Communicating Cyber-risk:

How exposure to cyber-attacks impacts support for cyber-protection policies

DRAFT: PLEASE DO NOT CIRCULATE

Nadiya Kostyuk[*]& Carly Wayne[†‡]

October 21, 2017

Abstract

Cyber safety and security presents a unique challenge for societies because hackers need not defeat powerful armies to have an impact; they can gain access to sensitive systems by exploiting any weakness in the system. Often, this weakness begins with an average civilian ill-prepared to defend themselves against a cyber-attack. In order to address this new challenge, it is thus critical to understand more about how individuals assess cyber-risk and how this risk perception impacts their personal cyber-protective behaviors and support for new cybersecurity policies. Despite a growing number of cyber-attacks on individuals over the last few years, the literature that assesses these questions is scarce. To address this gap, we use a novel experimental study in the United States to examine the impact of exposure to different types of cyber-threats on personal online behavior and individuals' support for various cyber-security policies. We find that baseline concerns about cyber-attacks and knowledge about safe online practices are low. However, exposure to cyber-attacks personally relevant to the individual heightens risk perception and their willingness to engage in safer online practices in the future. This study has important implications for how governments should communicate cyber-risk to their citizenry and educate them in the steps necessary to protect themselves – and their country – from cyber-attacks.

[*] Department of Political Science, University of Michigan, Ann Arbor; Predoctoral fellow, Belfer Center, Harvard University (2017-2018); nadiya@umich.edu

[†] Department of Political Science, University of Michigan, Ann Arbor; carwayne@umich.edu

[‡] Authors' names are listed alphabetically; this study is pre-registered with EGAP (ID#: 20170131AA)

The 2016 US Presidential Election and its myriad reports of purposeful cyber-attacks by the Russian government have spurred a renewed public interested in the importance of cyber-security and the potential vulnerability of the United States government to cyber-threats. Governments are not alone in this vulnerability. The 2017 ransomware attacks WannaCry and NotPetya, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency, demonstrated that average citizens and private companies all over the world are also incredibly vulnerable to cyber-attacks. However, despite these and other high-profile cyber-attacks in recent years – on both government and civilian targets – many computer users still fail to engage in even the most basic cyber hygiene practices. Indeed, many cybersecurity experts report that, "while we depend more and more on technology, technology is becoming more and more insecure" Cerrudo (2017). What causes this disconnect between the objective and perceived threat from cyber-attacks and how does this disconnect impact citizens' online behavior and states' cybersecurity policies? This research explores this question, investigating how individuals assess cyber-risk and how this risk perception impacts support for various cybersecurity policies and personal cybersecurity behavior.

We hypothesize that citizens perceive a low personal risk from cyber-attacks, despite growing evidence that cyber-threats may present objectively more risk than other concerns frequently mentioned by citizens (such as terrorism or violent crime), because cyber-attacks do not engage key appraisals central to heightening perceptions of risk. In other words, cyber-threats are less dreaded because they are perceived as less catastrophic and more controllable than physical attacks. However, exposure to a cyber-attack that personally affects an individual is likely to heighten perceptions of future risk from cyber threats, leading citizens to support costlier cybersecurity policies and engage in safer cyber-security practices themselves. We test these hypotheses using the novel survey experiment in the United States. Our findings demonstrate that indeed, cyber-attacks with a personal dimension are most likely to increase levels of perceived threat and lead to changes in online behavior. However, these threat perceptions - surprisingly - do not lead to significant changes in policy preferences.

This article makes three contributions to our understanding of cybersecurity today.

First, this study provides important information about baseline levels of knowledge about cybersecurity and safe online practices among average citizens, not just government officials. Because cyber-attacks are designed to exploit the weakest link in an online system, understanding the preparedness of individual citizens to defend their computers from cyber-threats is thus crucial to appreciating the potential vulnerability of the state to this type of attack. Second, this research demonstrates how these perceptions and behaviors can potentially be changed. Namely, we show how exposure to new cybersecurity threats can impact citizens' support for government cybersecurity policies and personal online behavior. Third, we present a unified framework for understanding how citizens perceive the relative risk from a variety of potential security threats to the state, providing important implications for policymakers seeking to inform and/or mobilize their publics to address new national security challenges.

The article proceeds as follows. Before introducing out theory (Section 3), we briefly provide an overview of the existing literature on cybersecurity and public opinion (Section 1) and clarify existing definition of cyber-attacks and hacking (Section 2). Then, we introduce our research design, laying out our hypotheses, participants, procedure, and measures (Section 4). We conclude with the discussion of our results (Section 5) and their implications (Section 6).

1 What We Know about Cybersecurity & Public Opinion

Currently, there is a dearth of academic work that systematically addresses cybersecurity from a bottom-up perspective (e.g., the attitudes of individual citizens). We know surprisingly little about how individuals assess cyber-risk, their level of support for various cybersecurity policies and their own personal online behavior. Indeed, most academic research on cybersecurity tends towards the technical aspect of this issue, focusing on vulnerabilities of the supervisory control and data acquisition (SCADA), distributed control systems (DCSs) networks protection (Ralston, Graham and Hieb, 2007; Nicholson et al., 2012; Igure, Laughter and Williams, 2006), risk assessments of the unmanned aerial vehicles (UAVs) to cyber-attacks (Hartmann and Steup, 2013; Kim et al., 2012; Javaid et al., 2012) or on cyber-physical security of systems operated by robots (Denning et al., 2009; McClean et al., 2013; Bonaci et al., 2015). Other research on cybersecurity emphasizes the macro-security dynamics surrounding issues like cyber-deterrence during conflict (Libicki, 2009; Sharma, 2010; Andres, 2012), cyber-crime, cyber-espionage, and theft of intellectual property (Richards, 1998; Andrijcic and Horowitz, 2006; Kshetri, 2010; Taylor, Fritsch and Liederbach, 2014).

Likewise, work on public opinion has yet to turn their attention to the cybersecurity realm or explore the antecedents and consequences of public opinion surrounding cyber-threats.[1] Rather, public opinion scholars interested in the role of digital and online technology in politics have largely focused on how the internet has changed political behavior. Existing scholarship mostly focuses either on the effects the World Wide Web on civic communication and their participation in politics (Coleman, Taylor and van de Donk, 1999; Bimber, 2001; Weber, Loumakis and Bergman, 2003; Kluver, 2004; Polat, 2005; Haynes and Pitts, 2009), or on their social activity (Brants et al., 1996; Franzen, 2000; Robinson et al., 2000; Howard, Rainie and Jones, 2001). Other academics study how citizens' online engagement changes their patterns of collective actions (Lupia and Sin, 2003) and how it transforms the relationship between citizens and bureaucrats (Scavo and Shi, 2000; Bovens and Zouridis, 2002; Welch and Fulla, 2005; Mossberger, Tolbert and Stansbury, 2003).

A growing literature that focuses on how people value their privacy has, however, begun to touch on these themes. This work focus on how individuals attempt to maximize their gains as a customer when they are uncertain about the nature of privacy trade-offs and their own preferences over them. For instance, Norberg, Horne and Horne 2007 demonstrates that even though people complain about the ability to control their personal information, they often freely disclose it. This paradox mirrors our central research question - why individuals might perceive cyber-threat as less risky than it actually is. Other research in this area investigates the relative malleability of this personal privacy tradeoff, examining the role of context in affecting such considerations (Acquisti, Brandimarte and Loewenstein, 2015). The context-dependency of such concerns may explain

[1] Two notable exceptions are recent articles by Cheung-Blunden and Ju (2015) and by Canetti, Gross and Waismel-Manor (2016) that explore the impact of exposure to cyber-attack on citizens' ability to process information, their anxiety, and overall psychological well-being. This work does not, however, explore how this exposure impacts either political attitudes or personal online behavior

why certain types of cyber-threats are more likely than others to mobilized changes in behavior and policy preferences.

Despite this nascent research on privacy concerns, however, researchers have yet to explore how public perception of cybersecurity risks impacts state cybersecurity policies or affects citizens' own personal online practices. This is because work in this field has largely been divided into three camps: those who study the technical aspects of cybersecurity, researchers who look at the macro-strategic dynamics of cyber-technology; and scholars who explore the implications of new technology on political participation and behavior. Thus, this study fills a large gap in the literature by examining how individuals assess cyber-risk and how this risk perception impacts support for government cybersecurity policies and changes personal online behaviors.

2 Classification of Cyber Activities

The world of cyber-attacks is incredibily broad and varied. Thus, before proceeding to our theory, we provide an overview of existing definitions of cyber-attacks and explain which attacks are the primary focus of the present study.

Depending on their purpose, the cybersecurity literature distinguishes between three primary types of attacks – propaganda, disruption, and crime. Cyber activities in the propaganda category seek to influence public opinion by "trolling" online comments pages and establishing forums and websites to promote certain messages. During the last few years, scholars have been intensively studying these efforts and demonstrated that China (King, Pan and Roberts, 2013, 2017) and Russia (Sanovich et al., 2015) are two leading governments in this regard. For instance, the Russian government has been quite successful in using virtual images of crucified babies and raped women that presumably took place in eastern Ukraine to influence public opinion, both in Ukraine and Russia, during the Ukrainian conflict (Kostyuk and Zhukov, 2017). The main focus of propaganda campaigns is a long-term goal of influencing public opinion, rather than infiltrating a system and directly harming national security. As such, this type of attack is beyond the scope of the current research.

The second category of cyber-attacks – disruption – includes efforts to inundate communications systems with floods of text messages and phone calls, to use firewalls and proxies to block access to websites, or to use malicious code to inflict physical damage or otherwise compromise infrastructure and military objects. These attacks have also become a popular tool of censorship (Deibert and Rohozinski, 2010; Villeneuve and Crete-Nishihata, 2011; King, Pan and Roberts, 2013; MacKinnon, 2013) and contention (Asal et al., 2016). With the increased reliance on the internet, activists have been using social platforms to self-organize and to promote their views of discontent with existing governments. Governments, in turn, used cyber attacks, such as DDoS attacks, to flood the activists' websites with requests that would eventually lead these websites to stop functioning (Deibert et al., 2010). Cyber attacks are also a popular tool among activists who block state's websites as a way of protesting against the government (Coleman, 2014). The international network of activists and hacktivists *Anonymous*, for instance, became known for executing a series of well-publicized DDoS attacks on government, religious, and corporate websites to protest their practices and decisions. Though disruption attacks are not the primary focus of this study, they are affected by the security practices of average citizens. For example, a careless government employee who accidentally connects a secure computer to the web to check a personal email or inserts an external USB drive to upload a document may allow hackers a backdoor to enter and disrupt vulnerable systems. Thus, our study, which focuses mainly on individual level cyber-attacks (see below) does have implications for the disruption-type of cyber attacks.

