Examining Potential Agreement Between Cybersecurity Stakeholders

Nicole M. Angelini

California Polytechnic State University, San Luis Obispo

Abstract

In the United States (US), the number of individuals affected by cyber-attacks has drastically increased in the past ten years. To determine how this problem should be addressed, we need to better understand stakeholder opinions. Currently, no research exists examining beliefs of cybersecurity stakeholders, both within the public sector and private industry, to understand their opinions regarding this problem. In this paper, I first examine the cybersecurity discourse to determine what problem definitions currently exist. Then, once the problem definitions are identified, I use them to map the opinions of cybersecurity stakeholders. From this I identified three groups of problem definitions, but when I tested these three groups against cybersecurity stakeholders, I found six different groups of stakeholder opinions rather than three. Overall, the results show that while the stakeholders agree in some areas, they disagree in many others. These areas of disagreement suggest further research is necessary to determine whether a problem definition could be leveraged to help mitigate the increasing problem of cybersecurity breaches.

INTRODUCTION

In the United States (US), the number of individuals affected by cyber-attacks has drastically increased in the past ten years (Verizon Wireless, 2016). For example, CNN Money finds that in 2014 alone, data breaches compromised personal information of 110 million Americans including medical information, credit cards, and social security numbers (Pagliery, 2014). Additionally, analysts with Juniper Research calculate that cybercrime will cost governments, corporations, and individuals $2.1 trillion annually by 2019 (Moar, 2015). Despite all of this, individuals in both the public and private sectors who work in cybercrime policy, that is cybersecurity stakeholders, disagree as to the extent to which cybercrime is an issue for contemporary politics. This disagreement is problematic, as it suggests that it may be impossible for stakeholders to effectively address this issue and mitigate, if not eliminate, cybersecurity attacks. The purpose of this exploratory research is to examine current cybersecurity stakeholder opinions regarding the cause of the increase in cybersecurity attacks.

The details behind different problem definitions provide an important representation of each group's beliefs and values. A problem definition is the complex process of how individuals characterize a particular problem (Rochefort & Cobb, 1994). A stakeholder's problem definition not only exemplifies how they view the problem, but also how they intend to solve the problem. If multiple problem definitions reach the agenda, several solutions to the problem may be enacted, but the problem itself might not be mitigated or resolved. Understanding how cybersecurity stakeholders define the problem of cybersecurity has implications for the development of the field of cybersecurity as it emerges.

Currently, the field of cybersecurity lacks a cohesive problem definition, as no comprehensive examination of the cybersecurity discourse exists. This discourse, including a

broad range of cybersecurity academic journals, periodicals, and books, remains disjointed, as stakeholders appear to disagree over key definitions[1]. Specifically, the discourse draws attention to several different reasons why cybersecurity attacks are rapidly increasing. Important stakeholders from private and public organizations are suggesting their own problem definitions as the discourse presents broad problem definitions. At the RSA Conference in May 2016, Admiral Mike Rodgers, the director of the National Security Agency and U.S. Cyber Command at that time, iterated this issue by explaining that private industry and the public sector were trapped in a battle of what cybersecurity solutions cannot be used, creating an impasse (Otto, 2016). Currently, no research systematically investigates cybersecurity stakeholders' problem definitions.

This paper begins by discussing the role and importance of problem definitions generally in public policy. The subsequent section identifies the problem definitions present in the current cybersecurity discourse. Using Q Sort methodology, I then investigate the patterns of beliefs of cybersecurity stakeholders. I then conclude with a discussion of the implications of my study and directions for future research.

PROBLEM DEFINTIONS

A problem definition is a statement that describes an individual's or group's values about why a situation is undesirable (Weiss, 1989). These statements demonstrate how a group views a problem, provides the rationale for the problem, what resources they can put towards the problem, and how they intend to address the problem (Guess & Farnham, 2000, p.7). Stakeholders use problem definition to shape the policy agenda surrounding the topic. When a

[1] See FISMA, 2000; NIST, 2015; "CIA Triad and Perkerian Hexad," 2013; Gordon & Ford, 2006; Finklea & Theohary, 2015 for discussion on other defintion disagreement within the field.

stakeholder determines the language and symbols of the problem definition, they maintain control over how the problem is understood (Rochefort & Cobb, 1994). With effective argumentation, stakeholder groups can place or remove beliefs on the agenda (Cobb & Elder, 1983). Depending on message and delivery, stakeholders can not only select the types of alternatives that are developed but also impact how the public perceives an issue. When a group can shape and control the problem definition, that group is also able to determine the alternative solutions to combat the issue.

Further, defining a problem definition has power, as it is not simply looking for the causality or the culpability of a situation; rather, it is looking to the different stakeholders and understanding their role in the situation (Dery, 1984; Rochefort & Cobb, 1994). When a problem is appropriately defined, not necessarily in any one stakeholder's interest, the problem definition has the power to solve or mitigate the problem it is defining. Examining the areas of similarities can promote collaboration, while examining the differences can uncover and possibly overcome certain challenges.

Incomplete problem definitions do not always solve the issue for several reasons. For example, sometimes stakeholders in power define the problem definition using preferred alternatives. This strategy is unsuccessful because the solution is not a cause and it narrows the possibility of effective solutions; it specifically and strategically maintains control for one group, while there are still competing problem definitions/stakeholder groups. Having multiple problem definitions also is ineffective as they can lead to different and sometimes conflicting problems and solutions making it on the agenda. This makes it difficult to address the problem holistically. An effective problem definition is multi-pronged, providing the capacity for support from multiple entities and the ability to effectively mitigate or even solve the problem (Rochefort &

Cobb, 1994). Few studies have comprehensively investigated definitions within the discourse to map the field of cybersecurity policy and effectively understand where the different stakeholders' perspectives lie. A major roadblock to good policy in cybersecurity is the varying and potentially contradictory problem definitions among stakeholder groups including those in the public, private, and subject matter expert sectors (Clark, 2011).

In fact, after surveying the discourse, I found that there was not one unifying definition. Rather, the discourse represents three distinct problem definitions: knowledge gap, regulation requirements, and purpose of the Internet. The first problem definition suggests that there is a perceived lack of expertise and knowledge regarding cybersecurity (see Singer & Friedman, 2014). The second definition suggests that some people fundamentally believe that there is not enough regulation (see Clarke & Knake, 2012). The last definition suggests that society believes that cybersecurity attacks are increasing because the purpose of the Internet at its inception was different than it is today (see Timberg, 2015). The following sections will examine these three problem definitions in more detail.

