants were more worried when ED was coupled with the hacking of electrical grids or hacking of nuclear technology, but they were less worried when paired with hacking of classified government information.

When hacking of the electrical grid was paired with ED, Q1 saw 50% of the participants increase their perception of how worrisome it is, while the other 50% had their perception of hacking decrease or stay the same. The average increase for Q1 was +2.27, and the average decrease was -1.90. The total average shift from the baseline question for Q1 was +0.50. For Q2 and Q3, the majority of participants saw hacking as being less or equally threatening, and the average decreases were higher than the average increases. Both questions also witnessed a negative average shift from the baseline results to the prompted results (Q2: -0.26, Q3: -0.10). For more detailed information on these negative shifts, please refer to the appendix.

The hacking of nuclear grids with ED elicited a positive shift for Q1 (+0.84) as well as 50% of participants who viewed the threat as being more worrisome. However, it saw a larger average decrease (-3.20) than an average increase (+2.73). Q2 and Q3 both had negative shifts (Q2: -0.03, Q3: -0.50). For classified government information

and ED, there were no positive results. All of the questions' average shifts were negative, the average decreases were more significant than the average increases, and a majority of respondents viewed hacking as less or equally threatening.

Privacy

Overall, the average shift across all three questions when ED was paired with privacy was an increase of +0.173. Both Q1 and Q3 witnessed a positive shift (+0.455 and +0.205 respectively), while Q2 saw a negative shift of -0.140. Similar to those results, Q1 and Q3 had both privacy topics (personal information and American companies) averaging a higher perception of the threat whereas Q2 had both topics averaging a lower perception. Generally, ED was ineffective at increasing the perception of the imminence of privacy being compromised; however, it was effective in increasing the perception of how worrisome privacy is, and how likely it is to affect the individual participant.

Interestingly, although the broad privacy numbers show a slightly bolstered view of the threat, the broken-down numbers paint a different picture. Across the three questions, only 33% of participants had an increased perception of personal information being compromised (vs 67% decreased/same), and only 35% of participants had an increased perception of American companies' information being compromised (vs 65% decreased/same). The average shift across the three questions was close to the same as well. For personal information, the average increase was +1.887 while the decrease was -1.640. For American companies, the average increase was +1.683 versus a decrease of -1.603. Both subtopics saw an increase shift from the average baseline responses to the average prompted responses for Q1 and Q3. For personal information, the increases

were +0.50 for Q1 and +0.13 for Q3. Q3 also had a higher average increase (+1.91) than decrease (-1.56). The average shift for personal information and Q2 was -0.03. For American companies, Q1's shift was +0.41 and Q3's was +0.28. Both of these questions had a higher average increase (Q1: +2.00, Q3: +1.80) than average decrease (Q1: -1.50, Q3: -1.64). Q2 and American companies witnessed a negative shift of -0.25.

Cyber War

Generally, ED was effective in increasing the threat perception of cyber war. The average shift across the three questions was +0.760 with Q1's shift being -0.145, Q2's shift being +0.050, and Q3's shift being +0.855. Q3 had the largest shift and was also the only question where both topics (cyber war with another country or with terrorists) had participants' perception shift upwards (+0.90 and +0.81 respectively). Both Q1 and Q2 were split. People were more worried about a cyber war with another country (+0.15) while they were less worried about a cyber war with terrorists (-0.44). Alternatively, participants saw a cyber war with terrorists to be more imminent (+0.22) and a cyber war with another country less so (-0.12).

When ED was paired with the threat of a cyber war from another country, the average number of participants who had an increase was 37% (vs 63% decrease/same) and the average increased shift was +2.69. The average decreased shift was -2.06. Q3 had the largest average positive shift (+2.88) and percentage of participants who perceived the threat higher (50%). However, Q1 had the largest gap between the average increase (+2.70) and average decrease (-1.83). Q1 had 31% of participants view the threat as more worrisome and 69% saw it as less or equally worrisome. Q2, which

referred to imminence, also had 31% of participants increase and 69% decrease. However, the average shifts were more similar in Q2 than Q1 (+2.50 and -2.23).

Broadly, there were very similar results when ED was coupled with a cyber war with terrorists. 36% of participants experienced the threat as being increased while 64% had a lower or equal perception. The average shifts for increase and decrease were +2.43 and -1.85 respectively. Just like when ED was paired with cyber war with a country, Q3 also saw 50% of participants increase their perception and 50% decrease. However, the average shifts were more similar (+2.45 and -2.11). Q1 had the largest delta between the average shifts with an increase of +2.75 and decrease of -1.83. 25% of participants were more worried after reading the prompt and 75% were less or equally worried after the prompt. Q2 fell in the middle of the other two prompts numbers-wise. 34% of participants saw the threat of cyber war as more imminent (with average increase of +2.09) while 66% saw it as less imminent (with average decrease of -1.60).

II. Perception Shift with Deleted Agent of the Passive

Table 2: Deleted Agent of the Passive Effectiveness Across Subtopics

	More Worried	Less / Equally Worried	More Imminent	Less / Equally Imminent	More Personal Affect	Less / Equally Personal Affect
HACKING **RECEIVER**	Elec. Grids Nuclear tech	Classified Info	N/A	Elec. grids Nuclear tech Classified info	Elec. grids	Nuclear tech Classified info
HACKING **ACTOR**	Elec. grids Nuclear tech Classified info	N/A	N/A	Elec. grids Nuclear tech Classified info	N/A	Elec. grids Nuclear tech Classified info
PRIVACY **RECEIVER**	N/A	Personal info Amer. companies (n/c)	N/A	Personal info Amer. companies	N/A	Personal info Amer. companies
PRIVACY **ACTOR**	N/A	Personal info Amer. companies	N/A	Personal info Amer. companies	N/A	Personal info Amer. companies
CYBER WAR **RECEIVER**	Country Terrorism	N/A	Country Terrorism	N/A	Country Terrorism	N/A
CYBER WAR **ACTOR**	Country Terrorism	N/A	Country Terrorism	N/A	Country Terrorism	N/A

Overview

Analyzing the impacts of deleted agent of the passive (DA) on perception includes a two-pronged approach: the influence of a statement that's been framed around what the actor is doing (herein referred to as actor statement) and the influence when a similar statement is framed around what is happening to the receiver (herein referred to as receiver statement). Overall, both forms of DA had parallel effects. Across each of the topics, both the actor statements and receiver statements saw a total positive effect, as well as positive shifts for Q1 and Q3, and negative shifts for Q2. Additionally, both statements had similar numbers for Q1 and Q2. The actor statements had an average increase of +0.335 with Q1 while the receiver statements had +0.327. For Q2, the actor statements had the average decrease of -0.183 and the receiver

statements experienced the decrease -0.153. The receiver statements saw a greater positive shift (+0.334) than the actor statements (+0.143) for Q3. The total increase across all three questions and topics was +0.098 for actor statements and +0.170 for receiver statements. Therefore, both forms were slightly effective in increasing perception numerically. However, those positive results were not reflected consistently across the topics after breaking the data down further. This section outlines a lot of data, but please refer to the appendix for more details and tables outlining the findings.

Hacking

The only question where DA (in either form) was effective across all three hacking subtopics was Q1 where participants were asked about how worried it made them. Actor statements showed a positive increase of +0.46, while receiver statements had an average shift of +0.08; Q1 and receiver statements were effective for electrical grids and nuclear technology but not classified government information. The average shifts in Q2 and Q3 across all three subtopics for actor statements were -0.46 and -0.17 respectively. Similarly, receiver statements had a shift of -0.43 for Q2 and -0.28 for Q3. None of the subtopics elicited an average positive shift from baseline Q2 to DA prompted Q2. Across the three questions, hacking and ED actor statements had an overall effect of -0.057, and hacking and ED receiver statements had -0.208.

Electrical grids being hacked had the most positive shifts from baseline average to prompted question averages. Additionally, the receiver statements were more effective than the actor statements in increasing perception of this subtopic. For Q1, both the receiver statement (+0.47) and actor statement (+0.22) were effective in making the threat more worrisome. Both forms of the DA had 41% of participants

increase how worried they were about the threat; the receiver statement had an average increase of +2.62 (compared to average decrease of -2.11), and the receiver statement had an average increase of +2.38 (with average decrease of -2.18). Neither form of DA was effective for the question of imminence; the receiver statement elicited an average shift of -0.31 and the actor statement saw -0.56. For the receiver statement, 38% of participants increased their ratings of imminence, but the average increase (+2.00) and the average decrease (-2.00) essentially cancelled each other out. For actor statement, 38% of participants saw the threat as more imminent, but their average increase (+1.75) was smaller than the 62% of participants who decreased (-2.38). Finally, DA receiver statements and the hacking of electrical grids was the only hacking/DA combination to elicit a positive shift for Q3 (+0.35). Again, only 38% of participants viewed the threat as more likely to affect them, but the average increase (+2.75) was higher than the average decrease (-2.00). The DA actor statement was ineffective in increasing the average rating among participants for Q3 (-0.06). 41% of participants reported an increased likelihood of them being personally affected, but that average increase was only +2.15 compared to the decrease of -2.50.