The third category of cyber-attacks, crime, is the primary focus of this paper, because it is the most widespread cyber-threat and is also most likely to impact individual citizens on a daily basis. In this particular study, we use reports of online identity theft to attempt to change citizens' perceptions and behavior regarding cyber-security. Indeed, identity theft is the fastest-growing crime in the United States, costing Americans over $50 billion in fraudulent charges and affecting about eight million people annually. It is a huge - and often unappreciated - threat to the well-being of individuals around the world. Moreover, these individual cases of identity threat aggregate to create a threat to the state - harming national economies, undermining confidence in markets, and leading to other security breaches if hacked identities are used to access sensitive government systems.

3 The Cyber-risk Theory

This project argues that perceptions of personal risk from cyber-attacks are relatively low in the population, despite growing evidence that cyber-threats may present objectively more risk to the average citizen than a host of other concerns citizens frequently reference, such as terrorism and violent crime. We present a theory to explain this paradox based on findings in the field of psychology regarding the particular cognitive biases individuals possess when they attempt to calculate probabilities and risk. Specifically, scholars of risk such as Slovic (2016) have identified two key dimensions that impact risk perceptions – the relative "dread" the unwanted outcome triggers and the extent to which the risk is "known" or "unknown." Figure 1 charts these dimensions and lists the variables affecting each dimension.

While things like terror attacks, mass shootings, and other violent crimes possess many of these components that maximize risk perception on both dimensions, cyber-threats

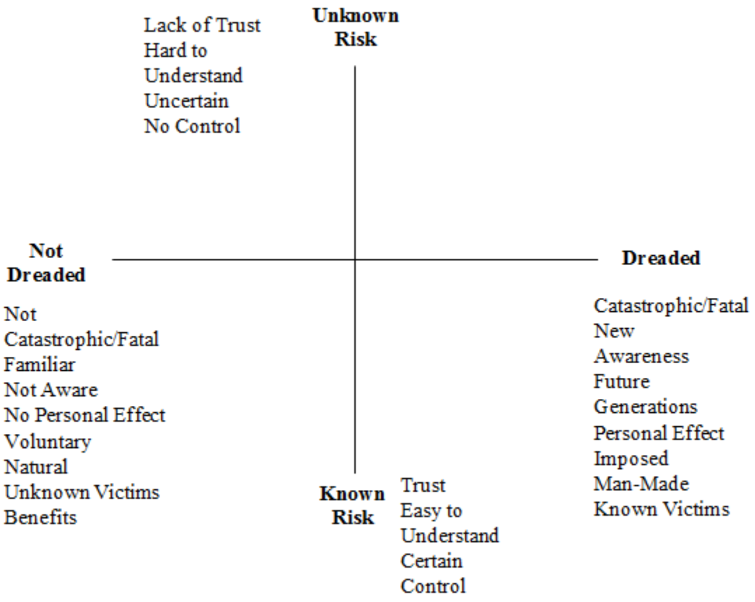

Figure 1: Slovic's dimensions of risk perceptions

do not. For example, terrorist attacks are often catastrophic and fatal; whereas cyber-attacks, at least to date, have not caused significant physical harm (they are more likely to cause monetary harm). Much of the suffering that cyber-attacks seem to bring lacks the pain and persistence of many physical injuries (Canetti, Gross and Waismel-Manor, 2016). As a result, the damage that cyber-attacks might cause does not trigger "light bulb memory" where the "emotionally potent events are better remembered than low emotional ones" (Siddiqui and Unsworth, 2011). Essentially, the "dread" factor of cyber-attacks is lower than those for physical violence. Even though cyber-attacks can indeed be catastrophic for the individuals involved – destroying their socio-economic well-being or exposing sensitive private information to the world – they are simply not *perceived* as such.

Moreover, terrorist attacks and violent crime are often highly uncertain and uncontrollable, whereas cyber-threats appear less so. This in many ways has to do with the type of events most widely covered in the news media. The terror attacks or shootings that are most widely covered in the news are random attacks on civilians, whereas the cyber-attacks most widely covered are systematic attacks against governments or corporations (individual cases of identity theft do not receive as broad of coverage). Thus, citizens tend to believe that they are not personally the target of hackers.

Likewise, computer usage itself often provides a veneer of controllability – we feel like we are in charge of our computers and online accounts in a way that we do not feel in charge of our physical safety in public. Individuals use computers from the relative safety and security of their own home and make what appear to be conscious choices about how they use these devices – setting their own passwords, choosing which websites they visit, and downloading the programs that they find most useful. This feeling of control is central to perceptions of risk – for example, it helps explain why people tend to be so much more scared of planes than automobiles, despite the fact that automobiles are exponentially more dangerous. People feel in control of automobiles – they are in the driver's seat – whereas being a passenger in a plane requires a surrender of control to those we do not necessarily know or trust. Computers possess that same characteristic feeling of control, particularly for those who use computers often in their daily life.[2]

As a result, the way that civilians think about cyber-threats versus physical threats suffers from an extreme form of probability neglect (Sunstein, 2003) whereby individuals "imagine the numerator" (Kahneman, 2011) and its "badness" and forget to think about the denominator - the actual probability that the event will come to pass. With terrorism, the denominator is very low; with cyber-threats, it is actually much higher. As a result, public support for costly counter-terror policies outstrips demand for costly cybersecurity policies, though the latter may in fact be a better use of limited tax-payer dollars. Moreover, the public will frequently make large, ill-advised changes to their personal behavior in the name of avoiding terrorism (such as driving rather than flying after 9/11, which is estimated to have contributed to 1,600 more traffic fatalities (Gaissmaier and Gigerenzer, 2012)), but few behavioral changes to protect their cyber-security (such as using more complicated passwords and changing them frequently).

However, we contend that exposure to a cyber-attack that does indeed personally threaten the individual may alter these underlying perceptions of dread and certainty. Namely, individuals may feel more personally vulnerable after experiencing an attack first-hand. They may learn from the exposure that this sense of security they had in using their computer was, in fact, misplaced. The personal data that they thought they had a high degree of control over is now shown to be very uncontrollable and vulnerable to breach. Moreover, the potential consequences of this breach – economic or reputational loss – are drawn into sharper relief. Thus, we expect exposure to a news story about a cyber-attack that compromised an individual's personal information to engender changes in perceptions about personal risk from cyber-attacks, attitudes toward government cybersecurity policies, and willingness to change personal online behaviors. In contrast, exposure to that same type of cyber-attack on a government target is unlikely to move risk perceptions to the same degree because it does not directly engage these two mechanisms of risk perception. In other words, an attack on the government fits the existing perception that citizens should not personally expect to be victimized and,

[2] In our study, we measure subjects' relative comfort with computers and find that, on average, comfort is very high. It is conceivable that other populations, for example the elderly, may feel less comfort and, therefore, see computer usage as more risky and uncertain.

so, does not increase a sense of dread. Moreover, because it fits the popular narrative of governments fighting directly with each other, it does not increase uncertainty.

4 Research Design

Getting at these specific mechanisms undergirding citizens' responses to cyber-threats requires experimental work to directly test the five core hypotheses that our cyber-risk theory makes regarding civilian responses to cyber-attacks.

4.1 *Study Hypotheses*

The cyber risk theory posits that exposure to cyber-attacks - particularly those personally relevant to the individual - should increase risk perceptions and, with that, change behavior and attitudes. As such, we have five central hypotheses:

- **H1a:** *Citizens will be more likely to overestimate the risk to their personal safety and report higher threat levels from cyber-attacks after exposure to any kind of cyber-attack.*
- **H1b:** *In particular, citizens will be more likely to overestimate the risk to their personal safety and report higher threat levels from cyber-attacks after exposure to attacks that directly threaten them than after attacks against the government (which do not directly threaten them).*
- **H2a:** *Citizens will be more likely to support larger, costlier government responses to cyber-attacks after exposure to any kind of cyber-attack.*
- **H2b:** *In particular, citizens will be more likely to support larger, costlier government responses to cyber-attacks following attacks on the mass public after exposure to attacks that directly threaten them than after attacks against the government (which do not directly threaten them).*
- **H3a:** *Citizens will be more likely to report a willingness to engage in cyber-protective behaviors after exposure to any kind of cyber-attack.*

- **H3b:** *In particular, citizens will be more likely to report a willingness to engage in cyber-protective behaviors after exposure to attacks that directly threaten them than after attacks against the government (which do not directly threaten them).*

- **H4a:** *Citizens will be more likely to actually engage in cyber-protective behaviors after exposure to any kind of cyber-attack.*

- **H4b:** *In particular, citizens will be more likely to actually engage in cyber-protective behaviors after exposure to attacks that directly threaten them than after attacks against the government (which do not directly threaten them).*

- **H5a:** *Citizens will be less likely to be susceptible to cyber-scams after exposure to any kind of cyber-attack.*

- **H5b:** *In particular, citizens will be less likely to be susceptible to cyber-scams after exposure to attacks that directly threaten them than after attacks against the government (which do not directly threaten them).*

4.2 *Participants*

To test these hypotheses, five hundred and eight students from the University of Michigan (211 males and 268 females), ages ranging from eighteen to fifty-eight ($M = 21.9957$, standard deviation [SD]=5.95), participated in the study and were entered into a raffle to win $50 USD for their participation.[3]

Figure 2 displays some basic descriptive statistics about the sample. White Americans (72%) were the most represented in our sample, followed by Asians (19%) and Hispanic (3%). 60% of our participants resides in suburban areas, and one-third resides in cities. Additionally, 30% of our sample identified that their annual family income was above $150,000 U.S. dollars, 16% identified that it was between $100,000-$150,000 U.S. dollars,

[3] Fifty-five students were omitted from our analyses because they did not finish the study. Additionally, seven more participants were excluded from our analyses because they fail two of our data checks: 1) they did not answer our attention question correctly; 2) they spent less than five seconds on article reading. As a result, our final sample consisted of four hundred forty-six participants (199 males and 242 females).

and about 9% mentioned that their families earned less than $10,000 U.S. dollars annually. Politically, the sample leaned to the left, like the University of Michigan in general, with 40.7% of the participants identifying themselves as belonging to the left or the extreme left, 19.7% identifying as moderate left-wingers, 11.4% identifying themselves as centrist, and 18% as belonging to the center-right, right, or extreme right.[4]