KNOWLEDGE GAP

The discourse suggests that individuals within the field of cybersecurity identify one possible problem definition type amongst stakeholders as a lack of cybersecurity knowledge in the population (Singer & Friedman, 2014). This definition refers to a lack of knowledge amongst lawmakers, law enforcement, executives and information technology employees in all sectors, and the general population. Broadly speaking, individuals do not know how to protect themselves or others, leaving major portions of cybersecurity vulnerable.

The overarching belief of those who subscribe to the knowledge gap problem definition believe that if the cybersecurity knowledge gap is not overcome, cyberattacks will continue to

increase. The knowledge gap is problematic because if lawmakers, at all levels, do not understand or do not use technology, they will be unable to develop laws to support safe practices on the Internet (Takala, 2016). If law enforcement officers do not understand technology or how to process cybercrime, then they will have a difficult time catching criminals and protecting the evidence against said criminals (Wolf, 2009).

Conditions surrounding this problem definition consider the lack of knowledge in several different types of people. The first considers the lack of knowledge in the general population, as people associated with this problem definition believe that the average individual does not understand best practices on how to protect their technology from cyber-attacks. Individuals can do simple things like change their passwords regularly or develop complex passwords that cannot be easily hacked. Yet, on average, 63 percent of people do not change their password frequently and use one password for multiple accounts (Ngo, 2010). A subset of the people who believe this problem definition believe that many Chief Information Officers or Chief Security Officers from all industries/sectors do not understand technology and cybersecurity. This is a problem because an executive's task is to lead their organizations in establishing safe practices. This level of understanding is even more relevant if these individuals in power are supposed to be highly knowledgeable in the fields of information technology and cybersecurity, or cyber Czars (Dillow, 2014). Another subset of this problem definition believe that employees are causing the increase in cyberattacks by being unable to protect their organization's proprietary information, allowing their organizations to fall victim to cyber-attacks.

Solutions to the knowledge gap problem definition vary widely. One solution suggests that governments and private corporations should engage in more public-private partnerships to develop, collaborate, and share information and resources (Wolf, 2009). Another solution argues

that if the average person does not know how to protect themselves, the government should develop a department, like the Center for Disease Control, to develop a nation-wide campaign to educate the population in cybersecurity (Singer & Friedman, 2014). Individuals who identify heavily with the government suggest that cyber-attacks are due to the lack of cybersecurity treaties with foreign governments, and that the US should diplomatically develop some (Goldsmith, 2011). Individuals typically associated with private industry argue that it is important to consider the current role of the US Government in dealing with the increase in number of attacks (Singer & Friedman, 2014). Specifically, although the DoD helped create the Internet, they no longer have the power to control it as private companies have taken over. As such, this group believes that rethinking the role of the U.S. government in the cybersecurity conversation might be necessary to mitigate the increase in cyber-attacks.

One critique of this problem definition is that even if the knowledge gap is a problem, it might not be possible to directly address the knowledge gap problem. Critics of these ideas that the U.S. should be trying to minimize the knowledge gap believe technology education cannot keep up with the pace of technology innovation.

REGULATION REQUIREMENTS

The discourse within the field of cybersecurity suggests that another potential problem definition focuses on the belief that the federal government needs to increase cybersecurity regulations on corporations and Internet Service Providers (ISPs) (Clarke & Knake, 2012). Specifically, individuals who prescribe to this definition broadly believe that the federal government is not regulating enough to ensure the protection of citizens. This group believes that increased regulation can mitigate cybersecurity risks.

This group believes that the government needs to implement regulation standards, otherwise cyberattacks will continue to increase. Proponents of this problem definition believe that ISPs are currently negligibly allowing customers to use their networks even when those customers' computers are being used maliciously (Rowe, Wood, Reeves, & Braun, 2011). If ISPs did not allow customers with infected computers to use their networks, at least until those computers were clean, they believe that the number of cyber-attacks would decrease. Other proponents of this problem definition believe that companies should do a better job of directly protecting their servers from cyber-attacks (Shinder, 2007). These proponents believe in strict regulations by the government to ensure companies are monitoring their servers and are constantly conducting penetration tests. Another offset trend is the belief that the government should impose regulations on the production of hardware and software. Currently, corporations are manufacturing their hardware and software overseas without guaranteeing that their products are free of malware and other problems (Lord, 2016). Proponents who believe there should be more regulation of the production process also believe that unless this is managed through regulation, the problem will continue to escalate.

Individuals in support of government regulation believe that corporations should be working towards meeting government regulation standards. This group believes that the U.S. government has the infrastructure and skillset to handle this issue through regulation. One way they believe this could be accomplished is by legally requiring ISPs to regulate the backbone of the Internet through automation, interoperability, and authentication (Clarke & Knake, 2012). Some of the individuals in this group remain frustrated because they believe that both Congress and the President, regardless of party control, are unwilling to regulate the standards for network security (Etzioni, 2014).

Individuals who subscribe to this belief do not necessarily believe the problem should be addressed in the same manner. For example, Clarke and Knake (2010) argue that one preferred solution is to develop and adopt a Cybersecurity Defensive Triad, which would mirror the Nuclear Defense Triad. This solution would include extensive standards and requirements to protect the backbone of the Internet, secure the power grid, and secure the supply chain of hardware and software. However, critics state that many resources have been allocated to develop plans like this, yet the U.S. is still experiencing an increase in attacks. As such, the US government should reallocate those resources towards figuring out how to physically stop or mitigate the rapid increase of attacks. Once some comprehensive measures are created, ISPs and corporations can use resources to understand the new methods.

Critics of increased regulation believe that compliance costs are increasing because the U.S. government does not know how to effectively regulate the cyber realm. Others also believe that increased regulation would lead to an increased amount of surveillance. With an increased amount of surveillance, more and more individuals would lose their privacy rights (Vanca, 2010).

PURPOSE OF THE INTERNET

The third problem definition category that presents itself in cybersecurity discourse stems from the creators of the Internet. This problem definition focuses on the original intent and design of the Internet, pointing out that it was never intended to serve the number of people it does today. This group broadly believes that since the Internet was not designed to accommodate the masses, it was bound to have problems.

The creators of Internet intended for researchers at different universities and institutes to share research with each other and not the populous. The creators of the Internet are unabashed

in their admission that they never expected or intended to allow others onto the Internet; now there are more than 3.2 billion users (Timberg, 2015). Due to the mismatch between design and use, the Internet's core structure lends itself to vulnerabilities that might have otherwise been avoidable. As Internet usage increases, vulnerabilities and cyber-attacks increase. Some proponents of this problem definition see value in increasing access to the Internet in that it has the power to be democratizing.