For DA and American nuclear technology being hacked, the only question that elicited a positive shift from the baseline was Q1, and both the receiver prompt (+0.15) and actor prompt (+0.69) had that outcome. Q1 and the receiver statement had 41% of participants report higher numbers from the prompt with an average increase of +2.15 and average decrease of -2.17. Despite there being a larger average decrease and percentage of participants who did not get more worried, there were three participants who kept their baseline scores of 10, which contributed to the higher average and

resulting positive shift from baseline to prompt. Q1 and the actor statement was the only combination for DA/hacking that had a majority (59%) of participants shift to a more threatening perception. The average increase was +2.16 and the average decrease was -3.17. Both Q2 and Q3 with both forms of the DA prompt had negative shifts from the prompts. Q2 saw shifts with the receiver statement and actor statement respectively as -0.31 and -0.44. Q2 and receiver had 66% of participants lower or keep their perception, and Q2 and actor had 69% of participants lower or keep their perception. They both had a higher average decrease (-1.90 and -2.11 respectively) than increase (+1.55 and +1.30 respectively). Q3 also saw negative shifts with both DA forms. The receiver statement shifted perception by -0.06 with 59% of participants lowering or maintaining their report of the threat; the average increase (+1.85) was marginally greater than the average decrease (-1.80). The actor statement and Q3 saw a shift of -0.18 with 69% of participants viewing the threat as less or equal to the baseline. The average increase was +2.40, and the average decrease was -2.00.

The last subtopic, classified government information being hacked, had only one combination in which there was a positive shift. That combination was Q1 and the prompt focusing on the actor. That shift was +0.47 with 41% of participants viewing hacking as more worrisome. The average increase was +2.38, and the average decrease was -2.42. All of the other combinations had negative shifts from the baseline and a majority of participants whose perception either lowered or did not change. Additionally, all but one (the Q3/actor statement) of the remaining combinations had a higher average decrease than a higher average increase. For details on these results see the appendix.

Privacy

Both forms of DA and privacy were broadly ineffective combinations for increasing the threat perception of participants. Privacy as an overarching topic had negative shifts for all three questions with both the receiver statement and the actor statement. This stayed true when breaking it down to the subtopics; every privacy subtopic and DA combination elicited either a negative or null shift. The overall shift with the receiver statement across both subtopics and the three questions was -0.285; this shift can be broken down with each question as follows: Q1 = -0.10; Q2 = -0.62; and Q3 = -0.14. For the actor statement, the shift was -0.573 with the break down as follows: Q1 = -0.30; Q2 = -0.62; and Q3 = -0.80. These shifts combined the average shifts for both subtopics (privacy of personal information and privacy of American companies). Breaking down the shifts by subtopic showed almost identical results; all of the DA/privacy combinations with the exception of one (Q1, American companies, focused on the receiver), which did not shift at all, were negative. For more information on this data, please see the appendix.

Cyber War

Cyber war and DA was the most potent combination for manipulation in the entire survey. Every single question, regardless of the form of DA or the subtopic, saw a positive shift from the baseline responses to the averaged prompt responses. To analyze broadly first, the average shift across cyber war and the three questions following the receiver statement was +0.925, and for the questions after the actor statement was +1.002. Breaking it down per question, across both subtopics the average shifts for receiver statements were Q1 = +1.00; Q2 = +0.59; and Q3 = +1.42. There were very

similar results for the breakdown of questions after the actor statement: Q1 = +0.85; Q2 = +0.53; and Q3 = +1.40. These positive shifts were so significant that they are the primary reason why the DA total average (across all three broad topics) was positive; essentially, the cyber war and DA combination carried the overall success rate of DA in this research. Both subtopics (cyber war with another country or with a terrorist organization) experienced positive shifts for all three questions with both forms of the DA prompt.

The first subtopic was a cyber war with another country. For Q1, Q2, and Q3, the receiver statement saw greater shifts than the actor statements, although both forms saw positive changes. Q1 and the receiver shifted +1.06 with 47% of participants increasing their perception by an average shift of +2.80 (versus average decrease of -1.67). Q1 and the actor was +0.41 with 41% of participants increasing with the average increase of +2.00 and average decrease of -1.70. Q2 had similar results; the receiver statement elicited a +0.47 shift while the actor statement had a +0.22 increase. Both statements had only 38% of participants increase their perception, but the receiver statement had a starker difference between the average increase (+2.17) and decrease (-1.33) than the actor statement's increase (+1.67) and decrease (-1.50). Q3 elicited the largest average shifts from the baseline responses to the prompted responses. Again, the receiver statement was slightly more effective (+1.40) than the actor statement (+1.12). Both subtopics and Q3 had 50% of participants increase their perception; the receiver statement had an average increase of +3.06 (average decrease of -1.50), and the actor statement had the average increase +2.44 (average decrease of -1.17).

The second subtopic was focused on cyber war with a terrorist organization. Both forms of DA elicited positive shifts in all three questions. While the receiver statement was more effective than the actor statement for a cyber war with another country, the opposite was true for a cyber war with a terrorist organization. Across all three questions the actor statement had a larger shift from the baseline responses to the prompted responses. Additionally, each question had a larger average increase than decrease, and all but one combination (Q2 / receiver statement) had a majority of participants who increased their perception. For Q1, the actor statement saw a +1.28 shift while the receiver statement a +0.94 shift. The actor statement had 59% of participants increase with the average increase of +2.68 and average decrease of -2.00. The receiver statement and Q1 had 53% of participants increase their reported worriedness with the average increase of +2.41 and decrease -1.86. For Q2, the actor statement had 53% of participants view the threat as being more imminent; the average increase was +1.94, and the average decrease was -1.33. The shift from baseline was +0.84. Q2 and the receiver statement was the only combination of this subtopic and DA to have a minority percentage (34%) of participants increase their perception. However, it still saw a positive shift from the baseline of +0.59, which was likely due to the difference between the average increase (+2.55) and average decrease (-1.50). Q3, as similar to the country subtopic, elicited the largest shifts from baseline out of the three questions. The actor statement shifted answers by +1.68 with 59% of participants reporting higher numbers; the average increase was +2.89 and the average decrease was -1.00. The receiver statement also positively shifted perception (+1.43) with 56% of

participants viewing the threat as more likely to personally affect them. The increase averaged at +2.72, and the decrease averaged at -1.00.

III. Perception Shift with Nominal Compounds

Table 3: Nominal Compounds Effectiveness Across Subtopics

	More Worried	Less / Equally Worried	More Imminent	Less / Equally Imminent	More Personal Affect	Less / Equally Personal Affect
HACKING	- Elec. grids	- Nuclear tech - Classified info	- Elec. Grids	- Nuclear tech - Classified info	- Elec. grids - Nuclear tech - Classified info	NONE
PRIVACY	- Amer. companies	- Personal info	NONE	- Personal info - Amer. companies	- Amer. companies	- Personal info
CYBER WAR	- Country - Terrorism	NONE	-Terrorism	- Countries (n/c)	- Country - Terrorism	NONE

Overview

Nominal compounds (NC) varied in effectiveness depending on the topic it was paired with. It had the greatest positive effect on each question when in tandem with cyber war. Hacking experienced an overall minor positive effect, and privacy had only negative effects, both for individual questions and as a total average. In sum, across all three topics, NC had a positive effect on Q1 by increasing the degree of participants who were worried by +0.167. It was the most affective in altering perception related to personal affect, Q3, by increasing participants by perception by +0.466. For Q2 and the

question of imminence, participants had their perception decrease by -0.175. Across the three questions, the total impact NC had on perception was +0.458, therefore it was generally an effective method for altering participants' perception. This section outlines a lot of data, but please refer to the appendix for more details and tables outlining the findings.

Hacking

The overall averages when hacking and NC were matched indicated a minor positive effect. The most significant impact was on Q3 regarding how much a participant felt they could be personally affected by hacking. That question had all three hacking prompts (electrical grids, nuclear technology, and classified government information) experience an increased perception with an average of + 0.517. For Q2 and Q3, the effects were negligible and negative respectively. NC only increased how worried participants were about hacking by + 0.04, and it decreased how imminently people viewed it by – 0.18. For those two questions, the only hacking prompt that saw a positive shift was based on the hacking of electrical grids (Q1: + 0.59, Q2: + 0.25). Both the hacking of nuclear grids (Q1: - 0.25, Q2: - 0.50) and classified government information (Q1: - 0.22, Q2: - 0.29) elicited decreases.