4.3 *Procedure*

All participants received a survey in which they were asked to answer several batteries of questions regarding political attitudes that past studies have found to be associated with cybersecurity policy attitudes and behaviors - partisanship, ideology and concerns about privacy and government surveillance. Additionally, we assessed subjects' comfort with using computers, their computer safety practices, general knowledge of cyber-terminology and high-profile cyber-attacks, and about any prior experiences of being a victim of hacking. Participants were then randomly assigned either to control, national, or personal condition. In the national scenario, participants were asked to read a fictional article (that they thought was genuine) about a cyber-attack on the U.S. government that took place a few days prior to the day that took the survey. In the personal scenario, participants were asked to read a fictional article (that they thought was genuine) about a cyber-attack against the university that they were attending (University of Michigan). As a result of this attack, students' record and ID numbers were stolen. After reading the article, the students were asked a battery of questions about their evaluation of gov-

[4] Though these samples are not representative, student samples are frequently used in social science research and appear to produce similar trends to those found in the general population (Altemeyer, 1996; Druckman and Kam, 2009; Mullinix et al., 2015). Additionally, students from our sample grew up with the internet always present and are more computer savvy than the older generations (Herring, 2008). In other words, our sample should have more access and a greater ability to use new technologies than the general population. They should thus *already* have a better understanding of the importance and value of government's cyber-policies and be most likely to practice safe computer behavior. Thus, if we see an impact of exposure on attitudes and behavior in this sample, it is likely that a less computer-literate sample would experience changes as well. In conclusion, as Druckman and Kam 2009 posit, while caution is advised, student samples are not an inherent problem for research.

ernment's cybersecurity policies and their online behavior.[5]

After respondents completed their survey forms, they received a debrief message that informed them the study was complete, but did not yet tell them that the news story they read was false. Later that evening, we sent an email to all participants that contained general tips on how to protect oneself online.[6] The email contained a title and four short blurbs with external links for additional information (in total five links).[7] Then, we matched up respondents' email addresses with their original survey form (for which they input their email in order to enter into a prize raffle) to monitor who opened this email and how many links the individual clicked on within this email. Thus, we were able to ascertain the impact of the manipulation on respondents' actual willingness to read more about tools for protecting their online security – a behavioral outcome.

The next morning, we emailed all participants, using a different email address (specifically created for this purpose) that contained a spam email informing them that they were about to receive an inheritance once they provided their personal information.[8] We were also able to monitor who opened this email and who responded to the provided email address. Then, we matched up respondents' email addresses with their original survey form in order to see if the manipulation affected respondents' susceptibility to online scams. Several hours later, all subjects received an actual debrief message – indicating that the news article they read the previous day was fictional and that both email messages had been a part of the study.

4.4 *Measures*

There are a variety of covariates that could potentially affect how exposure to cyberattacks changes attitudes and behavior. Most importantly, subjects' political predispositions and their familiarity and knowledge of cyber issues is likely to have a strong effect on how powerful exposure to a new cyber threat is on changing their political views

[5] The full survey instrument is located in the Online Appendix.

[6] The text of this email is in the Online Appendix.

[7] We provided links to real websites with information about how individuals could improve their security online.

[8] The text of this email is in the Online Appendix.

and personal behavior. To this end, we included several covariates in our study, using previously validated scales to assess each attribute.

Ideology was assessed using a 7-point scale from the American National Election Study, ranging from extremely liberal (1) to extremely conservative (7). *Party Identification* was assessed using a two-part question used in the American National Election Study to assess party identification on a 7-point scale from strong Democrat to strong Republican.

To measure *Privacy Concerns*, we used a six-question agree-disagree scale that measures respondents' concerns about government surveillance (Dinev, Hart and Mullen, 2008). Questions included the items, "The government needs to have greater access to personal information," "I am concerned about the power the government has to wiretap Internet activities," "The government needs broader wiretapping authority," "I am concerned that my Internet accounts and database information (e.g., e-mails, shopping records, tracking my Internet surfing, etc.) will be more open to government/business scrutiny," "The government needs to have more authority to use high tech surveillance tools for Internet eavesdropping," "I am concerned about the government's ability to monitor Internet activities." A high score on this scale represents individuals' higher level of concerns about government violating their privacy, while a low score represents individual's support of government's surveillance. This variable is important to measure because it is conceivable that a significant segment of the population is more worried about *government* hacking than *criminal or nonstate actor* hacking, in which case they may engage in very safe personal online behavior, but still be unwilling to support cybersecurity policies that potentially give the government more power.

To measure *Computer Safety*, we use an eight-question scale (Egelman and Peer, 2015). Questions included the items, "When I'm prompted about a software update, I install it right away," "I manually lock my computer screen when I step away from it," "I use a PIN or passcode to unlock my mobile phone," "I verify that my anti-virus software has been regularly updating itself," "When browsing websites, I mouseover links to see where they go before clicking them," "I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar," "I do not change my passwords unless I have to," "When I create a new online account, I try to use a password that goes beyond the site's minimum requirements," "I submit information to websites without first verifying that it will be sent securely (e.g., SSL, https://, a lock icon)." A high score on this scale represents individuals' more secure/careful online behavior. This *ex ante* level of computer safety may cause heterogeneity in the effect of exposure to a new cyber-threat: namely, those who already engage in safe computer practices will be less likely to shift their practices in response to a new threat.

Comfort with Computers Scale measures respondents' attitudes towards computers using a eight-item bi-polar scale developed by Shaft, Sharfman and Wu 2004. Questions contained eight pairs of adjectives that were used to describe computers. Some example of such pairs include: "Restrain creativity" vs. "Enhance creativity"; "Helpful" vs. "Harmful."[9] A high score on this scale represents individuals' high level of comfort using computers.

In this newly developed battery of questions, we ask respondents two types of questions to assess their *Computer Knowledge* – those regarding their knowledge of recent real-world cyber-attacks (e.g. Stuxnet virus, Sony Pictures Hack, WikiLeaks) and those about their familiarity with different types of cyber-attacks and what they do (for example, what a DDoS attack is, what phishing means, how to define a Trojan Horse). A high score on this scale represents individuals' better familiarity with cyber-attacks and cyber-terminology. To measure *Previous Exposure to Cyber-Attacks*, we asked respondents if (to their knowledge) they had ever had their online accounts hacked, had their computer infected with a virus, or had their personal information stolen. We measure this because other work in public opinion suggests that those most informed about an issue are least likely to change their views in response to new information. Thus, this is a potentially important source of response heterogeneity.

Moving to our dependent variables, we have three concepts of interest: 1) threat perceptions, 2) personal security behaviors; and 3) policy preferences. We operationalize each as follows. First, we measured individuals' *Threat Perception*, using four questions. Subjects were asked to estimate the likelihood of 1) cyber-attacks against the U.S government or infrastructure happening in the next year; 2) cyber-attacks against average American citizens happening in the next year; 3) they or someone they know being a victim of cyber-attacks in the next year; and 4) "the risk posed to their or their family's

[9] A complete list of adjectives can be found in the Online Appendix.

well-being" from a host of potential public health threats: gun violence, terrorism, heart disease, cancer, natural disasters, traffic accidents, cyber-attacks, or military conflict with nuclear powers.

Next, our *Policy Scale* measured individual's preferences towards various potential cybersecurity policies that have been suggested by national security professionals. We asked a series of six newly developed questions regarding potential policy responses that the government could engage in regards to cyber-threats, all of which were costlier than the status quo (on some dimension) and all of which have been recommended by cybersecurity experts. These questions asked participants' opinion on whether the government should 1) match salaries of Silicon Valley companies; 2) transfer some of the Department of Education budget into computer safety programs; 3) require private companies to disclose cyber-attacks; 3) share classified intelligence information on hackers with other countries; 4) adopt harsher legislation on cyber-crimes; 5) respond to every cyber-attack with retaliation for the purposes of deterrence. A high score on this scale represents individuals' higher support for these policies. We also asked a separate question regarding cyber-security spending, whether (and by how much) it should be increased or decreased.

Third, our *Online Behaviors* scale measured whether exposure to cyber-threats increased citizens' willingness to engage in costly or time-consuming cyber-protective behaviors. To assess this question, we asked seven questions, developed based on recommendations from cyber-security professionals. Specifically, we asked subjects how likely they were to start 1) using encrypted mobile messaging software; 2) using an encryption software on their computers; 3) using secure passwords; 4) updating their passwords more frequently; 5) using two-factor authentication; 6) covering their web-cameras; or 7) using only the secure versions of websites. A high score on this scale represents individuals' higher willingness to engage in safe online behavior.

5 Results

Statistical analysis for this study proceeded in three stages: 1) basic descriptive statistics of the sample to establish baseline attitudes and knowledge surrounding cyber-issues; 2) regression analysis of the main effects of the manipulation; and 3) regression analysis and the construction of marginal effects plots to explore potential heterogeneous treatment effects.

The results of the analysis revealed several interesting patterns in both citizens' baselines perceptions and behaviors and in their responses to exposure to threat. To begin, knowledge about cyber-issues and computer safety practices were indeed very low in our sample. Moreover, exposure to a personal cyber-threat resulted in significantly higher threat perceptions and perceived risk from hacking. Respondents in the personal threat condition were also marginally significantly more likely to express a willingness to engage in safer online behaviors in the future. This was, as expected, *not* the case after exposure to a cyber-attack on the government that was not personally relevant to the respondent. However, while respondents' expressed more support for increasing the cybersecurity budget in general, their specific policy preferences remained unchanged, even after exposure to a personal threat. Finally, though subjects expressed a *willingness* to engage in safer online behavior, their actual online behavior remained unchanged - respondents in the personal threat condition were no more likely to seek out information on cyber-security and were no less susceptible to spamming attempts than their counterparts in the other conditions. Below, we go into detail regarding each of these results.

5.1 *Descriptive Statistics and Correlations between Variables*

To begin, we analyzed basic descriptive statistics of our sample to get a sense of the socio-demographic distribution of our sample (Figure 2) as well as levels of cyber-knowledge and sophistication. This, in and of itself, is valuable, because little is known about how literate the general population is on issues of cybersecurity and computer safety.

Respondents were, in general, relatively concerned about privacy online and surveillance, perhaps stemming from, among other things, the 2013 Snowden revelations about the U.S. government spying on its citizens (Figure 3). 48% of all participants reported being at least somewhat concerned about their computer safety – a common trend across all conditions (Figure 4). Interestingly, despite being comfortable and actually enjoying using computers (Figure 5), 54.2% of the sample had very limited knowledge of cyber-terminology and of current events related to cybersecurity (Figure 6). This suggests that respondents think they are more sophisticated computers users than they actually are. 60.4% of the sample had either minor or no past experience with cyber-attacks (Figure 7).