This viewpoint does not believe that the Internet is inherently bad, but that individuals are inherently trusting and as such fall victim to cyber-attacks. People are the ones violating one another rather than the Internet itself, regardless of whether or not it was intended for such use (Lanstein, 2009). Individuals who use the Internet to violate the privacy of others are considered bad actors and the creators and developers argue that they should not be held responsible for bad actors' behavior. Similarly, the creators of cars and highways are not responsible for those who drink and drive (Timberg, 2015). This viewpoint also suggests that because the creators of the Internet did not focus on protecting the user, expecting this automatic protection is unrealistic. The original intent of the Internet did not require the protection of valuable personal information like social security numbers.

Patch management, or "patching," which is the act of finding a problem with the code and fixing or strengthening it, is one way that different sectors try to mitigate problems with their technology (Chan, 2004). Patch management is standard among programmers who continue to develop their technology. A particular subgroup subscribes to the belief that Open Source software allows technology to be more adaptive and easy to edit as problems or vulnerabilities arise. If more individuals have the ability to verify the code, problems arise less often (Noyes, 2010). When the software is Open Source, more eyes can view the code and patch it when there

is an issue. Open Source software requires different groups to trust and police one another, thus keeping the technology safe. This group believes that increasing the number of individuals who are policing the technology can decrease the number of cybersecurity issues.

A critique of this problem definition is that increasing surveillance potentially violates individual rights. While more individuals monitoring the Internet and having access to the code could potentially mitigate cyberattacks, the Open Source population does not ensure that bad actors cannot use the community's culture to violate each other's privacy. While Open Source populations depend on reliability and accountability, they do not eliminate the possibility of bad actors.

RESEARCH APPROACH

Clearly, the cybersecurity policy discourse contains conflicting policy problems, rather than a singular approach that addresses the complex, interdependent drivers of the increase in cyberattacks in the US. In other words, the potentially contradictory problem definitions among stakeholder groups could be creating a major roadblock. Without understanding how different stakeholders view cybersecurity policy there is no way to understand the similarities and differences in their beliefs, making it difficult if not impossible to develop an effective problem definition.

Further, the discourse does not reveal if there is room for potential agreement and disagreement between each of these problem definitions. For example, individuals who believe that there is a cybersecurity knowledge gap in the general public may also believe that one way to fix it is through increased government regulation of the Internet. While this is possible, there is no proof that potential overlap exists amongst cybersecurity stakeholders, as evidenced by the

discourse. The purpose of this project is to determine whether the problem definitions presented in the discourse are reflected in the belief patterns of cybersecurity stakeholders.

METHODOLOGY

To explore subjective understandings of different cybersecurity stakeholders' problem definitions, I have chosen to use a method of analysis that was developed specifically to better understand individual's subjective opinion toward a topic: Q Sort. Twenty-eight stakeholders within the field of cybersecurity participated in the study. The following paragraphs will present the participants and recruitment, instrumentation, and analytical process.

Participants & Recruitment

To obtain participants for this study, I used a two-stage, modified snowball sampling process. In the first stage, I contacted upper-level administrators within the field of cybersecurity who provided me the contact information for several individuals who met the qualifications, discussed below, for my analysis. I then reached out these participants via e-mail. Once people agreed to participate, I mailed them a packet that included the Q Sort statements, a Q response sheet, the demographic questions, as well as instructions and an informed consent letter. I asked them to mail back the packed when completed. Additionally, I asked them if they knew anyone else in the field of cybersecurity who was qualified and might be interested in participating. If I did not receive a packet after several weeks, I emailed a second time requesting that the individuals return their packets of information.

I recruited participants to this research project who met specific qualifications. I included individuals who are involved in cybersecurity policy, meaning they are actively involved in the cybercrime arena. For example, a participant's job could be: to prevent cyber-attacks from harming people in their organization, to protect the infrastructure of their organization, to

educate the public or students about cybersecurity and cybercrime, to make vital decisions for the government in regards to cybersecurity, to research cybersecurity and/or consult others on best practices, or to be involved in active conversations trying to prevent future crimes from occurring. I recruited participants from a broad range of backgrounds including the state and federal government, private corporations, consulting firms, and universities. I actively excluded participants who might have experience in sales but not cybersecurity policy itself. I did this intentionally to ensure that the study includes individuals who understand the technology as well as the policy climate, rather than individuals who want to sell products aimed at eliminating cybersecurity threats.

Q Sort does not require a large N-sample, as it is not intended to generalize the public. Rather, Q Sort utilizes a small-n sample to better understand potential diversity of opinion (McKeown & Thomas, 2013). Therefore, I sought participants from diverse arenas with a wide range of expertise within appropriate fields. Recall that participants come from both the public sector and private industry. These individuals are from fields at a local, state, and federal level.

Instrumentation- Q Sample

I structured the Q Sample, or the statements used in the Q Sort, from the current discourse in the field of cybersecurity. For each problem definition, I developed statements within trends, conditions, preferred solutions, and critiques per the Lasswell Policy Orientation framework[2] **(**Lasswell, 1971). Across each of the three problem definitions areas (Knowledge Gap, Regulation Requirements, and Purpose of the Internet), I tried to keep the number of

[2] Please note that the Q Sort did not include the projections since the difference between the trends and projections did not seem to vary greatly within the cybersecurity discourse. Instead, I included a critique section since those values were also in the discourse but not well represented (Lasswell, 1951).

statements even; however, to best reflect the discourse, some sections were slightly larger than others. When the sample was presented to the participants, the statements were presented on separate cards in a random order to overcome potential bias.

[Insert Table 1 Here]

Q Sort was developed specifically to test participant subjectivity (Brown, 1991). It is contextually sensitive, meaning participants arrange the statements based off their experiences with the statement (Brown, 1991; Clarke, 2006; Vogel & Lowham, 2007). This allows me to learn about the subjective understandings of the problem definition of cybersecurity for each individual and group. For this study, participants were exposed to the 36 statements and were asked to place these statements in a semi-normal distribution from -5 for most disagreement to +5 for most agreement. This procedure follows standard practices in the field (see Clarke, 2006; Lowham & Lowham, 2015). I phrased some of the statements with the opposite valance to prompt responses of the participants. I informed the participants that they could deviate from the requested semi-normal distribution if it did not accurately represent their opinions. [3]

Analysis- Cluster Methodology

I analyzed the Q Sort data using a series of algorithmic methods to examine common themes among cybersecurity stakeholders' beliefs. To ensure robust clusters, I used a series of four cluster analyses, which use response data to organize like belief patterns into clusters. Such an analysis procedure effectively identifies clusters, or groups, of individuals who share similar beliefs surrounding cybersecurity and the best way to resolve cybersecurity issues. That is, the analysis finds stakeholders who share a common problem definition.

[3] I also asked the participants to answer a few questions regarding demographics including gender, ethnicity, highest degree, and subject matter of highest degree.