The hacking of electrical grids was the only sub-topic of hacking that was effectively bolstered by NC; it was compared to a "cyber-9/11" in the prompt. The most significant shifts occurred in Q3 with 63% of participants viewing the threat as more likely to affect them as compared to their baseline answers (vs. 37% decreasing/staying same). Similarly, the degree of the shift was more significant on average in Q3 for those whose perception heightened (+ 2.45) versus those who decreased (- 1.71). Q3 therefore

saw the greatest contrast in relation to the NC and hacking of electrical grids prompt. Electrical grids also saw a modestly increased average compared to the baseline questions for Q1 (+ 0.59) and Q2 (+ 0.25). However, both of these questions had a higher average decrease (Q1: -2.17, Q2: -2.20) than increase (Q1: +2.13, Q2: +2.00), and they both had 53% of participants view the threat of hacking as lower or the same.

Both the hacking of nuclear grids (paired with cyber-Pearl Harbor) and the hacking of classified government information (paired with cyber-Hurricane Katrina) saw a positive effect when paired with Q3 and negative effects for Q1 and Q2. Focusing first on the hacking of nuclear grids and Q1, 75% of participants saw the threat as less worrisome with an average decrease of -2.21. For the 25% who perceived it as more worrisome, the increase was an average +3.00. Across all of their answers, the average answer was -0.25 lower than the answers reported for the baseline. Q2, which questioned the matter of imminence, had the reported answers be -0.50 lower than the average for the participants' baseline perception. Again, 75% of participants had their perception decrease with an average of -2.64, and 25% of participants had their average increase with an average of +2.63. Q3 was the only question eliciting a higher average than the baseline with an increase of +0.38. 53% of participants saw it less likely to personally affect them with an average decrease of -3.29, and 47% saw as more likely with the average change of +2.33.

The hacking of classified government information saw very similar results to that of nuclear technology. All three questions had a higher percentage of participants view the threat lower numerically, and only Q3 had the overall average perception increase. For Q1, the change from the baseline question was – 0.22 with 75% of

participants viewing the threat as less worrisome. Despite only 25% of participants reporting an opposite effect, the average increase was more significant (+2.25) than the average decrease (-1.56). It was a similar result for Q2 and classified information; 72% of participants saw the threat as less imminent, but they also had a less significant decrease (-1.44) than the 28% who viewed it as more imminent (+1.89). The overall shift from the baseline question across all participants was -0.29. For Q3, the average change from the baseline question had a marginal increase of +0.04. However, the majority of participants (62%) still saw the threat as less likely to personally affect them with an average decrease of -1.82. The 38% of survey participants who increased their perception had an average increase of +2.42.

Privacy

NC were overall ineffective in tandem with privacy. The changes between baseline and prompt for all three questions, and the total average change, were negative. When averaging across both topic, privacy as related to personal information and American companies' information, Q1 had an average decrease of -0.19. For Q2, the decrease was -0.48 and Q3 had a decrease of -0.27. Overall, the decrease was -0.31. The privacy of individual Americans being compromised did not yield any average positive results from the prompt, and the privacy of American companies yielded positive results from Q1 and Q3.

Personal information was paired with a "cyber-Pearl Harbor" for the prompt. Every question had a majority of participants rating the threat as lower, and the average decreases in perception were higher than the average increases. For Q1, 72% of participants were less worried after reading the prompt with an average decrease of -

2.86. For the 28% who were more worried, the average increase was +2.22. When asked about imminence (Q2), 84% of participants found the threat to be less imminent and the average decrease was -3.08 compared to the average increase of +2.80. Finally, Q3 yielded 69% of participants who saw the threat as less likely to personally affect them with the decrease being -3.07, and 31% saw it as more likely to affect them with an average of +2.60.

The prospect of American companies having their privacy compromised was paired with a "cyber-9/11" for the survey. The results were similar to those from personal information in that each question had a majority of participants decrease their perception, and the average decreases were larger than the average increases. Additionally, Q2 had an overall decrease from the baseline question of -0.15. 62% saw the threat as being less imminent (vs. 38% more) and the average decrease was -2.73 (vs increase of 2.08). The results differed from Americans' personal privacy in that Q1 and Q3 both had higher averages across all the participants compared to the baseline. Q1 saw an increase of +0.25 from the baseline question. However, only 44% of participants saw the threat as more worrisome (vs 56% less) with an increase of +2.36 (vs decrease of -2.50). Q3 and the question of personal affect had an increase of +0.13. 41% of participants viewed it as more likely to affect them (vs 59% less), and the average increase was +2.69 (vs decrease of -2.82).

Cyber War

Cyber war was the only topic that saw positive results across all three questions when paired with NC. The average delta from baseline question to prompted question across both topics and all three questions was +0.645. When breaking it down by

question, the average change across both topics for Q1 was +0.65, for Q2 was +0.135, and for Q3 was +1.15. Both topics, a cyber war with another country or a cyber war with a terrorist organization, yielded positive results for Q1 and Q3. For Q2's question of imminence, a cyber war with a terrorist organization saw an increase in perception, but with another country, the perception did not change from the baseline question.

For the survey version where NC and cyber war were paired up, a cyber war with another country was compared to a cyber-Hurricane Katrina. All three questions had the average increase be higher than the average decrease, but none of the questions had a majority of participants increase their perception. That said, all three questions had participants who couldn't increase their answers as their base perception was already at a 10. Q1 saw 40% of participants view cyber war as more worrisome with an average increase of +2.83; this compared to the 60% of participants who saw the threat as less or equally worrisome with an average decrease of -1.75. The overall change from the baseline question was +0.67. For Q2, there was no change from the baseline question to the prompted question – both averaged 6.30. 73% of participants had their perception of imminence decrease or stay the same (-2.00) and 27% had their perception increase (+2.50). Q3 had the most striking change from the baseline question with the average increasing +1.20. 50% of participants felt cyber war was more likely to personally affect them after reading the prompt; the average increase was +2.93. The other 50% saw the threat as being less or equal to their baseline, with the average decrease being -1.14.

A cyber war with a terrorist organization was equated to a "cyber-9/11" for the survey. All three prompted questions resulted in a higher average than the baseline

question average. However, again, all three questions had a majority percentage of participants whose perception of cyber war decreased or stayed the same. Q1 had an increase from the baseline question of +0.63. There were 43% of participants who perceived the threat as being more worrisome (with increase of +2.69) and 57% of participants who perceived it as less or equally worrisome (with decrease of -2.67). Within the 57%, four of those participants stayed the same because they had rated it a 10 in their baseline answer and therefore couldn't increase. For Q2, the increase from the baseline was +0.27 with 40% increasing and 60% decreasing or staying the same. The group that increased their perception had an average delta of +2.75, and those that decreased their perception had an average delta of -3.13. Again, four participants gave a baseline answer of 10. Similar to the results from NC and cyber war with another country, Q3 had the largest change from baseline out of the three questions; the average rating increased by +1.10. 47% increased and 53% decreased or stayed the same (two participants stayed at 10). The average increase (+2.50) was higher than the average decrease (-2.14).

Results: Focused on Topic

I. **Introduction**

Since this thesis is specifically about the linguistic devices that could be used in manipulating perception, most of the data is provided in the above results section focused on the linguistic difference or in the appendix. However, given the quantity of data provided, the results below highlight patterns centered on the topics as additional context and framing. It also includes information about participants self-reported knowledge from the base perception section of the survey. The same baseline knowledge was relevant for each of the subtopics as it only asked about how much a participant felt they know about the broad topic.

II. Perception Shift within Hacking

Hacking had mixed results; different subtopics were successful with different linguistic devices. Generally, electrical grids was the subtopic where the most increased perception occurred. The baseline knowledge for hacking averaged 4.55 across the three sets of data (red: 4.77, green: 4.41, purple: 4.47).

Electrical grids had the most increases out of all of the subtopics for hacking in terms of the average deltas from the baselines. Nominal compounds and electrical grids were the only combination with hacking where every question saw a positive increase from the baseline. Nuclear technology and classified government information only saw increases with Q3 in nominal compounds. Nominal compound was also the only linguistic device that elicited a positive broad shift (+0.126).

Experiencer deletion was completely ineffective with classified government information; all of the questions saw negative deltas from the baseline, a majority of participants whose perception decreased or remained the same, and a higher average decrease than increase. It was however effective for Q1 with electrical grids (+0.50) and nuclear technology (+0.84). The overall effectiveness across the questions and subtopics was -0.324.

Finally, deleted agent of the passive was the most effective with electrical grids. There weren't any patterns identifying a certain form of DA being more effective. Rather, they differed in effectiveness based on the subtopic. For electrical grids, the receiver statement was more effective and increased both Q1 and Q3, while the actor statement only increased Q1; therefore, 50% of the questions saw increases. The two other subtopics only saw increases with Q1; nuclear technology had increases for Q1 with both forms of DA, and classified government information had Q1 increase when paired with the actor statement. All of the other questions had negative deltas. The average change with DA across the three subtopics and three questions was -0.057 for the actor and -0.208 for the receiver (refer to the appendix for these averages in more detail).