Next, we analyzed some basic correlation patterns among our variables. Figure 8 displays a correlation matrix between our moderators and DVs. *Computer Safety* is positively correlated with both *Cyber Knowledge* and *Behavior Scale*, suggesting that people who care about their online safety are *already* more knowledgeable about current cyber-threats and are, perhaps, not as likely to be affected by our manipulation (Figure 6). *Cyber Knowledge* is also positively correlated with both *Privacy Concerns* and *Behavior Scale*, suggesting that the respondents who follow the news about cyber-attacks are more concerned about their privacy at baseline and, thus, are already involved in more careful online behavior. We explore these potential interaction effects below in Section 5.3.

5.2 *Main Effects*

While this general information about computer literacy and online safety habits in our sample are interesting, the core of our analysis - and contribution of this paper - focuses on the impact of exposure to a *new* cyber-threat on subsequent perceptions of risk, behavior and political attitudes. This section summarizes these main effects in detail. To begin, Figure 9 demonstrates that, as compared to respondents in the control condition, respondents in the national (but not personal) threat condition are marginally significantly more likely to believe that another attack against the United States government will happen in the next year ($\beta = 0.05, p < 0.05$). Likewise, as compared to respondents in the control condition, respondents in the personal (but not national) threat condition are significantly more likely to believe that another attack against citizens of the United

States will happen in the next year ($\beta = 0.07, p < 0.05$).

This is a relatively intuitive result - subjects are more likely to believe that an attack *similar to the one that just occurred* will happen in the future. However, it is interesting that subjects do not appear to extrapolate from one type of threat to another. In other words, if hackers can attack the U.S. Navy, it stands to reason they may also try to extract information from U.S. civilians (who are less well-protected), but respondents do not appear to recognize this potential for crossover attacks.

Next, we examined whether exposure to a cyber-attack could alter respondents' *personal* (rather than general, national) perceptions of threat. We found that, indeed, as compared to respondents in the control condition, respondents in the personal threat condition were marginally significantly more likely to believe that they personally would be the victim of a cyber-attack in the next year ($\beta = 0.04, p < .05$). Respondents in the national threat condition were, however, no more likely to believe that they personally would be the victim of a cyber-attack in the next year ($\beta = -0.01, p = NS$) (Figure 9 and Table 1). In other words, a cyber-attack that personally affected the individual significantly impacted perceptions of future risk, but a cyber-attack on the government did not. This is interesting since an attack on government databases arguable demonstrates higher capacity of the attacker to launch cyber-attacks in the future. But respondents do not appear to see it this way - they care more about who was attacked, rather than how difficult the attack was to pull off. Citizens' may also simply believe that the government will boost their cyber-capability as a result of the suffered attack.

As compared to respondents in the control condition, respondents in the personal threat condition were also significantly more likely to rank being the victim of a cyber-attack as a higher personal risk, when compared to other risks such as terrorism, gun violence, etc. ($\beta = 0.08, p < 0.05$). In contrast, respondents in the national threat condition were no more likely to rank being the victim of a cyber-attack as a higher personal risk ($\beta = 0.03, p = NS$) (Figure 9 and Table 1). Again, this demonstrates a failure by citizens to appreciate the potential for crossover cyber-operations - from a government target one time, to a civilian target the next.

But what effect does this exposure and increased threat perception have on actual political attitudes? Figure 10 and Table 2 demonstrate that as compared to respondents in the control condition, respondents in both the national ($\beta = 0.05, p < 0.05$) and personal threat ($\beta = 0.05, p < 0.05$) conditions were significantly more likely to support higher government spending on cyber-security programs .

However, surprisingly, while support for cybersecurity spending was altered by exposure to new cyber-threats, there was no effect of exposure on which *types* of cybersecurity policies respondents supported. In other words, we find that respondents in both the personal ($\beta = 0.003, p = NS$) and national threat ($\beta = 0.011, p = NS$) conditions were no more likely to support any of the cyber-security policies suggested by experts (Figure 11 and Table 3).[10]

Finally, we found that, as compared to respondents in the control condition, respondents in the personal threat condition were marginally significantly more likely to report that they would engage in a variety of safer online security behaviors ($\beta = 0.04, p < 0.05$). Respondents in the national threat condition were, in contrast, no more likely to report safer online practices ($\beta = 0.002, p = NS$) (Figure 12 and Table 4). Again, this result suggests that it is the personal relevance embodied in the exposure to a cyber-attack that has the potential to change future behavior. Attacks against other targets simply do not have the same personal resonance.

However, though subjects in the personal threat condition *said* they would engage in safer online behaviors, they were, in fact, no more likely to seek out information on cybersecurity in response to our follow-up email (by opening the email or clicking the links) ($\beta = 0, p = 0$) and were no less susceptible to spamming attempts ($\beta = 0, p = 0$). This suggests that simple exposure to a cyber-attack may not be enough to change actual online behavior, even if citizens' perception of risk are temporarily heightened and they express a willingness to change their behavior. This willingness does not actually translate into behavior (see Table 5).[11]

[10] We assessed these policies each individually and collectively as a scale.

[11] The null effect may also be due to ceiling or floor effects in this particular sample - almost all respondents opened the cybersecurity email and almost none clicked on any of the links; likewise almost all respondents opened the spam email and almost none responded to it.

5.3 *Heterogeneous Treatment Effects*

Finally, we turned to examine potential heterogeneous treatment effects in our sample. For example, based on the correlation patterns in our data, it stands to reason that respondents who are more careful with their computer usage or more knowledgeable about cyber-issues may be more willing to engage in cyber-protective behaviors across the board and not be affected much by the manipulation. On the other hand, those that are highly suspicious of government surveillance may be unwilling to support larger government interventions in the cyber-realm regardless of exposure to different types of cyber-threats.

These heterogeneous effects can be modeled using interactions terms in the regression model. The basic model is as follows:

$$Y_i = \alpha + \beta_1(T_i) + \beta_2(\gamma_i) + \beta_3[(T_i) * (\gamma_i)] + \beta_4(X_i)\epsilon_i, \tag{1}$$

In this regression, a moderator γ_i and an interaction term of the moderator and treatment condition $[(T_i) * (\gamma_i)]$ are introduced. If the interaction term β_3 is significant, marginal effects plots can then be used to make substantive interpretations regarding who is driving the treatment effect most – those high or low in γ_i.

Interestingly, we find that with each moderator tested - privacy concerns, computer safety practices, and knowledge of cyber terminology - it is those individuals *low* in each of these that are *most* moved by exposure to a personally relevant cyber-attack. In other words, respondents who, prior to the experiment, are not very concerned about surveillance or privacy online (Figure 14 & Table 7), are not very diligent in their computer safety behaviors (Figure 13 & Table 6), and who do not know much about cyber terminology or cyber current events (Figure 15 & Table 7), are most likely to have significantly increased perceptions of risk following exposure to the attack. This demonstrates how exposure to cyber attacks may be most important in catalyzing changes in attitudes and behaviors from segments of the population who, otherwise, may not be particularly concerned with cyber safety and security.

6 Discussion and Implications

The present research has demonstrated three important facets of the public's cyber-knowledge and responses to cyber-attacks.

First, on average, citizens' understanding of cyber-issues and familiarity with current events surrounding cyber is surprisingly low. Despite espousing a high confidence in the use of computers, the majority of our sample was unable to correctly answer questions about very high-profile cyber-attacks, such as WikiLeak's publication of Democratic National Committee emails during the election, Israel's and U.S.'s cyber-attack on Iran's Stuxnet program or North Korea's hack of Sony Entertainment. Moreover, subjects, in general, were unfamiliar with three of the most prevalent types of hacking - the use of a Trojan Horse, Distributed Denial of Service attacks, and the use of phishing tactics. Perhaps it is this lack of familiarity with cyber-risks that contributes to the relatively low rate of computer safety practices we observe in our sample at baseline. This is surprisingly because, again, we would expect the younger student sample used in our study to *most* familiar with computer usage and terminology, as compared to the general population

Second, we demonstrate that only certain types of exposure to cyber-attacks are likely to shift citizens' risk perceptions and attitudes. Namely, attacks on their government do little to alter respondents' perceptions of their own personal vulnerability and, as a result, do not change their willingness to use safer computer practices. Instead, an attack must be personally relevant to the respondent to trigger a change in perceptions. This suggests that citizens pay more attention to *who* was targeted rather than *how difficult* the attack was to accomplish. In other words, citizens, who are not very well-versed in the world of hacking, do not perceive cues about overall hacker capacity and how that may increase the possibility of *all* kinds of cyber-attacks, including those that threaten civilians.

Third, this study shows that even personal exposure to a cyber-attack may not be enough to change attitudes and behavior. On the one hand, subjects in the personal threat condition were more likely to *express* a willingness to change their online behavior, but this willingness did not manifest itself in their actual behavior only one day later.

Moreover, though subjects in both threat conditions expressed support for a higher cybersecurity budget, they were not any more supportive of new, costly cyber-policies that have been highlighted by national security experts as crucial in improving the United States' overall cybersecurity. This may be due to high levels of suspicion regarding government surveillance and reflect subjects' beliefs that cyber-threats are just as likely to come from state actors as non-state ones.

Finally, our experiment showed important heterogeneity among respondents - demonstrating that the citizens most likely to be affected by exposure to cyber-attacks are those citizens who previously possessed the least knowledge or concern about cyber-issues. This is a somewhat encouraging result, suggesting that even those with little interest in the world of cyber can have their perceptions changed following personal exposure to a cyber-threat.

These results have important implications for policymakers. Perhaps most critically, government and industry must do more to improve baseline knowledge of how individuals can secure their computers and find ways to drive home this message. Indeed, up to 30% of hacks on companies originate not with a software or hardware failure but with a wet-ware failure[12] (Levin, 2015). Even though companies are now beginning to provide training in basic online security, individuals need to change their mindset in order to internalize these messages and really change behavior. As our experiment has shown, the effective communication of *personal risk* from hacking, is one way to achieve this change in perception. Highlighting a vague threat or pointing to past attacks that are not personally relevant to the individual do not engage the dread and uncertainty dimensions that are most likely to increase perceptions of risk and, as a result, alter behavior.

An important question for future research is the extent to which these findings hold across national contexts. To this end, we are currently conducting a similar experiment in Ukraine. Ukraine is an interesting comparison case because it is much less well-developed than the United States, yet it has also suffered numerous high-profile cyber-attacks in recent years that may have increased the salience of cybersecurity issues

[12] *Wet-ware* is when workers fail to use basic cyber-hygiene to protect their computers, such as updating their software on time, changing passwords, etc.

for the civilian population there.