For this research study, I identified subjects as a cluster if three of the four analysis procedures clustered them together. [4] This led me to identify six different clusters, each representing a different understanding of the problem of cybersecurity. Seventy-eight percent of respondents are represented by the six clusters. The largest cluster consists of six respondents and the smallest consists of two.

RESULTS

To best understand the opinions of the six groups that emerged from the cluster analysis, I averaged each cluster's response to each statement (see Table 2). To develop each cluster's preferred problem definition, I focused on the opinions each cluster was most passionate about, identified by a mean with an absolute value of 2.5 or greater.

[Inset Table 2 here]

Overall, the sample group initially appears to hold different views on the problem of cybersecurity. Of the 36 statements, 15 had a range of nine or greater, meaning that on many of the questions participant responses varied greatly. No statements had a range five or less, indicating that overall there was no consensus on statements—including statements about the general pervasiveness of cybersecurity attacks. I considered any statement with a lower absolute value score to reflect low consensus within the cluster, or reflected a statement that the cluster was less passionate about. All clusters feel negatively about one statement, with four of the six clusters feeling strongly (-2.5 or less) about the statement. This statement focuses on the U.S.

[4] To ensure robustness of the clusters, I conducted a series of analyses using two measures of similarity, Pearson Correlation and Squared Euclidian, and two algorithms. With Pearson Correlation distance measure, I used Complete Linkage and Average Linkage; with Squared Euclidean distance measure, I used Complete Linkage and Ward Linkage. I then identified subjects as a cluster if they were grouped together by three of the four analyses.

government's lack of infrastructure and skillset to handle the problem of cybersecurity [21][5]. The following sections will present a closer examination of each cluster and their perspective problem definitions.

PUBLIC EDUCATION

Throughout the Q sample, this cluster believes that the public needs to be educated about cybersecurity. In fact, they were unique in their perspective regarding how the problem of cybersecurity should be addressed, specifically that cybersecurity policy should be considered like public health policy. This cluster is interesting because its participants all identify as part of the public sector (60% public sector, 40% consultants) and is made up of mostly women (60% female). (For complete demographic descriptions of all clusters, please see Table 3).

Overall, the Public Education cluster believes that as technology expands, the number of cyber-attacks increases [5]. The crux of their belief is grounded in the belief that humans are inherently trusting, and as such fall victim to cyber-attack [16]. Overall, increasing use and access to the Internet increases the potential for attacks. They do not believe that employees know how to protect their organization's proprietary information [17] and further that the government does not have the infrastructure and skillset to handle the problem of cybersecurity [21]. They differ from all other groups in their belief that a solution would be to implement cybersecurity policy structured like public health policy, focusing on teaching people how to best protect themselves [31].

COLLABORATIVE SOLUTION

The Collaborative Solution cluster believes that neither the government nor the private sector knows how to solve the problems of cybersecurity independently. Due to this, they believe

[5] Numbers in brackets represent the corresponding statement number for reference.

the two groups need to collaboratively work together to solve the problem. This cluster represents a hodgepodge of industries/sectors (50% as public, 33.3% as multiple fields, and 16.7% as private) and a majority female (66.7%).

Similar to the Public Education cluster, the Collaborative Solution cluster believes that that the population does not understand how to best protect their technology [14]. They believe that the government's role in cybersecurity should be reconsidered [28]. They believe that the U.S. government should implement the Cybersecurity Defensive Triad [26] and that private corporations should provide security solutions [29]. They believe that public-private partnerships are needed to develop solutions [25]. It is also important to note that this group does not believe that monitoring the Internet increases the likelihood that an individual's privacy will be violated [36].

GOVERNMENT SOLUTION

The individuals in the Government Solution cluster do not have a firmly established belief about who or what is causing the problems associated with cybersecurity; however, they believe that the government should implement a solution. This cluster has three participants, all men, each identifying with a different field.

The Government Solution cluster believes that ISPs should not allow customers to use their networks even when under cyberattack [4]. To fix the issues associated with cybersecurity, they believe that the U.S. government should focus on implementing the Cybersecurity Defensive Triad [26]. Not only do they believe that the government should focus on implementing the Cybersecurity Defensive Triad, they feel more strongly about this than any cluster feels about any statement (mean of 4.67). They do not believe that using Open Source Software is helpful in combatting this issue [24]. Similar to the Collaborative Solutions cluster,

they believe that implementing PPPs would be helpful [25]. As such, they realize that the role of the government needs readjusting [28], but that it has a vital role in finding a solution—particularly with the implementation of the Defensive Triad. Additionally, this group also believes that monitoring the Internet does not increase the likelihood that an individual's privacy will be violated [36].

PUBLIC PRIVATE PARTNERSHIP

Similar to the individuals in the Government Solution cluster, the Public Private Partnership cluster believes that the government does not have the capability to effectively solve this problem alone, nor should they. Rather than focusing on a government solution, as above, or on a combination of solutions like the Collaborative Solution cluster, this cluster believes that the focus should be on developing more Public Private Partnerships. This cluster identifies as male (100%) with all (3) identifying as having a master's degree as their highest degree.

Unlike other clusters, this cluster believes that increasing access to the Internet is a good thing [7], but that valuable assets reside on the Internet, which provides motivation for cyber-attacks [19]. They do not believe, however, that the government can solve the problem because it lacks the infrastructure or skillset to handle the problem of cybersecurity [21] and that it is not flexible enough to effectively regulate the cyber realm [35]. Unlike the collaborative cluster, they do not have strong feelings either way about whether private corporations should be providing security solutions independent of government regulation [29]. Interestingly, they seem to have a different understanding of leadership than the other groups and believe that not all U.S. government cybersecurity leaders must be technologically proficient [22]. This means that they look at leadership differently, perhaps believing that good leaders work well with other people and can direct people rather than necessarily having the skill themselves. They do believe, like

the Government Solution and the Collaborative Solution clusters, that public-private partnerships should be developed to solve cybersecurity issues [25]. However, of these three groups, they believe the strongest in the need for public private partnerships, which is the defining feature of this group.

FREE MARKET CYBERSECURITY

The Free Market Cybersecurity cluster does not believe that the government should have any role in mitigating the problems in cybersecurity. This cluster only has two participants, both of which are white males with master's degrees. One identifies as part of the public sphere and the other identities as part of the private sphere.

The Free Market cluster does not believe the government has the skillset or the infrastructure to help handle the problem of cybersecurity [21], nor does this group believe that the U.S. government is flexible enough to effectively regulate the cyber realm [35]. This group believes that ISPs should not be required to regulate the backbone of the Internet [9], and that private corporations should provide security solutions independent of government regulation [29]. They do not believe that the government should require organizations to adopt cybersecurity best practices [23], and they are adamantly against implementation of the Cybersecurity Triad [26]. Additionally, it is important to note that they strongly believe that monitoring the Internet increases the likelihood that an individual's privacy will be violated [36].