III. Perception Shift within Privacy

Privacy was the least vulnerable to manipulation based on the results collected from this survey. Specifically, privacy of personal information had less increases than privacy of American companies. Additionally, not a single prompt was effective in increasing the fear of imminence (Q2) as related to privacy. The baseline knowledge for privacy was the highest at 4.81 (red: 4.60, green: 4.69, purple: 5.13).

Deleted agent of the passive was not effective for either subtopic; there was not a single question where the delta between the baseline answers and the prompted answers was positive. Additionally, every question had a majority of participants who viewed the threat as less or equally threatening, and all but four (out of twelve) questions had a higher average decrease than average increase; there was no pattern for the form of DA with those increases. The broad average delta for the three questions and two subtopics was -0.573 for the actor statement and -0.285 for the receiver statement.

For experiencer deletion, neither subtopic saw increases with Q2. However, privacy of personal information did have a larger average increase than decrease. The other two questions had increases for both subtopics; Q1 had larger increases than Q3. Therefore, it had the most positive impact on how worried participants felt about privacy. The average change across the three questions was +0.173, again with Q1 having the largest average delta out of the three questions (+0.455). This linguistic device was the most effective tool for manipulation for the topic privacy.

Nominal compounds had no effect on privacy for personal information and a minor positive impact on privacy of American companies. Personal information had negative deltas for all three questions; it also had higher average decreases than increases and a majority of participants who saw privacy as being less or equally threatening. However, nominal compounds had a minor increase with Q1 (+0.25) and Q3 (+0.13) when paired with privacy of American companies. However, none of the three questions had a majority increase their perception, nor did any of them have a

larger increase than decrease. The overall effect across both subtopics and the three questions was -0.313.

IV. Perception Shift within Cyber War

The most significant shifts in perception occurred in relation to cyber war. Neither of the subtopics stood out as being more easily influenced than the other. Cyber war had the lowest reported base knowledge out of the three main topics with 3.51 (red: 3.70, green: 3.03, purple: 3.81). Q3 saw a positive increase with every linguistic device.

Experiencer deletion was the least effective combination compared to the other linguistic changes and cyber war; however, cyber war was the most effective topic for experiencer deletion. Both subtopics had an increase with Q3 and one other, but they differed on which other question increased; for cyber war with another country, Q1 increased (+0.15), and cyber war with a terrorist organization saw an increase for Q2 (+0.22). For both subtopics, Q3 had the larger delta from base (compared to the other question increasing) and had 50% of participants increase their perception. Every question had a larger average increase than decrease. The overall effectiveness of ED on cyber war was +0.76.

Nominal compounds were the second most effective linguistic device for cyber war. Again, cyber war was the topic with the most increases for nominal compounds. Almost every question for the two subtopics had an increase; the one exception was Q2 with the country subtopic having no change from the base response to the prompted response. Q3 had the largest delta for both subtopics out of the three questions. Additionally, almost every question had a larger average increase than decrease; the only one that didn't was Q2 and a cyber war with a terrorist organization. The average

overall impact nominal compounds had on cyber war was +0.645 with Q3 being the highest (+1.15), Q1 being next (+0.65), and Q2 being the least (+0.14).

Finally, deleted agent of the passive was the most effective linguistic device for increasing perception of the threat of cyber war. Cyber war, again, was the topic with the most significant increases for deleted agent of the passive as well. Every single question had an increase; this included every combination among the forms of DA and the subtopics of cyber war. The most effective combinations were the actor form with the terrorist subtopic and the receiver form with the country subtopic. Across all four prompt sets, Q3 consistently had the largest delta from the base responses to the prompted responses. Q1 had the second largest delta, and Q2 had the smallest deltas. In addition to every question having a positive delta, every question also had a larger average increase than average decrease. The overall impact of the actor statement on cyber war was +0.925, and the receiver statement's impact was +1.002.

Discussion

Although this study was focused on determining which linguistic devices capable of being employed within threat inflation were effective on increasing perception, none of the devices were equally effective across the three topics. Rather, the most patterns resided within the topics themselves. For example, cyber war was influenced by every linguistic device while privacy was only impacted by experiencer deletion. Therefore, the data proves that there is no one lethal linguistic tool for manipulating perception; instead, the most effective manipulation occurs within nuanced pairings.

As previously mentioned, cyber war was the only topic to have the threat be perceived as greater with every linguistic device. Additionally, cyber war was the topic with the largest deltas from the baseline for each of the linguistic changes. There are a few reasons this could be true. The first is that the world has yet to see a full-fledged cyber war, and therefore it's likely that participants have fewer personal experiences to consider while assessing the risk. That said, participants might be more easily influenced by manipulated statements such as the ones in this study. The second interesting aspect with cyber war is that it was the topic with the lowest average baseline knowledge (3.51). This relates back to the fact that cyber war has not yet happened on a global, far-reaching scale. However, the numerical identification of participants seeing this topic as the one they know the least about and it being the one with the largest degree of successful manipulation creates an interesting connection. Further research regarding this connection would be useful to understand the full implications of it and to understand how the less educated someone is changes how

malleable they are to manipulation. It is also possible that the shifts were greater than with the other topics because participants rated their initial perception lower due to not knowing what cyber war was. Out of the 94 responses, 14 participants indicated that they did not know what cyber war was for the written question in the base perception. Although this is not the majority of participants, it is the only topic where any participants did not know what cyber war is or had never heard of it.

Another interesting pattern was that although a minority percentage of participants would have their perception increase, the degree of that increase could be significantly greater than the degree of the average decrease. This raises the question of what is more important: the number of people who are having their perception altered or the degree in which it's altered? Additionally, there are instances where the average decrease and percentage of participants with a decreased or equal perception of the threat were greater, but the overall shift from the baseline to the prompt increased. This will be addressed more in depth in limitations, but it highlights the myriad of interpretations that can arise from this data depending on what someone wants to focus on.

A consistent finding across all of the topics and linguistic changes was that participants would report in the written question of the survey that their perception was unchanged, however, their numbers would be different from that participants' baseline numbers. There were 284 instances across the three sets where participants reported their perception stayed the same, but at least one of their answers for the three questions was different. Out of those instances, 185 participants had their perception decrease numerically and 99 participants had their perception increase numerically. Either these

findings were a result of subconscious perception change or self-report error. If it is the former, it could mean that the large number of individuals who had their perception decrease despite stating they do not see the threat differently could speak to how hearing about a threat repeatedly can result in subconsciously becoming numb to it. Another possibility is that individuals were able to identify these statements as being manipulated, even if subconsciously, and therefore take them less seriously. The participants who reported no change but numerically had a positive shift could indicate the subtle linguistic, subconscious manipulation that occurs. Again, this could be attributed to self-report error, but it is an interesting pattern that points to statements adjusting how people perceive issues even if they don't realize that adjustment is happening.

Nominal compounds saw mixed success across the three topics. It was essentially ineffective for privacy, slightly effective for hacking, and the most effective with cyber war. The results from the question (Q4) prompting a written response offered further insight into its impact on participants, and the results were mixed. For some, the comparison of cybersecurity topics with major catastrophes in the US heightened the fear, and for others, it was seen as "hyperbolic", "offensive", and other phrases suggesting the comparison was poor or overdramatic. Cyber war had 8 participants who identified in their written answer that the comparison was valid and impactful due to their associations with the known catastrophe. There were also 8 participants who saw the prompts as "dramatic" or "dissonant" (as two examples of adjectives used). However, that was the only topic in which the two sides of the spectrum were equal. Both hacking and privacy had more participants identify the

comparison as being dramatic than valid. Hacking had 7 instances where individuals perceived hacking as being more threatening due to their new association with the catastrophes in the prompt. Alternatively, there were 15 instances where the comparison was not taken seriously. For privacy, there were 7 instances where participants perceived the comparison as valid. However, unlike the other topics, all 7 of those instances occurred from a single prompt, which was the one relating compromised privacy of American companies to a cyber-9/11. The prompt where personal privacy being compromised was likened to a cyber-Pearl Harbor did not have a single person who took the comparison seriously. Across the two subtopics of privacy, there were 13 instances of the comparison being ridiculed (personal privacy: 8, American companies: 5). This varying effectiveness across the three topics highlights how differently the linguistic devices can alter perception. Neither of the two other linguistic forms elicited written responses that ridiculed the prompt or felt it was hyperbolic. Therefore, this suggests nominal compounds can have the opposite effect from intended threat inflation and make individuals take the threat less seriously.