References

Acquisti, Alessandro, Laura Brandimarte and George Loewenstein. 2015. "Privacy and human behavior in the age of information." *Science* 347(6221):509–514.

Altemeyer, Bob. 1996. *The authoritarian specter*. Cambridge Univ Press.

Andres, Richard. 2012. "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence." *Trans. Array Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Derek S. Reveron. 1st ed. Washington DC: Georgetown University Press* .

Andrijcic, Eva and Barry Horowitz. 2006. "A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property." *Risk Analysis* 26(4):907–923.

Asal, Victor, Jacob Mauslein, Amanda Murdie, Joseph Young, Ken Cousins and Chris Bronk. 2016. "Repression, Education, and Politically Motivated Cyberattacks." *Journal of Global Security Studies* 1(3):235–247.

Bimber, Bruce. 2001. "Information and political engagement in America: The search for effects of information technology at the individual level." *Political Research Quarterly* 54(1):53–67.

Bonaci, Tamara, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno and Howard Jay Chizeck. 2015. "To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots." *arXiv preprint arXiv:1504.04339* .

Bovens, Mark and Stavros Zouridis. 2002. "From street-level to system-level bureaucracies: how information and communication technology is transforming administrative discretion and constitutional control." *Public administration review* 62(2):174–184.

Brants, KLK, Martine Huizenga, R van Meerten et al. 1996. "The new canals of Amsterdam: an exercise in local electronic democracy." *Media, Culture & Society* 18(2):233–249.

Canetti, Daphna, Michael L Gross and Israel Waismel-Manor. 2016. "Immune from Cyberfire?" *Binary Bullets: The Ethics of Cyberwarfare* p. 157.

Cerrudo, Cesar. 2017. "Why Cybersecurity Should Be The Biggest Concern Of 2017." *Forbes Magazine* .

Cheung-Blunden, Violet and Jiarun Ju. 2015. "Anxiety as a Barrier to Information Processing in the Event of a Cyberattack." *Political Psychology* .

Coleman, Gabriella. 2014. *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso books.

Coleman, Stephen, John Taylor and Wim van de Donk. 1999. *Parliament in the Age of the Internet*. Oxford University Press Oxford.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, Jonathan Zittrain and Miklos Haraszti. 2010. *Access controlled: The shaping of power, rights, and rule in cyberspace*. Mit Press.

Deibert, Ronald and Rafal Rohozinski. 2010. "Liberation vs. control: The future of cyberspace." *Journal of Democracy* 21(4):43–57.

Denning, Tamara, Cynthia Matuszek, Karl Koscher, Joshua R Smith and Tadayoshi Kohno. 2009. A spotlight on security and privacy risks with future household robots: attacks and lessons. In *Proceedings of the 11th international conference on Ubiquitous computing*. ACM pp. 105–114.

Dinev, Tamara, Paul Hart and Michael R Mullen. 2008. "Internet privacy concerns and beliefs about government surveillance–An empirical investigation." *The Journal of Strategic Information Systems* 17(3):214–233.

Druckman, James N and Cindy D Kam. 2009. "Students as experimental participants: A defense of the'narrow data base'." *Available at SSRN 1498843* .

Egelman, Serge and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM pp. 2873–2882.

Franzen, Axel. 2000. "Does the Internet make us lonely?" *European Sociological Review* 16(4):427–438.

Gaissmaier, Wolfgang and Gerd Gigerenzer. 2012. "9/11, Act II A Fine-Grained Analysis of Regional Variations in Traffic Fatalities in the Aftermath of the Terrorist Attacks." *Psychological science* p. 0956797612447804.

Hartmann, Kim and Christoph Steup. 2013. The vulnerability of UAVs to cyber attacks-An approach to the risk assessment. In *Cyber Conflict (CyCon), 2013 5th International Conference on*. IEEE pp. 1–23.

Haynes, Audrey A and Brian Pitts. 2009. "Making an impression: New media in the 2008 presidential nomination campaigns." *PS: Political Science & Politics* 42(01):53–58.

Herring, Susan C. 2008. "Questioning the generational divide: Technological exoticism and adult constructions of online youth identity." *Youth, identity, and digital media* pp. 71–94.

Howard, Philip EN, Less Rainie and STEVE Jones. 2001. "Days and nights on the Internet." *American Behavioral Scientist* 45(3):383–404.

Igure, Vinay M, Sean A Laughter and Ronald D Williams. 2006. "Security issues in SCADA networks." *Computers & Security* 25(7):498–506.

Javaid, Ahmad Y, Weiqing Sun, Vijay K Devabhaktuni and Mansoor Alam. 2012. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*. IEEE pp. 585–590.

Kahneman, Daniel. 2011. *Thinking, fast and slow*. Macmillan.

Kim, Alan, Brandon Wampler, James Goppert, Inseok Hwang and Hal Aldridge. 2012. Cyber attack vulnerabilities analysis for unmanned aerial vehicles. In *Infotech@ Aerospace 2012*. p. 2438.

King, Gary, Jennifer Pan and Margaret E Roberts. 2013. "How censorship in China allows government criticism but silences collective expression." *American Political Science Review* 107(2):326–343.

King, Gary, Jennifer Pan and Margaret E Roberts. 2017. "How the Chinese government fabricates social media posts for strategic distraction, not engaged argument." *American Political Science Review* 111(3):484–501.

Kluver, Randolph. 2004. "Political culture and information technology in the 2001 Singapore general election." *Political Communication* 21(4):435–458.

Kostyuk, Nadiya and Yuri M. Zhukov. 2017. "Invisible Digital Front: Can cyber attacks shape battlefield events?" *Journal of Conflict Resolution* p. forthcoming.

Kshetri, Nir. 2010. *The global cybercrime industry: economic, institutional and strategic perspectives*. Springer Science & Business Media.

Levin, Adam. 2015. "Wetware: The Major Data Security Threat You've Never Heard Of." *Forbes Magazine* .

Libicki, Martin C. 2009. *Cyberdeterrence and cyberwar*. Rand Corporation.

Lupia, Arthur and Gisela Sin. 2003. "Which public goods are endangered?: How evolving communication technologies affect the logic of collective action." *Public Choice* 117(3-4):315–331.

MacKinnon, Rebecca. 2013. *Consent of the networked: The worldwide struggle for Internet freedom*. Basic Books (AZ).

McClean, Jarrod, Christopher Stull, Charles Farrar and David Mascareñas. 2013. A preliminary cyber-physical security assessment of the Robot Operating System (ROS). In *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics pp. 874110–874110.

Mossberger, Karen, Caroline J Tolbert and Mary Stansbury. 2003. *Virtual inequality: Beyond the digital divide*. Georgetown University Press.

Mullinix, Kevin J, Thomas J Leeper, James N Druckman and Jeremy Freese. 2015. "The generalizability of survey experiments." *Journal of Experimental Political Science* 2(02):109–138.

Nicholson, Andrew, Stuart Webber, Shaun Dyer, Tanuja Patel and Helge Janicke. 2012. "SCADA security in the light of Cyber-Warfare." *Computers & Security* 31(4):418–436.

Norberg, Patricia A, Daniel R Horne and David A Horne. 2007. "The privacy paradox: Personal information disclosure intentions versus behaviors." *Journal of Consumer Affairs* 41(1):100–126.

Polat, Rabia Karakaya. 2005. *European journal of communication* 20(4):435–459.

Ralston, Patricia AS, James H Graham and Jefferey L Hieb. 2007. "Cyber security risk assessment for SCADA and DCS networks." *ISA transactions* 46(4):583–594.

Richards, James R. 1998. *Transnational criminal organizations, cybercrime, and money laundering: a handbook for law enforcement officers, auditors, and financial investigators*. CRC press.

Robinson, John P, Meyer Kestnbaum, Alan Neustadtl and Anthony Alvarez. 2000. "Mass media use and social life among Internet users." *Social Science Computer Review* 18(4):490–501.

Sanovich, Sergey, Denis Stukal, Duncan Penfold-Brown and Joshua Tucker. 2015. Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia. In *Annual Conference of the International Society of New Institutional Economics*.

Scavo, Carmine and Yuhang Shi. 2000. "Public Administration The Role of Information Technology in the Reinventing Government ParadigmŠNormative Predicates and Practical Challenges." *Social Science Computer Review* 18(2):166–178.

Shaft, Teresa M, Mark P Sharfman and Wilfred W Wu. 2004. "Reliability assessment of the attitude towards computers instrument (ATCI)." *Computers in human behavior* 20(5):661–689.

Sharma, Amit. 2010. "Cyber Wars: A Paradigm Shift from Means to Ends." *Strategic Analysis* 34(1):62–73.

Siddiqui, Aisha P and Nash Unsworth. 2011. "Investigating the role of emotion during the search process in free recall." *Memory & cognition* 39(8):1387–1400.

Slovic, Paul. 2016. *The perception of risk*. Routledge.

Sunstein, Cass R. 2003. "Terrorism and probability neglect." *Journal of Risk and Uncertainty* 26(2-3):121–136.

Taylor, Robert W, Eric J Fritsch and John Liederbach. 2014. *Digital crime and digital terrorism*. Prentice Hall Press.

Villeneuve, Nart and Masashi Crete-Nishihata. 2011. "Control and Resistance: Attacks on Burmese Opposition Media." *Access Contested, ONI [OpenNet Initiative] Access: Denied, Controlled, Contested: http://access. opennet. net/contested/chapters/, geprüft am* 14:2012.

Weber, Lori M, Alysha Loumakis and James Bergman. 2003. "Who participates and why? An analysis of citizens on the Internet and the mass public." *Social Science Computer Review* 21(1):26–42.

Welch, Eric W and Shelley Fulla. 2005. "Virtual interactivity between government and citizens: The Chicago Police Department's citizen ICAM application demonstration case." *Political communication* 22(2):215–236.