CORPORATE PROBLEM

The Corporate Problem group views the problem definition in a fundamentally different way than all the other clusters. Unlike the other clusters, which focus on trends and conditions, this cluster focuses on solutions. This group specifically believes that this is not a problem with the population or a problem with the government; rather, they believe that companies' inability

to protect themselves is the root cause of the problem. This cluster includes one male and one female, one individual identifies as being part of the public sphere while the other identifies as being part of the private sphere.

The Corporate Problem cluster does not believe that cyberattacks increase as a result of technological expansion [5]. They believe strongly that companies are falling victim to cyber-attacks and do not know how to protect themselves [6]. They believe that the general population understands best practices to protect their technology [14] and that a cause of the cybersecurity problem has to do with an unclean cyber ecosystem [12]. However, they do not believe that a cause of the cybersecurity problem is because valuable assets reside on the Internet, motivating cyber criminals [19]. The Corporate Problem cluster believes that Congress and the President are willing to deal with the issues of cybersecurity [20], and that patch management is not a solution to fix the cybersecurity problem. This cluster believes that the U.S. government is not flexible enough to effectively regulate the cyber realm [35] and that monitoring the Internet increases the likelihood that an individual's privacy will be violated [36].

DISCUSSION

Considering the current cybersecurity discourse, I expected belief patterns to distinctly align with the three-problem definitions: knowledge gap, regulation requirement, and purpose of the Internet. This was not the case as each cluster's belief patterns included a combination of opinions from the three problem definition areas. Further, I expected people from the same industry or sector to hold similar beliefs. This was also not the case as membership in each cluster crossed industry and sector lines. This could, perhaps, represent significant cross-fertilization between public and private sectors in the field and practice of cybersecurity as individuals move between employment opportunities. However, I might expect that significant

cross-fertilization would result in some sort of regression to similar problem definitions. This was also not the case. Further, this may suggest that while private industry and the public sector seem separated on beliefs about how cybersecurity should be addressed, their opinions about how the problem should be handled are much more similar than they initially appear. In the next paragraphs, I will discuss broad similarities between each of the groups as well as some interesting and poignant differences.

[Insert Table 4]

SIMILARITIES

Some clusters share similarly strong viewpoints on a small number of statements. Four of the six clusters agreed that the U.S. government does not have the infrastructure and skillset to handle the problem of cybersecurity [21]. This broadly suggests that no matter what cluster a participant resides in, they do not believe the U.S. government has the tools necessary to solve the cybersecurity problem. This statement is particularly interesting because its structure suggests that the government has both the people and the technology/organization that make it capable of regulating the cybersecurity realm. The groups that responded strongly and negatively to this statement indicate a critique of the government's capacity–either in infrastructure and/or skillset. No group believes that the government has the means of regulating the cyber realm.

There were six statements that elicited strong opinions, both positively and negatively, from more than one cluster. Perhaps the most interesting response from the perspective of this study deals with the public's knowledge of best practices. There is a general belief that the public does not understand best practices in four of the six groups [14]. This suggests that despite varying viewpoints as to how cybersecurity should be addressed, there is agreement that the lack of understanding in the general population may be a primary cause of the problem. However,

participants in the Corporate Problem cluster do not believe that the source of the problem is the public's lack of understanding [14]. This dissonance between a majority of participants and a small but passionate minority indicates the causes of cybersecurity problems are multifaceted and more complex than they initially appear. And importantly, it reflects that participants' understandings of the problem are more complex than the discourse presents and may complicate attempts to design and implement solutions.

DIFFERENCES

Despite nearly 42% of statements having an overall range of 9 or greater, indicating potential differences in beliefs, there are only a few statements that provoked strong differences between clusters. The statement that led to the most polarizing responses had to do with monitoring the Internet and the likelihood that an individual's privacy will be violated [36]. Those within the Free Market and Corporate Problem clusters see monitoring of the Internet as increasingly violating privacy. However, the two groups who were solution-focused, Collaborative and Government, disagree; they believe that monitoring the Internet does not increase privacy violations. Interestingly, the demographics of these clusters do not align perfectly with the expectations in the discourse. Clusters with higher concentrations of private sector individuals believe that monitoring will not violate privacy. This disagreement regarding privacy is crucial for two reasons. First, the discourse leads me to anticipate a belief pattern that did not hold. The discourse indicates that public sector individuals believe that monitoring is a violation of privacy whereas private sector individuals do not. While the pattern in the Q data was not a perfect inversion, there was enough evidence to indicate that the discourse was incorrect in its assumptions. Second, and more importantly from a policy perspective, privacy is perhaps one of the bigger conversations in the public side of the policy discourse. For the general

public, and for practicing cybersecurity professionals, privacy becomes a major policy sticking point.

Further, there are major disagreements about core beliefs across two or more groups. Shockingly, there was disagreement between the Public Education cluster and the Corporate Problem cluster on the general trend that as technology usage expands, the number of cyber-attacks increases [5]. This statement is distinctly related to the problem definition focusing on the purpose of the Internet and how technology is not set up to be inherently safe. The Public Education cluster believes that, in fact, as technology expands, the number of cyberattacks increases. Disagreement with this statement could suggest that the Corporate Problem cluster believes that the Internet's structure is safe, or that on whole cyber-attacks are not increasing because of increased usage.

Another interesting difference between the groups is the stark contrast regarding the implication of a Cybersecurity Defensive Triad. Despite all three groups being strongly solution-focused, participants in the Collaborative Solution, Government Solution, and Free Market Solution clusters feel very different about how a solution can be reached. Specifically, the Government Solution group believes that the government ought to implement the Triad, whereas the Free Market Cluster does not. As the three parts of the Cybersecurity Triad include protecting the backbone of the Internet, securing the power grid, and securing the supply chain of both hardware and software, this disagreement makes sense. A key element of the triad, the government’s current use of and future implementation of the Triad, could each be an underlying cause why these groups cannot agree.

Overall, this project reveals that the cybersecurity field is disjointed, but in unexpected ways. Some of these ways include how groups perceive the problem, whether it is a core issue

with the cause, or how they believe the issue should be addressed with preferred solutions. It could be that groups have differing fundamental beliefs about privacy and individual security. As discussed in the review of the discourse, knowing these unexpected similarities and differences is the key to being able to understand how to improve the current cybersecurity conversation to mitigate cyberattacks. With these results, it became clear how unrepresentative the discourse is of the current state of cybersecurity, and demonstrates the real need for more research to better understand specific differences in beliefs. Such research is crucial to effectively navigate potential roadblocks to collaboration between groups to help solve the cybersecurity problem.