Deleted agent of the passive had both forms paired with each of the subtopics; however, the two forms did not have a striking difference in how they affected perception. This opposed the initial prediction which was that the statements focusing on the receiver would have a greater impact due to it being framed more personally on the participant. However, each form of DA was effective on varying occasions. Cyber war saw an increase with every question when paired with DA, but the most definitive increases occurred when the country subtopic was paired with the receiver statement, and the terrorism subtopic was paired with the actor statement. A similar difference

occurred with subtopics of hacking; the hacking of electrical grids was more influenced with receiver statements, whereas the hacking of nuclear technology increased more with actor statements. The through line across these increases and why the receiver statement is more potent with some subtopics while the actor statement more potent with others is something that requires further research. Doing so could help us understand the nuances of how Americans view threats in relation to themselves. It could be that Americans interact more with and therefore feel closer to certain issues in day-to-day life, such as electrical grids or relations with other countries, so they relate more to the receiver. On the other hand, issues that feel distant, such as nuclear weapons or terrorism, may be perceived as scarier when in the hands of an anonymous actor since it aligns with the feeling of it being out of someone's day-to-day reach. Again, this would require further research to identify if there is a pattern with how personally connected Americans feel to certain cybersecurity issues and subtopics.

Finally, experiencer deletion had mixed effects across the three broad topics. It was the most effective with both subtopics under cyber war, the hacking of electrical grids, the hacking of nuclear technology, and both subtopics under privacy. For cyber war and the hacking of electrical grids or nuclear technology, those are all scenarios to not yet happen in the United States and therefore not be covered in mainstream media frequently. Therefore, one explanation for experiencer deletion's vague wording being effective is that there are fewer real-life scenarios to compare the prompt to, and therefore a higher likelihood of participants ignoring the fact there is no credible source. However, privacy being compromised is something that has been occurring in the US on a mainstream level. Therefore, privacy does not fit into that pattern, and it is unclear

why experiencer deletion was so effective in that case. Another aspect to consider with experiencer deletion is that there is a possibility that participants are used to taking the news they read at face value without fact-checking. The very deletion of a firm source, which defines experiencer deletion, might not be different from some of the participants standard ways of consuming media. Therefore, it is important to consider that it might be a habit of not checking sources of claims that is influencing the effectiveness of experiencer deletion rather than the experiencer deletion itself.

Survey Limitations

This specific study examined the shift of perceptions from the baseline responses to the prompted responses. However, the data is nuanced and at times conflicting, which leads to a myriad of conclusions that can be drawn depending on which points of data are being looked at. An example of how they can be conflicting is that there are instances where there is a positive shift from the baseline responses to the prompted responses despite the majority of participants decreasing or maintaining their perception and the average decrease being greater than the average increase. This is due to participants' who reported "10" on their baseline understanding and maintained that 10 in their prompted response. Therefore, it did not contribute to the average increase or percent of those with an increased perception; however, it did contribute to the overall average and thus the shift from the baseline average to the prompted average. This same concept applies to the responses where "1" was maintained from the baseline response to the prompted response. However, since this study is specifically looking at means for increasing the perception, those results are less relevant to this research.

Another challenge is that the scope of the research was limited to a smaller subject pool of 94 participants. This is not representative of America and does not capture the diversity of thought and experiences that a nation-wide poll on perception would. 52 of the participants identified as a Democrat, liberal, or left leaning. Meanwhile, only 7 participants identified themselves as a Republican, conservative, or right-leaning. The other 35 participants spanned various political beliefs; some identified as independent, moderate, Centrist, Socialist, Communist, Marxist, unaffiliated, or they preferred not to disclose. Additionally, not all 50 states were represented, and it was not a nationally representative sample for age or race either. This survey could be more readily applied to the whole country if it were representing a sample of participants who reflected America's population. In theory, conclusions could be drawn about the sample population represented in this study; however, it could not be determined an anomaly or only applied to these demographics until the other demographics are equally surveyed.

Another limitation that was inherent to this form of research is the challenge of self-reporting and pre-existing bias. While this was attempted to be accounted for through the baseline perception, it undoubtedly exists. The self-report challenge refers to the human error that can occur in surveys. While participants were subject to the Prolific protocols such as attention checks, it is not as controlled as research conducted in a lab setting. Additionally, although there are established ways that rhetoric can be manipulated through linguistics, people also inherently have different associations with words. For example, there was one respondent who self-identified as a communist and wrote responses that were in favor of America enduring cybersecurity crises. This

individual was clearly an extreme outlier in terms of data collection, but it is a good example of how prior conceptions of these topics could influence responses.

Finally, some other self-imposed limitations that could be corrected for future research are changes to the survey. Each of the survey sets were randomly distributed, and each of the question sets were randomly organized within each participant's copy of the survey. The intention behind this choice was to mix up the order in which participants read the questions to prevent a repeated bias on the later questions from the prior questions. However, participants were not aware of this, so some individuals would include references to their previous answers in their written responses; since it was randomized, it was difficult to tell what they were referencing. There also were not baseline knowledge questions specific to the subtopics; if there had been, perhaps there would have been even deeper connections made to how perceived knowledge relates to manipulation. If I were to conduct this survey again, I would include a baseline question asking where the participants get their information about the specified cybersecurity topic. I would also ask what their highest level of education is as part of the demographics section and include something to understand their degree of scientific literacy. Either this would be done be asking what science they've studied in the past or conducting a short quiz on cybersecurity issues to avoid the self-report bias. Finally, I think it would've been valuable to include a final question asking how much each participant would want to invest in each of these areas for protection.

Conclusion

There was not a single linguistic device that was conclusively effective in positively increasing perception of a cybersecurity issue. However, there were combinations that elicited heightened fears of the topics. This suggests that the linguistic tools themselves are not as effective as an entity; rather what they're paired with is where the power and opportunity to manipulate is. Specifically, cyber war was the most likely topic to have participants' perception change. Given it was also the least known at the start of the survey according to participants, this research suggests the less Americans know about a cybersecurity issue, the more likely they are to increase their perception from manipulated facts. Despite there not being a specific linguistic device that was completely effective, this study highlighted the numerical possibility of strategic combinations between topics and manipulated language affecting perceptions of cybersecurity threats.

This research opens up a necessary dialogue for how Americans perceive linguistic shifts as related to key national security issues. While this is just a start to the many subjects that could be researched on the national security front, the results highlight that it is possible for claims without real facts and with manipulated language construction to change Americans perception of threats. There are direct 1:1 impacts on single prompts that are not designed to be informative, specific, or reliable impacting how fearful individuals are of cybersecurity topics. In the future, further research could help us understand exactly what makes certain combinations more effective than others, and what the long-term impacts of these perception shifts are.

Appendices

Appendix A: Survey Prompts

Base Perception:

"The following questions will ask about your current perception of **hacking** as a threat to the US (including hacking electrical grids, nuclear technology, classified government information, etc.):"

"The following questions will ask about your current perception of **cyber privacy** as a threat to the US (including compromised privacy of individuals, US companies, etc.):"

"The following questions will ask about your current perception of **cyber war** as a threat to the US (including with other countries, terrorist organizations, etc.):"

Red Test Set:

Hacking // Experiencer Deletion

Electrical grids:

- It seems as if the risk of US cities' electrical grids being hacked poses a serious danger to civilians.

Nuclear technology:

- The US may be facing a major threat in the form of American nuclear technology being hacked.

Classified government information:

- It appears classified US government information is at risk of being hacked.

Privacy // Deleted Agent of the Passive

Personal information:

- **Focus on receiver** As more of American's lives move into the virtual space, they are vulnerable to their private information being compromised, stolen, damaged, or tracked.
- **Focus on actor** There are actors, both in the US and globally, who compromise, steal, damage, and track American's private information that is in virtual spaces.

American companies:

- **Focus on receiver** Many American companies have transitioned away from paper records and instead have their business information in online drives. With this transition, more American companies have been victims of hacking.
- **Focus on actor** Some hackers target American companies' online infrastructure to access key operational information.

Cyber War // Nominal Compounds

Country:

- A cyber war with another country would be the equivalent to a cyber 9/11 for America. The impacts would be catastrophic, devastating, and an existential event.

Terrorist group:

- The next thing the US must brace itself for is a cyber war with a terrorist organization. If that day comes, the country will be facing a cyber-Hurricane Katrina.

Green Test Set:

Hacking // Nominal Compounds

Electrical grids:

- The possibility of infrastructure, such as America's electrical grids, being hacked would be the equivalent to a cyber 9/11 for America. The impacts would be catastrophic, devastating, and an existential event.

Nuclear technology:

- The next thing the US must brace itself for is America's nuclear technologies being attacked by hackers. If that day comes, the country will be facing a cyber-Pearl Harbor.

Classified government information:

- If the US government had classified information compromised by hackers it would be disastrous, like a Cyber Hurricane-Katrina.

Privacy // Experiencer Deletion

Personal information:

- The US may be facing a major threat in the form of American citizens private information being vulnerable within digital spaces.

American companies:

- It seems as if the risk of American companies having their privacy compromised poses a serious danger to businesses and civilians alike.

`

Cyber War // Deleted Agent of the Passive

Country:

- **Focus on receiver** As more of American infrastructure moves into the virtual space, the US and American citizens become vulnerable to damage in a cyber war with other countries.
- **Focus on actor** As other countries become more technologically sophisticated, they are more capable of waging cyber war.