7 Figures & Tables

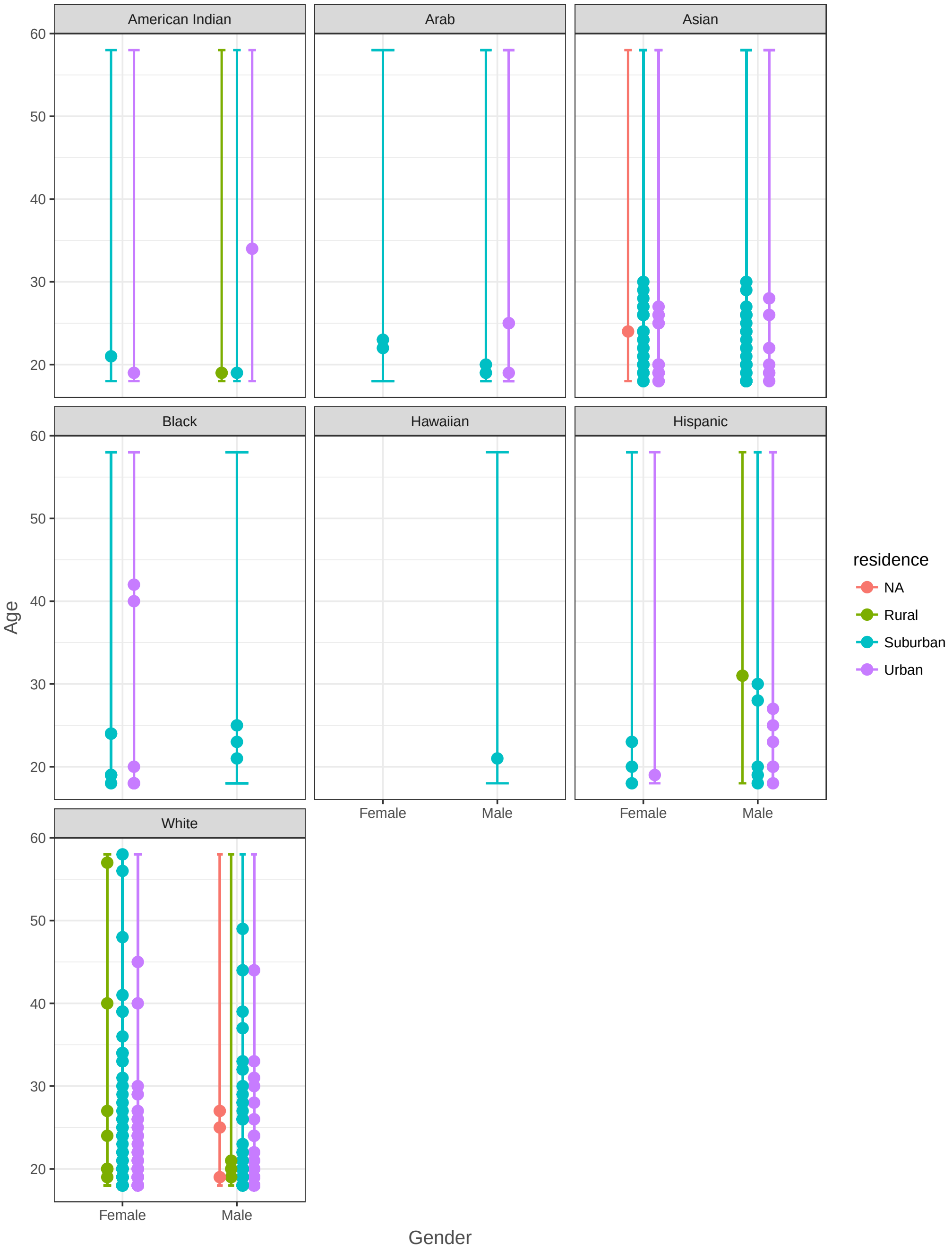

Figure 2: Sample Demographics

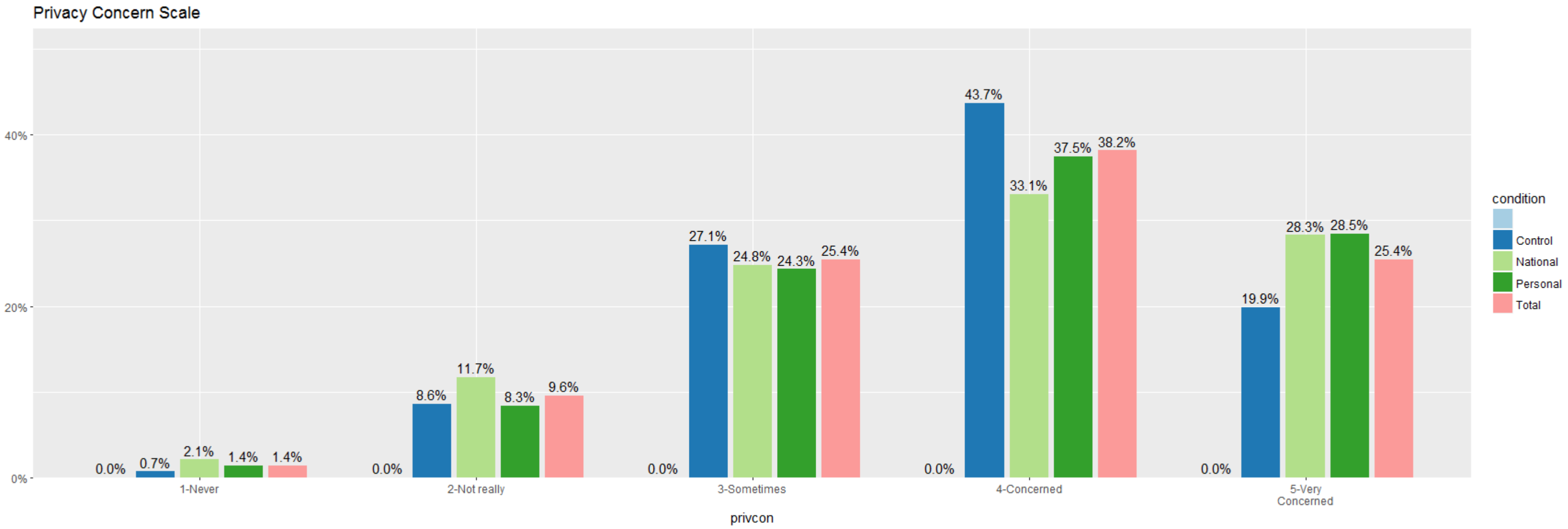

Figure 3: Privacy Concern Scale

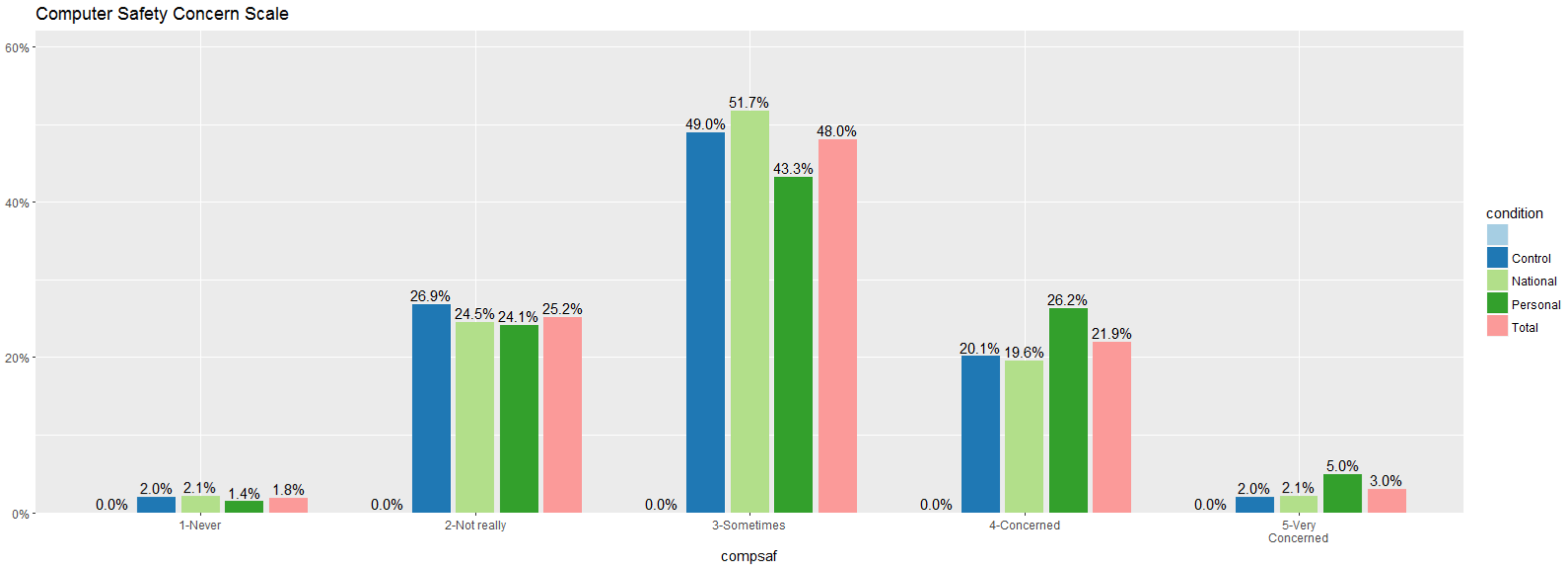

Figure 4: Computer Safety Concern

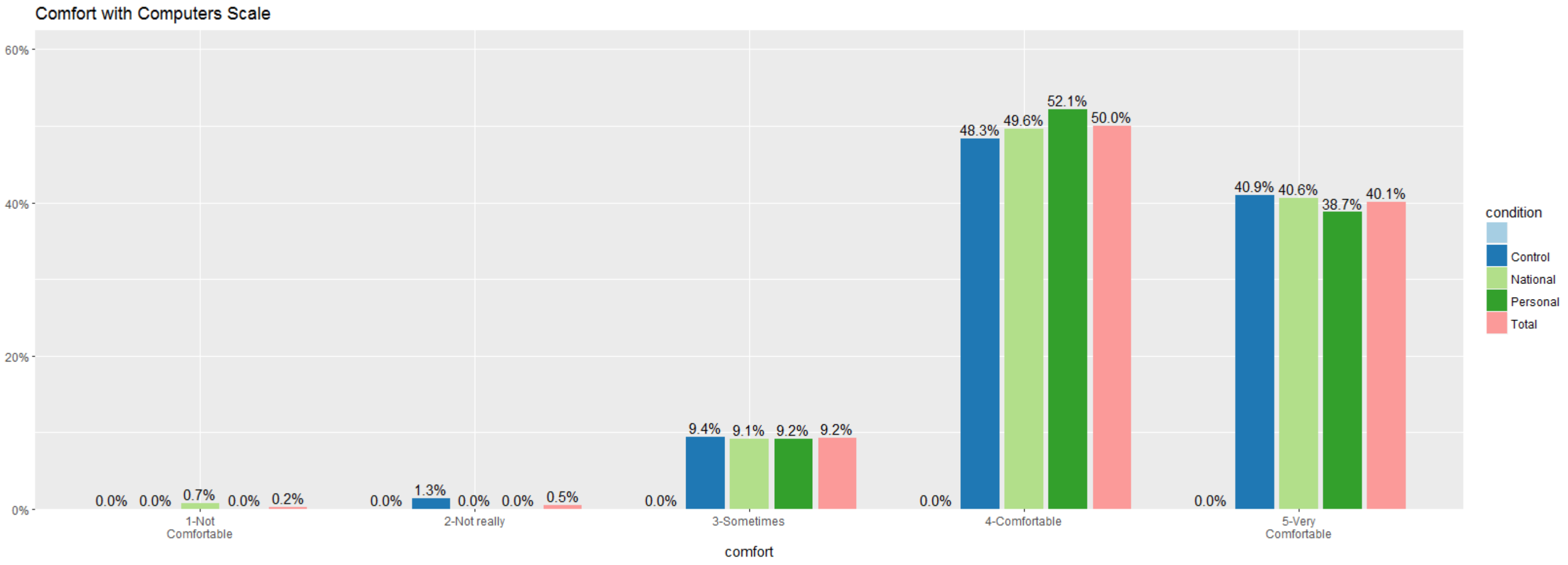

Figure 5: Comfort Using Computers

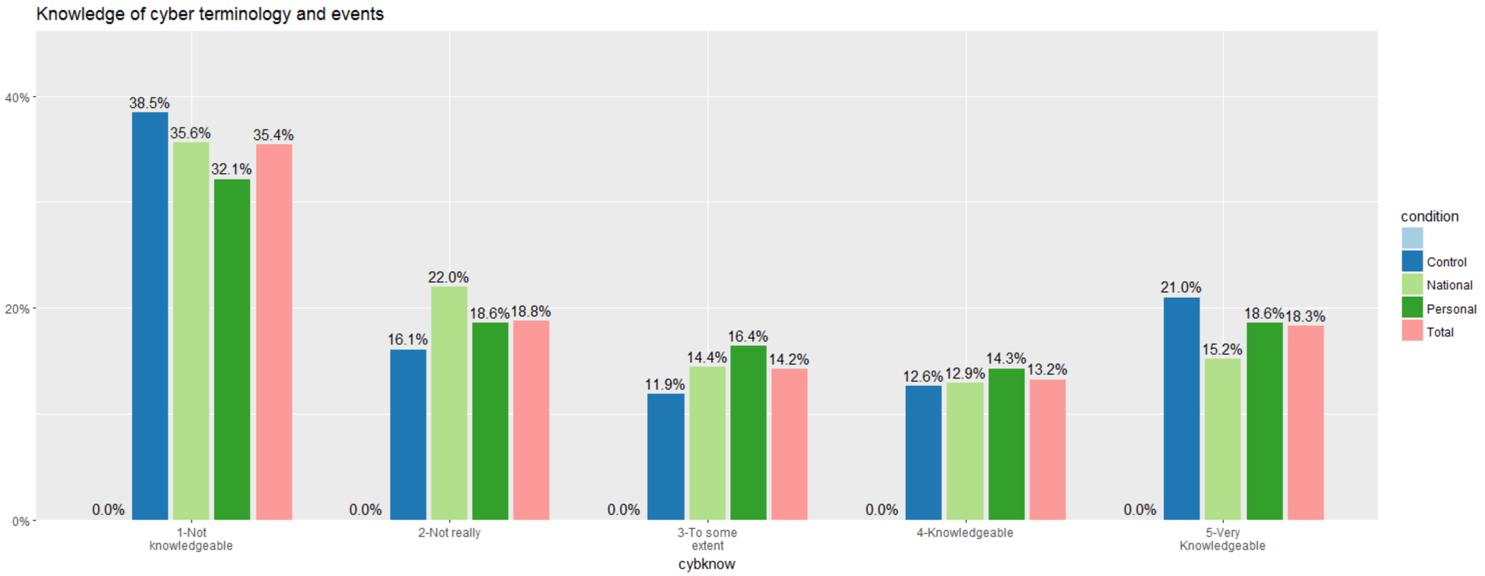

Figure 6: Knowledge of cyber terminology and events

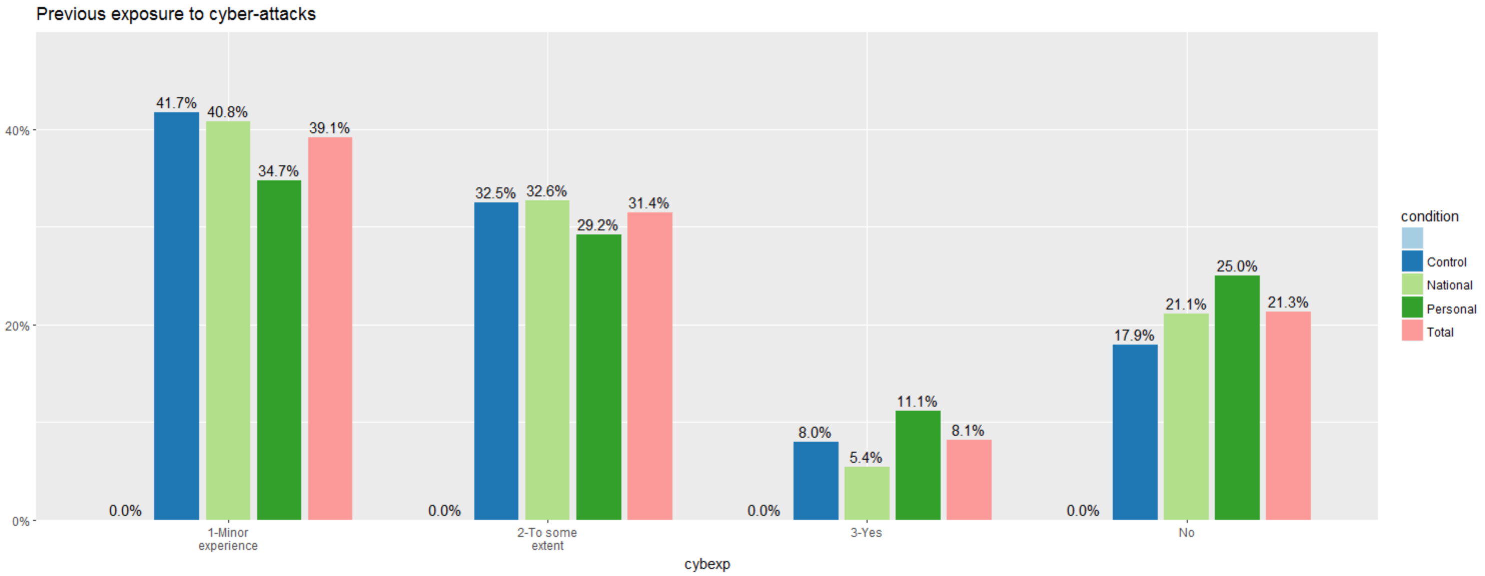

Figure 7: Previous exposure to cyber attacks

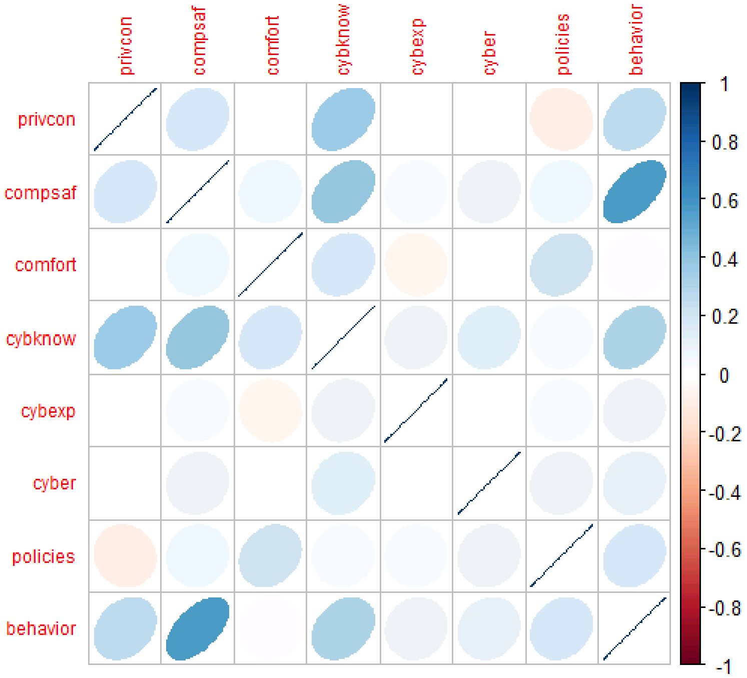

Figure 8: Correlation Matrix between Moderators and DVs

Figure 9: Threat Perceptions

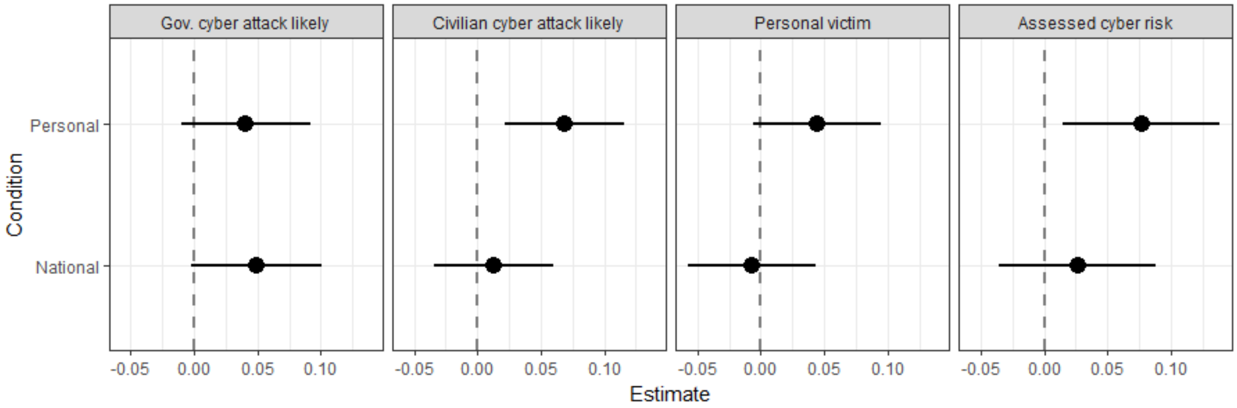

Table 1: Threat perceptions

	Dependent variables			
	Likelihood of cyber attacks against the government	*Likelihood of cyber attacks against civilians*	*Likelihood of becoming a victim of cyber attacks*	*Higher likelihood of becoming a victim of cyber attacks*
National	0.049* (0.026)	0.013 (0.024)	-0.007 (0.026)	0.026 (0.032)
Personal	0.041 (0.026)	0.069*** (0.024)	0.044* (0.026)	0.077** (0.032)
Constant	0.732*** (0.018)	0.780*** (0.017)	0.683*** (0.018)	0.500*** (0.022)
N	440	440	440	438
R-squared	0.009	0.021	0.010	0.014
Adj. R-squared	0.005	0.016	0.006	0.009
Residual Std. Error	0.224 (df = 437)	0.206 (df = 437)	0.221 (df = 437)	0.270 (df = 435)
F Statistic	2.044 (df = 2; 437)	4.617** (df = 2; 437)	2.277 (df = 2; 437)	3.058** (df = 2; 435)