CONCLUSION

After analyzing and understanding the current state of the field of cybersecurity, it is apparent that cybersecurity stakeholders do indeed have beliefs that are different from each other in important ways. While this was apparent in several ways as presented above, the best example of these distinct differences is how each group perceived the general population's understanding of ways to protect their technology. Recall that many participants believe that individuals in the general population do not know cybersecurity best practices to protect their technology, while a dissenting minority believes the opposite. It is important to realize that while a minority might have strong dissenting opinions from the majority, this does not mean that there is not room for the two groups to come together and have agreement. Recall Q sort allows for individuals to answer statements based off their subjective opinions. This means that these results are more complex then they might appear. The majority might not actually disagree with the minority and vis-a-vis.

Surprisingly, the discourse suggests that individuals from similar industries/sectors would maintain similar opinions, while this is not what occurred. Rather, cross-fertilization between the

fields suggests that individuals in private industry and individuals in the public sector do not necessarily maintain beliefs consistent with what the discourse anticipates in their field. Additionally, it is important to note that individuals may not actually be speaking past one another; rather, they may simply disagree on some important areas. Despite lack of agreement between clusters, there may be room to develop a problem definition based on some of the statements that had much support (i.e., the U.S. government does not have the tools necessary to solve the cybersecurity problem and the general population does not understand best practices to protect themselves). Based on this data, it appears there are some potential areas where the problem definitions of the six clusters overlap, creating a possibility of collaborative policy making. Despite this, there are a few core areas in which the groups do not agree that could make it impossible to address this problem holistically.

More research is needed to better understand the implications of this research and to determine whether they can be used to help understand the field of cybersecurity and develop appropriate dialogue to address this issue. Further research should first aim to verify that these six clusters are the only clusters that exist and that each of the clusters is representative of a belief pattern amongst cybersecurity stakeholders. Additionally, more research is needed to understand which of these areas has the most potential to develop a shared problem definition amongst stakeholders. This is necessary if cybersecurity stakeholder groups will ever agree on how to address the issue of cyber-attacks. Overall, this research is a great first step in understanding cybersecurity stakeholder opinions; however, more research is needed to truly combat this growing issue.

Works Cited

Brown, S. (1991). A q methodological tutorial.

Chan, J. (2004). Essentials of patch management policy and practice. *PatchManagement.org*.

CIA Triad and Perkerian Hexad. (2013). *Infinite Secure*.

Clarke, R., & Knake, R. (2012). *Cyber war: The next threat to national security and what to do about it* (2nd ed.). Ecco Press.

Clarke, S. (2006). Context-sensitive policy methods. In *Handbook of Public Policy Analysis*. CRC Press.

Clark, S. (2011). *The policy process: A practical guide for natural resource professionals*. New Haven, CT: Yale University Press.

Cobb, R., & Elder, C. (1983). *Participation in American politics: The dynamics of agenda-building*. Baltimore, MD: John Hopkins University.

Dery, D. (1984). *Problem definition in policy analysis*. University of Kansas Press.

Dillow, C. (2014). Cybersecurity is for the C-suite, "not just the IT crowd." *Fortune Magazine*.

Etzioni, A. (2014). A private sector: A reluctant partner in cybersecurity. *Georgetown Journal*.

Goldsmith, J. (2011). Cybersecurity treaties: A skeptical view. *Hoover Institution- Stanford University*.

Guess, G., & Farnham, P. (2000). *Cases in public policy analysis* (2nd ed.). Georgetown University Press.

Lanstein, A. (2009). Exposing bad actor sites that support cybercrime. *CIO from IDG*.

Lasswell, H. D. (1951). The policy orientation. In *The policy sciences: Recent developments in scope and method* (pp. 3–15). Stanford: Stanford University Press.

Lasswell, H. D. (1971). *Preview of policy sciences*. New York, NY: Elsevier.

Lasswell, H. D. (1999). *The science of public policy: Evolution of policy sciences* (Vol. 1). London and New York: Routledge.

Lord, N. (2016). Supply chain cybersecurity: Experts on how to mitigate third party risk. *Digital Guardian*.

Lowham, E., & Lowham, J. (2015). Understanding the constellations of democratic and civic beliefs of educators. *Democracy & Education*, *23*(1), 1–13.

McKeown, B., & Thomas, D. (2013). *Q Methodology* (2nd ed., Vol. 66). Sage Publications.

Moar, J. (2015). *Cybercrime will cost businesses over $2 trillion by 2019* (Financial & Corporate Threats & Mitigation 2015-2020). Hampshire, UK: Juniper Research Ltd.

Ngo, D. (2010). Survey: 63% don't change passwords very often. *CNet*.

Noyes, K. (2010). 10 reasons open source is good for business. *PCWorld*.

Otto, G. (2016). U.S. power grid cyberattack: When, not if, says NSA chief. *FedScoop*.

Pagliery, J. (2014). Half of American adults hacked this year. *CNN Money*.

Rochefort, D., & Cobb, R. (1994). *The politics of problem definition: Shaping the policy agenda*. University of Kansas Press.

Rowe, B., Wood, D., Reeves, D., & Braun, F. (2011). The role of Internet Service Providers in cyber security. *Institute for Homeland Security Solutions*.

Shinder, D. (2007). 10 physical security measures every organization should take. *Tech Republic*.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. New York, NY: Oxford University Press, Inc.

Takala, R. (2016). Lawmaker: Congress is in the "dark ages" on cybersecurity. *Washington Examiner*.

Timberg, C. (2015). A flaw in the design: The internet's founders saw its promise but didn't foresee users attacking one another. *The Washington Post*.

Vanca, D. (2010). Richard A. Clarke and Robert K. Knake's "Cyber War: The Next Threat to National Security and What to Do About It." *Georgetown Security Studies Review*, *1*(1).

Verizon Wireless. (2016). *2016 Data Breach Investigations Report*.

Vogel, J., Cherney, D., & Lowham, E. (2017). The policy sciences as a transdisciplinary approach for policy. In *The Oxford Handbook of Interdisciplinary* (Second). Oxford, UK: Oxford University Press, Inc.

Vogel, J., & Lowham, E. (2007). Building consensus for constructive action: A study of perspectives on natural resource management. *Journal of Forestry*, *105*(1), 20–27.

Weiss, J. (1989). The powers of problem definition: The case of government paperwork. *Policy Sciences*, *22*(2), 97–121.