Terrorist group:

- **Focus on receiver** It is possible that terrorist organizations will exploit technological vulnerabilities and conduct cyber war against American citizens and institutions.
- **Focus on actor** There are terrorist organizations, both in the US and globally, who are capable of instigating a cyber war.

Purple Test Set

Hacking // Deleted Agent of the Passive

Electrical grids:

- **Focus on receiver** As more US cities rely on centralized electrical grids, the cities and citizens are vulnerable to blackouts resulting from the grids being hacked.
- **Focus on actor** There are actors, both in the US and globally, who are capable of hacking the electrical grids that power entire US cities and causing widespread blackouts.

Nuclear technology:

- **Focus on receiver** While the US works hard to safeguard its nuclear infrastructure, much of the nuclear technology remains on digital platforms and at risk of being hacked.
- **Focus on actor** If hackers were to get past the securities in place to protect American nuclear systems, they would be capable of accessing America's nuclear technology.

Government classified information:

- **Focus on receiver** The US government has transitioned away from paper records and instead have more classified information in online drives. With

this transition, the US government's classified materials are more likely to be a victim of hacking.
- **Focus on actor** Some hackers target the American government's online infrastructure to access key classified information.

Privacy // Nominal Compounds

Personal info:
- If American citizens had their online privacy jeopardized it would be disastrous, like a cyber-Pearl Harbor.

American companies:
- The possibility of American companies having online, private information compromised would be the equivalent to a cyber 9/11 for America. The impacts would be catastrophic, devastating, and an existential event.

Cyber War // Experiencer deletion

Country:
- It seems as if the risk of a cyber war with another country poses a serious danger to America's institutions and civilians.

Terrorist group:
- The US may be facing a major threat in the form of a cyber war with a terrorist organization.

Appendix B: Red Survey Set Results

Table 4: Hacking and Experiencer Deletion Results

	# less	# same	# more	% inc	% dec	Avg. inc	Avg. dec	Δ from base
Electrical Grids Q1	10	5 (1 ten)	15	50%	50%	+2.27	-1.90	+0.50
Electrical Grids Q2	12	10 (4 tens)	8	27%	73%	+1.63	-1.67	-0.26
Electrical Grids Q3	11	10 (2 tens)	9	30%	70%	+2.44	-2.27	-0.10
Nuclear Tech Q1	5	10 (1 ten)	15	50%	50%	+2.73	-3.20	+0.84
Nuclear Tech Q2	9	13 (4 tens)	8	27%	73%	+2.13	-2.00	-0.03
Nuclear Tech Q3	13	10 (2 tens)	7	23%	77%	+2.29	-2.38	-0.50
Classified Info Q1	14	7 (1 one) (1 ten)	9	30%	70%	+2.00	-2.79	-0.70
Classified Info Q2	17	9 (3 tens)	4	13%	87%	+1.25	-2.00	-0.96
Classified Info Q3	18	8 (2 tens)	4	13%	87%	+2.00	-3.28	-1.70

Table 5: Privacy and Deleted Agent of the Passive Results

	# less	# same	# more	% inc	% dec	Avg. inc	Avg. dec	Δ from base
Personal / Receiver Q1	13	5	12	40%	60%	+2.00	-2.31	-0.20
Personal / Receiver Q2	15	10 (3 tens)	5	17%	83%	+1.40	-1.87	-0.70
Personal / Receiver Q3	13	8 (1 ten)	9	30%	70%	+2.11	-1.85	-0.17
Personal / Actor Q1	13	9	8	27%	73%	+2.38	-1.92	-0.20
Personal / Actor Q2	14	11 (4 tens)	5	17%	83%	+2.00	-2.00	-0.60
Personal / Actor Q3	14	8 (2 tens)	8	27%	73%	+1.75	-1.79	-0.37
Companies / Receiver Q1	12	7 (1 ten)	11	37%	63%	+2.00	-1.92	N/C
Companies / Receiver Q2	13	10 (4 tens)	7	23%	77%	+1.71	-2.15	-0.54
Companies / Receiver Q3	12	8 (2 tens)	10	33%	67%	+1.60	-1.58	-0.10
Companies / Actor Q1	13	7 (1 ten)	10	33%	67%	+2.00	-2.46	-0.40
Companies / Actor Q2	12	12 (5 tens)	6	20%	80%	+2.67	-2.92	-0.64
Companies / Actor Q3	18	4 (2 tens)	8	27%	73%	+1.38	-2.72	-1.23

Table 6: Cyber War and Nominal Compounds Results

	# less	# same	# more	% inc	% dec	Avg. inc	Avg. dec	Δ from base
Country Q1	8	10 (4 tens)	12	40%	60%	+2.83	-1.75	+0.67
Country Q2	10	12 (5 tens)	8	27%	73%	+2.50	-2.00	N/C
Country Q3	7	8 (2 tens)	15	50%	50%	+2.93	-1.14	+1.20
Terrorist Org. Q1	6	11 (4 tens)	13	43%	57%	+2.69	-2.67	+0.63
Terrorist Org. Q2	8	10 (4 tens)	12	40%	60%	+2.75	-3.13	+0.27
Terrorist Org. Q3	7	9 (2 tens)	14	47%	53%	+2.50	-2.14	+1.10

Appendix C: Green Survey Set Results

Table 7: Hacking and Nominal Compounds Results

	# less	# same	# more	% inc	% dec	Avg. inc	Avg. dec	Δ from base
Electrical Grids Q1	6	11 (1 one) (1 ten)	15	47%	53%	+2.13	-2.17	+0.59
Electrical Grids Q2	10	7 (1 one) (1 ten)	15	47%	53%	+2.00	-2.20	+0.25
Electrical Grids Q3	7	5 (2 ones)	20	63%	37%	+2.45	-1.71	+1.13
Nuclear Tech Q1	14	10 (1 one)	8	25%	75%	+3.00	-2.21	-0.25
Nuclear Tech Q2	14	10 (1 one) (1 ten)	8	25%	75%	+2.63	-2.64	-0.50
Nuclear Tech Q3	7	10 (3 tens)	15	47%	53%	+2.33	-3.29	+0.38
Classified Info Q1	16	8 (1 one) (1 ten)	8	25%	75%	+2.25	-1.56	-0.22
Classified Info Q2	18	5 (1 one) (1 ten)	9	28%	72%	+1.89	-1.44	-0.29
Classified Info Q3	11	9 (3 ones)	12	38%	62%	+2.42	-1.82	+0.04

Table 8: Privacy and Experiencer Deletion Results

	# less	# same	# more	% inc	% dec	Avg. inc	Avg. dec	Δ from base
Personal Q1	11	9 (1 ten)	12	38%	62%	+1.75	-1.82	+0.50
Personal Q2	13	10 (2 tens)	9	28%	72%	+2.00	-1.54	-0.03
Personal Q3	9	12 (1 one) (1 ten)	11	34%	66%	+1.91	-1.56	+0.13
Companies Q1	14	7 (1 ten)	11	34%	66%	+2.00	-1.50	+0.41
Companies Q2	12	12 (2 tens)	8	25%	75%	+1.25	-1.67	-0.25
Companies Q3	11	6 (1 ten)	15	47%	53%	+1.80	-1.64	+0.28

Table 9: Cyber War and Deleted Agent of the Passive Results

	# less	# same	# more	% inc	% dec	Avg. inc	Avg. dec	Δ from base
Country / Receiver Q1	12	5 (1 one)	15	47%	53%	+2.80	-1.67	+1.06
Country / Receiver Q2	9	11 (1 one) (1 ten)	12	38%	62%	+2.17	-1.33	+0.47
Country / Receiver Q3	8	8 (3 tens)	16	50%	50%	+3.06	-1.50	+1.40
Country / Actor Q1	10	9 (1 one)	13	41%	59%	+2.00	-1.70	+0.41
Country / Actor Q2	10	10 (2 ones) (1 ten)	12	38%	62%	+1.67	-1.50	+0.22
Country / Actor Q3	6	10 (3 ones)	16	50%	50%	+2.44	-1.17	+1.12
Terrorist Org. / Receiver Q1	7	8 (1 one)	17	53%	47%	+2.41	-1.86	+0.94
Terrorist Org. / Receiver Q2	6	15 (1 one) (1 ten)	11	34%	66%	+2.55	-1.50	+0.59
Terrorist Org. / Receiver Q3	5	9 (3 ones)	18	56%	44%	+2.72	-1.00	+1.43
Terrorist Org. / Actor Q1	5	8 (1 one)	19	59%	41%	+2.68	-2.00	+1.28
Terrorist Org. / Actor Q2	6	9 (1 one) (1 ten)	17	53%	47%	+1.94	-1.33	+0.84
Terrorist Org. / Actor Q3	4	9 (3 ones)	19	59%	41%	+2.89	-1.00	+1.68