Wolf, U. (2009). Cyber-crime: Law enforcement must keep pace with tech-savvy criminals. *Digital Communities*

Table 1: Q Sample

	Knowledge Gap	Regulation Requirements	Purpose of the Internet
Generalized Trends		1. The number of cyber-attacks is increasing uncontrollably	
		2. Costs related to cyber-attacks are becoming unbearable	
Specialized Trends	3. As the pace of technology development increases, knowledge about technology decreases	4. Internet service providers should continue to allow customers to use their networks even when the customer is under cyber attack	5. As technology usage expands, the number of cyber-attacks increases
		6. Companies are falling victim to cyber-attacks and don't know how to protect themselves	7. Increasing access to the Internet is a good thing
Conditions	8. Lawmakers are not technologically savvy	9. Internet service providers should be required to regulate the backbone of the Internet	10. Cybersecurity problems are due to the bad behavior of individuals
	11. Executives and Information Technology employees do not have the same concerns regarding cybersecurity	12. We need to develop a heathier ecosystem through automation, interoperability and authentication	13. The Internet's core structure enables cybersecurity issues
	14. The general population does not understand best practices to protect their technology	15. Corporations are providing sufficient security when customers access their servers	16. Humans are inherently trusting and as such, increasingly fall victim to cyber-attacks
	17. Employees do know how to protect their organizations' proprietary information on the Internet	18. Internet service providers are not doing enough to ensure the safety of their customers on the Internet	19. Valuable assets reside on the Internet, providing motivation for cyber-attacks
		20. Regardless of party control, both Congress and the President are unwilling to regulate standards for network security	

		21. The U.S. government has the infrastructure and skillset to handle the problem of cybersecurity	
Preferred Solutions	22. All U.S. government cybersecurity leaders must be technologically proficient	23. The U.S. government should require organizations to adopt cybersecurity best practices	24. The way to fix the cybersecurity problem is to use Open Source Software
	25. The U.S. needs to develop more public-private partnerships to solve cybersecurity issues	26. The U.S. should focus on implementing a Cybersecurity Defensive Triad by protecting the backbone of the Internet, securing the power grid, and securing the supply chain of both hardware and software.	27. Patch management cannot fix cybersecurity problems
	28. We need to rethink the role of the U.S. Government in cybersecurity	29. Private corporations should provide security solutions independent of government regulation	30. Increasing the number of independent individuals monitoring the Internet would decrease cybersecurity issues
	31. We should think of cybersecurity policy like public health policy, focusing on teaching people how to best protect themselves	32. Resources to provide cybersecurity solutions are being misallocated	
	33. The U.S. government should seek a cybersecurity treaty with foreign governments		
Critique	34. Technology education cannot keep up with the pace of technology innovation	35. The U.S. government is not flexible enough to effectively regulate the cyber realm.	36. Monitoring of the internet increases the likelihood that an individual's privacy will be violated

Table 1 provides the statements that were given to participants in the Q Sort. These statements were developed from the cybersecurity discourse and are broken down into general trends, specialized trends, conditions, preferred solutions, and critique (see Laswell, 1951).

Table 2: Means & Ranges Comparison

Policy Orientation	Questions	Statistics for Overall Sample		Means for Each Cluster					
		Range is 9 or more		Mean (-2.5 or Less, 2.5 or Greater)					
		Mean	Range	Public Education	Collaborative Solution	Government Solution	Public Private Partnership	Free Market Cybersecurity	Corporate Problem
Generalized Trends	1. The number of cyber-attacks is increasing uncontrollably.	0.37	7	2.20	-0.33	2.33	-1.33	-1.50	-2
	2. Costs related to cyber-attacks are becoming unbearable.	-0.56	8	-1.20	-1.17	0.00	-0.33	1.50	0
Specialized Trends	3. As pace of technology increases, knowledge about technology decreases.	-1	8	-1.80	-1.67	1.00	-1.33	1.50	-1
	4. Internet Service Providers should continue to allow customers to use their networks even when the customer is under cyber-attack.	-1.07	7	0.00	-1.50	-3.33	0.67	1.5	-3.5
	5. As technology usage expands, the number of cyber-attacks increases.	1.89	9	3.4	1.00	0.67	1.33	0.5	-2.5
	6. Companies are falling victim to cyber-attacks and don't know how to protect themselves.	1.22	8	2.6	2.00	-0.67	-0.67	0.00	3.5
	7. Increasing access to the Internet is a good thing.	1.59	11	1.60	1.00	-0.67	4.33	2.50	1.5
Conditions	8. Lawmakers are not technologically savvy.	1.74	9	2.20	1.5	1.67	1.67	2.50	-1
	9. Internet Service Providers should be required to regulate the backbone of the Internet.	-1.37	6	-2.20	-0.33	0.67	-2	-5.00	0.5

	10. Cybersecurity problems are due to the bad behavior of individuals.	-0.33	7	-0.20	-0.17	-0.67	-1.33	-0.50	-0.5
	11. Executives and Information Technology employees do not have the same concerns regarding cybersecurity.	0.3	6	-1.80	1.67	1.00	0.33	0.5	1
	12. We need to develop a healthier ecosystem through automation, interoperability, and authentication.	1.93	9	2.40	3.5	-2.33	3.00	1.50	2.5
	13. The Internet's core structure enables cybersecurity issues.	1.3	6	1.20	0.67	2.33	1.00	0.5	1
	14. The general population does not understand best practices to protect their technology.	2.41	8	3.2	4.17	2.67	0.33	2.50	-2.5
	15. Corporations are providing sufficient security when customers access their servers.	-1.52	9	-3.2	-3.33	-1	-0.33	0.00	-1.5
	16. Humans are inherently trusting and as such, increasingly fall victim to cyber-attacks.	1.3	7	3	2.5	0.00	0.67	1.00	-0.5
	17. Employees do know how to protect their organizations' proprietary information on the Internet.	-2.11	8	-4	-3.67	-2	0.00	-0.50	-2
	18. Internet Service Providers are not doing enough to ensure the safety of their customers on the Internet.	0.33	8	-0.60	0.83	2.00	1.33	-2	1.5
	19. Valuable assets reside on the Internet, providing motivation for cyber-attacks.	2.56	10	3	3	2.33	2.33	3	-3
	20. Regardless of party control, both Congress and the President are unwilling to regulate standards for network security.	-1.22	8	-2.20	-0.83	0.00	-0.33	-3.00	-3