Appendix D: Purple Survey Set Results

Table 10: Hacking and Deleted Agent of the Passive Results

	# less	# same	# more	% inc	% dec	Avg. inc	Avg. dec	Δ from base
Electrical Grid / Receiver Q1	9	10 (3 tens)	13	41%	59%	+2.62	-2.11	+0.47
Electrical Grid / Receiver Q2	8	12 (4 tens)	12	38%	62%	+2.00	-2.00	-0.31
Electrical Grid / Receiver Q3	11	9 (2 tens)	12	38%	62%	+2.75	-2.00	+0.35
Electrical Grid / Actor Q1	11	8 (2 tens)	13	41%	59%	+2.38	-2.18	+0.22
Electrical Grid / Actor Q2	13	7 (3 tens)	12	38%	62%	+1.75	-2.38	-0.56
Electrical Grid / Actor Q3	12	7 (2 tens)	13	41%	59%	+2.15	-2.50	-0.06
Nuclear Tech / Receiver Q1	12	7 (3 tens)	13	41%	59%	+2.15	-2.17	+0.15
Nuclear Tech / Receiver Q2	10	11 (3 tens)	11	34%	66%	+1.55	-1.90	-0.31
Nuclear Tech / Receiver Q3	15	4 (2 tens)	13	41%	59%	+1.85	-1.80	-0.06
Nuclear Tech / Actor Q1	6	7 (3 tens)	19	59%	41%	+2.16	-3.17	+0.69
Nuclear Tech / Actor Q2	9	13 (4 tens)	10	31%	69%	+1.30	-2.11	-0.44

Nuclear Tech / Actor Q3	15	7 (2 tens)	10	31%	69%	+2.40	-2.00	-0.18
Classified Info / Receiver Q1	14	8 (3 tens)	10	31%	69%	+2.00	-2.29	-0.38
Classified Info / Receiver Q2	12	10 (3 tens)	10	31%	69%	+1.40	-2.25	-0.66
Classified Info / Receiver Q3	17	10 (2 tens)	5	16%	84%	+2.20	-2.76	-1.12
Classified Info / Actor Q1	12	7 (2 tens)	13	41%	59%	+2.38	-2.42	+0.47
Classified Info / Actor Q2	11	10 (4 tens)	11	34%	66%	+1.82	-2.18	-0.38
Classified Info / Actor Q3	16	7 (2 tens)	9	28%	72%	+2.56	-2.50	-0.27

Table 11: Privacy and Nominal Compounds Results

	# less	# same	# more	% inc	% dec	Avg. inc	Avg. dec	Δ from base
Personal Q1	14	9 (4 tens)	9	28%	72%	+2.22	-2.86	-0.63
Personal Q2	13	14 (2 tens)	5	16%	84%	+2.80	-3.08	-0.81
Personal Q3	14	8	10	31%	69%	+2.60	-3.07	-0.40
Companies Q1	10	8 (3 tens)	14	44%	56%	+2.36	-2.50	+0.25
Companies Q2	11	9 (1 ten)	12	38%	62%	+2.08	-2.73	-0.15
Companies Q3	11	8	13	41%	59%	+2.69	-2.82	+0.13

Table 12: Cyber War and Experiencer Deletion Results

	# less	# same	# more	% inc	% dec	Avg. inc	Avg. dec	Δ from base
Country Q1	12	10 (1 one) (1 ten)	10	31%	69%	+2.70	-1.83	+0.15
Country Q2	13	9	10	31%	69%	+2.50	-2.23	-0.12
Country Q3	8	8 (1 one) (1 ten)	16	50%	50%	+2.88	-2.13	+0.90
Terrorist Org. Q1	12	12 (2 ones) (2 tens)	8	25%	75%	+2.75	-1.83	-0.44
Terrorist Org. Q2	10	11 (1 one) (2 tens)	11	34%	66%	+2.09	-1.60	+0.22
Terrorist Org. Q3	9	7 (1 ten)	16	50%	50%	+2.45	-2.11	+0.81

Appendix E: Hacking Changes by Question and Subtopic

Question 1:

Table 13: Hacking and Question 1 Results

	Baseline Knowledge:	Baseline Question:	Prompted Question:	Change from Baseline Q:	
ED / Electrical Grids	4.77	6.63	7.13	+ 0.50	
ED / Nuclear Tech	4.77	6.63	7.47	+ 0.84	
ED / Classified Govt. Info	4.77	6.63	5.93	- 0.70	
DA / Electrical grids (R)	4.47	6.69	7.16	+ 0.47	-
DA / Electrical grids (A)	4.47	6.69	6.91	+ 0.22	
DA / nuclear tech (R)	4.47	6.69	6.84	+ 0.15	
DA / nuclear tech (A)	4.47	6.69	7.38	+ 0.69	
DA / classified govt. info (R)	4.47	6.69	6.31	- 0.38	
DA / classified govt. info (A)	4.47	6.69	7.16	+ 0.47	
NC / Electrical Grids	4.41	5.91	6.50	+ 0.59	
NC / nuclear tech	4.41	5.91	5.66	- 0.25	
NC / classified govt. info	4.41	5.91	5.69	- 0.22	

How worried does hacking make you make you? (1 = not at all worried, 5 = indifferent, 10 = very worried)

Question 2:

Table 14: Hacking and Question 2 Results

	Baseline Knowledge:	Baseline Question:	Prompted Question:	Change from Baseline Q:	
ED / Electrical Grids	4.77	6.93	6.67	- 0.26	
ED / Nuclear Tech	4.77	6.93	6.90	- 0.03	
ED / Classified Govt. Info	4.77	6.93	5.97	- 0.96	
DA / Electrical grids (R)	4.47	7.47	7.16	- 0.31	
DA / Electrical grids (A)	4.47	7.47	6.91	- 0.56	
DA / nuclear tech (R)	4.47	7.47	7.16	- 0.31	
DA / nuclear tech (A)	4.47	7.47	7.03	- 0.44	
DA / classified govt. info (R)	4.47	7.47	6.81	- 0.66	
DA / classified govt. info (A)	4.47	7.47	7.09	- 0.38	
NC / Electrical Grids	4.41	6.13	6.38	+ 0.25	
NC / nuclear tech	4.41	6.13	5.63	- 0.50	
NC / classified govt. info	4.41	6.13	5.84	- 0.29	

How imminent of a threat do you see hacking as? (1 = not at all imminent, 5 = indifferent, 10 = very imminent)

Question 3:

Table 15: Hacking and Question 3 Results

	Baseline Knowledge:	Baseline Question:	Prompted Question:	Change from Baseline Q:	
ED / Electrical Grids	4.77	6.60	6.50	- 0.10	
ED / Nuclear Tech	4.77	6.60	6.10	- 0.50	
ED / Classified Govt. Info	4.77	6.60	4.90	- 1.70	
DA / Electrical grids (R)	4.47	6.56	6.91	+ 0.35	
DA / Electrical grids (A)	4.47	6.56	6.50	- 0.06	
DA / nuclear tech (R)	4.47	6.56	6.50	- 0.06	
DA / nuclear tech (A)	4.47	6.56	6.38	- 0.18	
DA / classified govt. info (R)	4.47	6.56	5.44	- 1.12	
DA / classified govt. info (A)	4.47	6.56	6.29	- 0.27	
NC / Electrical Grids	4.41	5.25	6.38	+ 1.13	
NC / nuclear tech	4.41	5.25	5.63	+ 0.38	
NC / classified govt. info	4.41	5.25	5.29	+ 0.04	

How likely do you think it is for you personally to be affected by hacking? (1 = not at all likely, 5 = indifferent, 10 = very likely)

Appendix F: Privacy Changes by Question and Subtopic

Question 1:

Table 16: Privacy and Question 1 Results

	Baseline Knowledge:	Baseline Question:	Prompted Question:	Change from Baseline Q:	
ED / Personal Info	4.69	5.78	6.28	+ 0.50	
ED / American Companies	4.69	5.78	6.19	+ 0.41	
DA / Personal Info (R)	4.60	6.93	6.73	- 0.20	
DA / Personal Info (A)	4.60	6.93	6.73	- 0.20	
DA / American companies (R)	4.60	6.93	6.93	N/C	
DA / American companies (A)	4.60	6.93	6.53	- 0.40	
NC / Personal info	5.13	6.41	5.78	- 0.63	
NC / American companies	5.13	6.41	6.66	+ 0.25	

How worried does cyber privacy make you? (1 = not at all worried, 5 = indifferent, 10 = very worried)

Question 2:

Table 17: Privacy and Question 2 Results

	Baseline Knowledge:	Baseline Question:	Prompted Question:	Change from Baseline Q:	
ED / Personal Info	4.69	6.50	6.47	- 0.03	
ED / American Companies	4.69	6.50	6.25	- 0.25	
DA / Personal Info (R)	4.60	7.17	6.47	- 0.70	
DA / Personal Info (A)	4.60	7.17	6.57	- 0.60	
DA / American companies (R)	4.60	7.17	6.63	- 0.54	
DA / American companies (A)	4.60	7.17	6.53	- 0.64	
NC / Personal info	5.13	6.84	6.03	- 0.81	
NC / American companies	5.13	6.84	6.69	- 0.15	