	21. The U.S. government has the infrastructure and skillset to handle the problem of cybersecurity.	-2.22	9	-3.6	-2.83	-2.00	-4.33	-3.00	-1
Preferred Solutions	22. All U.S. government cybersecurity leaders must be technologically proficient.	0.59	8	1.80	0.67	-0.33	-2.67	2.50	-0.5
	23. The U.S. government should require organizations to adopt cybersecurity best practices.	0.96	10	1.40	2.33	0.67	-0.33	-4.50	-2
	24. The way to fix the cybersecurity problem is to use Open Source Software.	-1.78	8	-2.20	-0.50	-3.67	-4.00	0.50	1.5
	25. The U.S. needs to develop more public-private partnerships to solve cybersecurity issues.	2.22	9	1.20	2.50	3	3.67	0.00	2
	26. The U.S. should focus on implementing a Cybersecurity Defensive Triad by protecting the backbone of the Internet, securing the power grid, and securing the supply chain of both hardware and software.	1.44	10	0.80	2.50	4.67	2.00	-3.5	2
	27. Patch management cannot fix cybersecurity problems.	0.33	9	-2.40	1.83	-1	1.33	1.00	3
	28. We need to rethink the role of the U.S. government in cybersecurity.	1.81	8	1.20	2.67	3.00	2.33	-2.00	1.5
	29. Private corporations should provide security solutions independent of government regulation.	2.67	6	2.8	3.33	2.00	2.33	3.50	1
	30. Increasing the number of independent individuals monitoring the Internet would decrease cybersecurity issues.	-1.52	8	-2.20	-1.83	-2.00	-0.33	1.00	0
	31. We should think of cybersecurity policy like public health policy, focusing	1.67	9	3.2	1.17	0.67	2.33	1.00	1

	on teaching people how to best protect themselves.								
	32. Resources to provide cybersecurity solutions are being misallocated.	0.07	7	-1.00	1.17	-1.00	-0.67	1.00	0
	33. The U.S. government should seek a cybersecurity treaty with foreign governments.	0.67	8	1.40	1.83	-2.00	-0.33	-1.50	1.5
Critique	34. Technology education cannot keep up with the pace of technology innovation.	-0.3	10	0.60	-1.50	2.33	-1.67	-2.5	1.5
	35. The U.S. government is not flexible enough to effectively regulate the cyber realm.	1.19	9	2.00	0.17	1.00	3.67	4.5	2.5
	36. Monitoring of the Internet increases the likelihood that an individual's privacy will be violated.	-0.44	10	1.40	-3.83	-4.00	-2.00	4.5	3

Table 2 provides the mean of each cluster's opinion of each of the statements provided to them. The green identifies the statements that they most agree with (+2.5), while the red represents statements they least agree with (-2.5). The ranges for each of the questions shows just how varied the participants were to each of the questions.

Table 3: Cluster Demographics

	Total Sample	All Clusters	Public Education	Collaborative Solution	Government Solution	Corporate Solution	Free Market	Corporate Problem
Participants	28	21	5	6	3	3	2	2
Sector								
Public	29.6%	28.6%	0%	50%	33%	0%	50%	50%
Private	40.7%	42.9%	60%	17%	33%	67%	50%	50%
Consultant	11.1%	14.3%	40%	0%	0%	33%	0%	0%
2+	14.8%	14.3%	0%	33%	33%	0%	0%	0%
Degree								
Associates	3.7%	4.8%	20%	0%	0%	0%	0%	0%
Bachelors	11.1%	9.5%	20%	0%	33%	0%	0%	0%
Masters	74.0%	76.2%	40%	83%	67%	100%	100%	100%
Doctorate	11.1%	9.5%	20%	17%	0%	0%	0%	0%
Gender								
Male	66.7%	66.7%	60%	33%	100%	100%	100%	50%
Female	33.3%	33.3%	40%	67%	0%	0%	0%	50%
Race								
White	92.6%	95.2%	100%	100%	67%	100%	100%	100%
Other	7.4%	4.8%	0%	0%	33%	0%	0%	0%

This table provides demographics for the total sample, each intendent cluster, and all clusters totaled together.

Table 4: Similarities and Differences Between Clusters

	Public Education	Collaborative Solution	Government Solution	Public Private Partnership	Free Market Cybersecurity	Corporate Problem
Specialized Trends	*1.As usage expands, cyber-attacks increase* 2. Companies falling victim to attacks		ISPs should NOT continue use when under attack	Increasing access to internet=good	Increasing access to internet=good	1. ISPs should NOT continue use networks under attack 2. *As usage expands, cyber-attacks to NOT increase* 3. Companies are falling victim to attacks
Conditions	1. ***The general pop does not understand best practices*** 2. Corps are not providing sufficient security 3. Humans are inherently trusting and fall victim to attacks 4. Employees do not know how to protect orgs info 5. *Valuable assets reside on Internet, providing motivation* 6. **The U.S. gov does not have infrastructure and skillset to handle problem**	1. We need to develop a healthier ecosystem 2. ***The general pop does not understand best practices*** 3. Corps are not providing sufficient security 4. Humans are inherently trusting and fall victim to attacks 5. Employees do not know how to protect orgs info 6.*Valuable assets reside on Internet, providing motivation* 7. **The U.S. gov does not have infrastructure and skillset to handle problem**	*1.* ***The general pop does not understand best practices***	1. We need to develop a healthier ecosystem 2. **The U.S. gov does not have infrastructure and skillset to handle problem**	1. Lawmakers are no technologically savvy 2. ISPs should NOT be required to regulate the backbone of the Internet 3. ***The general pop does not understand best practices*** 4. *valuable assets reside on Internet, providing motivation* 5. Regardless of party control, congress & POTUS are willing to regulate standards 6**. The U.S. gov does not have infrastructure and skillset to handle problem**	1. We need to develop a healthier ecosystem 1. *The general pop DOES understand best practices* 2. *A cause is NOT that valuable assets reside on the internet providing motivation for attacks* 3.Regardless of party control, congress & POTUS are willing to regulate standards

Preferred Solutions	1. Private Corporations should provide security independent of government regulation 2. Public Health Policy	1. PPP 2. *Cybersecurity Defensive Triad* 3. Rethink U.S. government role 4. Private Corporations should provide security independent of government regulation	1. NOT Open Source Software 2. PPP 3. *Cybersecurity Defensive Triad* 4. Rethink role of U.S. government	1. *U.S. government leaders do NOT have to be cyber proficient* 2.NOT Open Source 3. PPP	*1. All U.S. government leaders do have to be cyber proficient* 2. U.S. government should NOT require orgs to adopt cyber best practices 3. *NO Cyber Triad* 4. Private corporations should provide cyber independent of government regulation	1. Patch management cannot fix cyber problems
Critique		*1. Monitoring the Internet does not increase likelihood that an individual's privacy will be violated*	*1. Monitoring the Internet does not increase likelihood that an individual's privacy will be violated*	1. The U.S. gov is not flexible enough to effectively regulate cyber realm	1. Technology education CAN keep up with the pace of technology education 2. The U.S. gov is not flexible enough to effectively regulate cyber realm *3. Monitoring increases the likelihood an individual privacy WILL be violated*	1. The U.S. gov is not flexible enough to effectively regulate cyber realm *2. Monitoring increases the likelihood an individual privacy WILL be violated*

This table represents the strongest opinions of each of the clusters. The italicized represents different or independent viewpoints while the bold is 4 or more groups agreeing on something.