How imminent of a threat do you see cyber privacy as? (1 = not at all imminent, 5 = indifferent, 10 = very imminent)

Question 3:

Table 18: Privacy and Question 3 Results

	Baseline Knowledge:	Baseline Question:	Prompted Question:	Change from Baseline Q:	
ED / Personal Info	4.69	6.00	6.13	+ 0.13	
ED / American Companies	4.69	6.00	6.28	+ 0.28	
DA / Personal Info (R)	4.60	6.70	6.53	- 0.17	
DA / Personal Info (A)	4.60	6.70	6.33	- 0.37	
DA / American companies (R)	4.60	6.70	6.60	- 0.10	
DA / American companies (A)	4.60	6.70	5.47	- 1.23	
NC / Personal info	5.13	6.28	5.88	- 0.40	
NC / American companies	5.13	6.28	6.41	+ 0.13	

How likely do you think it is for you personally to be affected by cyber privacy? (1 = not at all likely, 5 = indifferent, 10 = very likely)

Appendix G: Cyber War Changes by Question and Subtopic

Question 1:

Table 19: Cyber War and Question 1 Results

	Baseline Knowledge:	Baseline Question:	Prompted Question:	Change from Baseline Q:	
ED / Country	3.81	6.38	6.53	+ 0.15	
ED / Terrorism	3.81	6.38	5.94	- 0.44	
DA / Country (R)	3.03	4.78	5.84	+ 1.06	
DA / Country (A)	3.03	4.78	5.19	+ 0.41	
DA / Terrorism (R)	3.03	4.78	5.72	+ 0.94	
DA / Terrorism (A)	3.03	4.78	6.06	+ 1.28	
NC / Country	3.70	5.90	6.57	+ 0.67	
NC / Terrorism	3.70	5.90	6.53	+ 0.63	

How worried does cyber war make you? (1 = not at all worried, 5 = indifferent, 10 = very worried)

Question 2:

Table 20: Cyber War and Question 2 Results

	Baseline Knowledge:	Baseline Question:	Prompted Question:	Change from Baseline Q:	
ED / Country	3.81	6.78	6.66	- 0.12	
ED / Terrorism	3.81	6.78	7.00	+ 0.22	
DA / Country (R)	3.03	5.44	5.91	+ 0.47	
DA / Country (A)	3.03	5.44	5.66	+ 0.22	
DA / Terrorism (R)	3.03	5.44	6.03	+ 0.59	
DA / Terrorism (A)	3.03	5.44	6.28	+ 0.84	
NC / Country	3.70	6.30	6.30	N/C	
NC / Terrorism	3.70	6.30	6.57	+ 0.27	

How imminent of a threat do you see cyber war as? (1 = not at all imminent, 5 = indifferent, 10 = very imminent)

Question 3:

Table 21: Cyber War and Question 3 Results

	Baseline Knowledge:	Baseline Question:	Prompted Question:	Change from Baseline Q:	
ED / Country	3.81	5.13	6.03	+ 0.90	
ED / Terrorism	3.81	5.13	5.94	+ 0.81	
DA / Country (R)	3.03	3.91	5.31	+ 1.40	
DA / Country (A)	3.03	3.91	5.03	+ 1.12	
DA / Terrorism (R)	3.03	3.91	5.34	+ 1.43	
DA / Terrorism (A)	3.03	3.91	5.59	+ 1.68	
NC / Country	3.70	4.93	6.13	+ 1.20	
NC / Terrorism	3.70	4.93	6.03	+ 1.10	

How likely do you think it is for you personally to be affected by cyber war? (1 = not at all likely, 5 = indifferent, 10 = very likely)

Appendix H: Average Shifts for Each Linguistic Change Across Broad Topics

Nominal Compounds:

Table 22: Nominal Compounds Average Shifts Across Broad Topics

	Q1	Q2	Q3	TOTAL
HACKING	+0.04	-0.18	+0.52	+0.126
PRIVACY	-0.19	-0.48	-0.27	-0.313
CYBER WAR	+0.65	+0.14	+1.15	+0.645
TOTAL	+0.167	-0.175	+0.466	+0.458

Experiencer Deletion:

Table 23: Experiencer Deletion Average Shifts Across Broad Topics

	Q1	Q2	Q3	TOTAL
HACKING	+0.213	-0.42	-0.77	-0.324
PRIVACY	+0.46	-0.14	+0.21	+0.173
CYBER WAR	-0.15	+0.05	+0.86	+0.760
TOTAL	+0.218	-0.507	+0.293	+0.004

Deleted Agent of the Passive:

Table 24: Deleted Agent of the Passive Average Shifts Across Broad Topics

	Q1	Q2	Q3	TOTAL
HACKING RECEIVER	+0.08	-0.43	-0.28	-0.208
HACKING ACTOR	+0.46	-0.46	-0.17	-0.057
PRIVACY RECEIVER	-0.10	-0.62	-0.14	-0.285
PRIVACY ACTOR	-0.30	-0.62	-0.80	-0.573
CYBER WAR RECEIVER	+1.00	+0.59	+1.42	+1.002
CYBER WAR ACTOR	+0.85	+0.53	+1.40	+0.925
TOTAL RECEIVER	+0.327	-0.153	+0.334	+0.170
TOTAL ACTOR	+0.335	-0.183	+0.143	+0.098

Appendix I: Base Knowledge Averages

Table 25: Base Knowledge Averages

	RED	GREEN	PURPLE	TOTAL
HACKING	4.77	4.41	4.47	4.55
PRIVACY	4.60	4.69	5.13	4.81
CYBER WAR	3.70	3.03	3.81	3.51

Bibliography

Bakker, Bert N., et al. "Hot Politics? Affective Responses to Political Rhetoric." *American Political Science Review*, vol. 115, no. 1, 9 Sept. 2020, www.cambridge.org/core/journals/american-political-science-review/article/hot-politics-affective-responses-to-political-rhetoric/DD2E00B93E17141F6A5198509C2CB794.

Bolinger, Dwight. "Truth Is a Linguistic Question." *Language*, vol. 49, no. 3, Sept. 1973, doi.org/10.2307/412350.

Brito, Jerry, and Tate Watkins. "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy." *Harvard Law School National Security Journal*, vol. 3, no. 1, 2011, harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Brito-and-Watkins.pdf.

Cavanaugh, Jeffrey M. "From the 'Red Juggernaut' to Iraqi MWD: Threat Inflation and How It Succeeds in the United States." *Political Science Quarterly*, vol. 122, no. 4, winter 2007, pp. 555-84, www.jstor.org/stable/20202927.

Cramer, Jane K. *American Foreign Policy and the Politics of Fear*. Routledge, 2009.

Flynn, D. J., et al. "The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs about Politics." *Political Psychology*, vol. 38, no. S1, Feb. 2017, pp. 127-50, https://doi.org/10.1111/pops.12394.

Gil, Marta. "Emotions and Political Rhetoric: Perception of Danger, Group Conflict and he Biopolitics of Fear." *Human Affairs*, vol. 26, no. 2, 6 Apr. 2016,

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton University Press, 1976.

Liu, Chu. "The Linguistics of Mass Persuasion: How Politicians Make 'Fetch' Happen (Part I)." JSTOR Daily, ITHAKA, 10 Feb. 2016, daily.jstor.org/the-linguistics-of-mass-persuasion-how-politicians-make-fetch-happen/.

Mok, Kenneth. "Cyber Threat or Cyber Threat Inflation? – Assessing the Risk to U.S. National Security." *Small Wars Journal*, 7 Aug. 2017, smallwarsjournal.com/jrnl/art/cyber-threat-or-cyber-threat-inflation-assessing-the-risk-to-us-national-security.

Mueller, John. "Public Opinion on War and Terror: Manipulated or Manipulating?" CATO Instititute, CATO Institute, 10 Aug. 2021, www.cato.org/white-paper/public-opinion-war-terror.

NSA/CSS Technical Cyber Threat Framework v.2. U.S. Department of Defense, 29 Nov. 2018, media.defense.gov/2019/Jul/16/2002158108/-1/-1/0/CTR_NSA-CSS-TECHNICAL-CYBER-THREAT-FRAMEWORK_V2.PDF.

Pennycook, Gordon, and David G. Rand. "Lazy, Not Biased: Susceptibility to Partisan Fake News Is Better Explained by Lack of Reasoning than by Motivated Reasoning." *Cognition*, vol. 188, July 2019, pp. 39-50, https://doi.org/10.1016/j.cognition.2018.06.011.

Thierer, Adam. "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle." *The Minnesota Journal of Law, Science and Technology*, 25 Jan. 2013, pp. 312-18, www.mercatus.org/publications/technology-and-innovation/technopanics-threat-inflation-and-danger-information.