$^{***}p < .01$; $^{**}p < .05$; $^{*}p < .1$

Figure 10: Spending Preferences

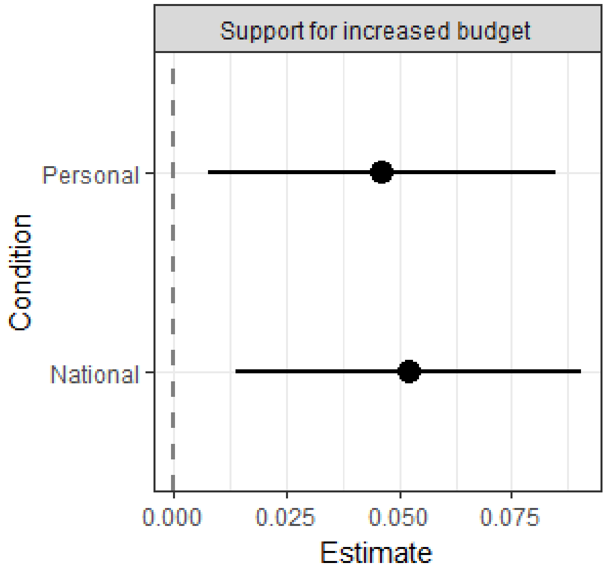

Table 2: Spending Preferences

	Support for increased budget
National	0.052*** (0.019)
Personal	0.046** (0.020)
Constant	0.723*** (0.014)
N R-squared Adj. R-squared Residual Std. Error F Statistic	436 0.020 0.015 0.167 (df = 433) 4.306** (df = 2; 433)
***p < .01; **p < .05; *p < .1	

Figure 11: Support for Cybersecurity Policies

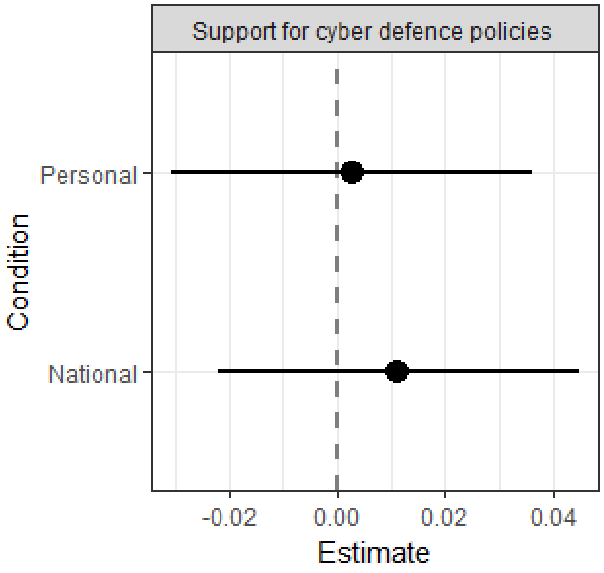

Table 3: Support for Cybersecurity Policies

	Support for cybersecurity policies
National	0.011 (0.017)
Personal	0.003 (0.017)
Constant	0.555*** (0.012)
N R-squared Adj. R-squared Residual Std. Error F Statistic	433 0.001 -0.004 0.145 (df = 430) 0.239 (df = 2; 430)
$^{***}p < .01$; $^{**}p < .05$; $^{*}p < .1$	

Figure 12: Online Behavior

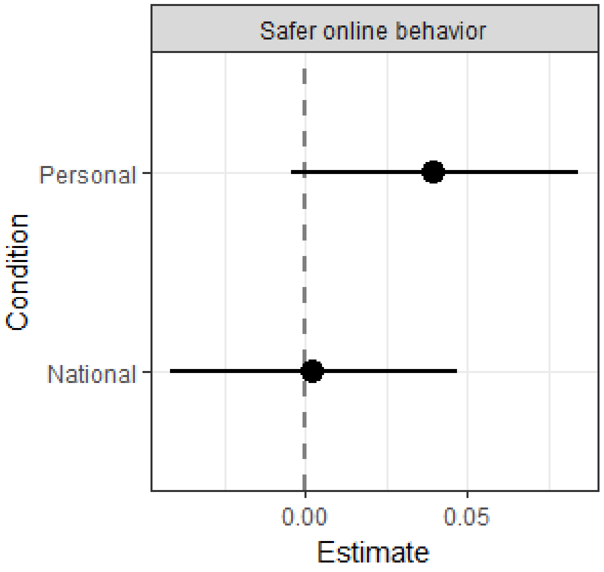

Table 4: Online Behavior

	Safer online behavior
National	0.002
	(0.023)
Personal	0.040*
	(0.023)
Constant	0.457***
	(0.016)
N	397
R-squared	0.010
Adj. R-squared	0.005
Residual Std. Error	0.184 (df = 394)
F Statistic	1.913 (df = 2; 394)
***p < .01; **p < .05; *p < .1	

Table 5: Behavior Measures

	Opened Email with Cybersecurity Tips	*Number of Links Clicked*	*Opened Spam Email*
National	-0.101^{**}	0.029	0.003
	(0.051)	(0.030)	(0.048)
Personal	0.004	-0.004	0.093
	(0.052)	(0.030)	(0.057)
Constant	0.757^{***}	0.066^{***}	0.178^{***}
	(0.036)	(0.021)	(0.032)
Observations	446	446	353
R^2	0.012	0.003	0.009
Adjusted R^2	0.007	-0.001	0.003
Residual Std. Error	0.446 (df = 443)	0.262 (df = 443)	0.399 (df = 350)
F Statistic	2.642^{*} (df = 2; 443)	0.693 (df = 2; 443)	1.528 (df = 2; 350)
$^{***}p < .01$; $^{**}p < .05$; $^{*}p < .1$			

Table 6: Heterogeneous treatment effects: Computer Safety

	Likelihood of cyber attacks against the government	*Likelihood of cyber attacks against civilians*	*Likelihood of becoming a victim of cyber attacks*	*Higher likelihood of becoming a victim of cyber attacks*	*Support for increased budget*	*Safer online behavior*	*Support for cybersecurity policies*
National	0.173*	0.177**	0.076	0.407***	0.110	0.104	0.024
	(0.094)	(0.086)	(0.093)	(0.111)	(0.070)	(0.068)	(0.063)
Personal	0.213**	0.150*	0.144	0.323***	-0.016	0.075	-0.016
	(0.092)	(0.083)	(0.091)	(0.108)	(0.069)	(0.066)	(0.060)
Computer safety	0.195	0.324***	0.180	0.569***	0.111	0.825***	0.035
	(0.128)	(0.116)	(0.126)	(0.151)	(0.096)	(0.093)	(0.084)
National*Computer safety	-0.254	0.343**	-0.162	-0.774***	-0.125	-0.230*	-0.031
	(0.184)	(0.167)	(0.181)	(0.217)	(0.137)	(0.133)	(0.122)
Personal*Computer safety	-0.343*	-0.180	-0.202	-0.499**	0.116	-0.117	0.034
	(0.176)	(0.160)	(0.173)	(0.208)	(0.133)	(0.126)	(0.115)
Constant	0.638***	0.624***	0.595***	0.221***	0.669***	0.055	0.538***
	(0.065)	(0.059)	(0.064)	(0.077)	(0.049)	(0.047)	(0.043)
N	431	431	431	427	427	388	424
R-squared	0.019	0.042	0.014	0.052	0.035	0.338	0.003
Adj. R-squared	0.007	0.031	0.00	0.041	0.024	0.329	-0.009
Residual Std. Error	0.224 (df = 425)	0.204 (df = 425)	0.221 (df = 425)	0.264 (df = 421)	0.166 (df = 421)	0.151 (df = 382)	0.145 (df = 418)
F Statistic	1.614 (df = 5; 425)	3.717*** (df = 5; 425)	1.240 (df = 5; 425)	4.663*** (df = 5; 421)	3.087*** (df = 5; 421)	38.923*** (df = 5; 382)	0.244 (df = 5; 418)
***p < .01; **p < .05; *p < .1							

Table 7: Heterogeneous treatment effects: Privacy Concerns

	Likelihood of cyber attacks against the government	*Likelihood of cyber attacks against civilians*	*Likelihood of becoming a victim of cyber attacks*	*Higher likelihood of becoming a victim of cyber attacks*	*Support for increased budget*	*Safer online behavior*	*Support for cybersecurity policies*
National	-0.041	0.210***	-0.023	0.160	0.122*	0.012	0.009
	(0.089)	(0.080)	(0.087)	(0.108)	(0.067)	(0.074)	(0.058)
Personal	0.112	0.183**	0.079	0.325***	0.026	0.137*	0.013
	(0.093)	(0.084)	(0.091)	(0.112)	(0.070)	(0.076)	(0.060)
Privacy concerns	0.022	0.374***	0.181*	0.223*	0.055	0.306***	-0.065
	(0.097)	(0.087)	(0.094)	(0.116)	(0.072)	(0.079)	(0.062)
National*Privacy concerns	0.135	-0.300**	0.025	-0.196	-0.107	-0.017	0.008
	(0.130)	(0.117)	(0.128)	(0.157)	(0.098)	(0.108)	(0.084)
Personal*Privacy concerns	-0.105	-0.183	-0.059	-0.364**	0.027	-0.156	-0.012
	(0.133)	(0.120)	(0.130)	(0.160)	(0.100)	(0.109)	(0.086)
Constant	0.717***	0.535***	0.565***	0.351***	0.687***	0.258***	0.597***
	(0.066)	(0.059)	(0.064)	(0.079)	(0.049)	(0.053)	(0.042)
N	438	438	438	433	434	395	431
R-squared	0.018	0.074	0.035	0.028	0.026	0.090	0.011
Adj. R-squared	0.007	0.063	0.024	0.017	0.014	0.078	-0.001
Residual Std. Error	0.224 (df = 432)	0.202 (df = 432)	0.219 (df = 432)	0.269 (df = 427)	0.167 (df = 428)	0.177 (df = 389)	0.144 (df = 425)
F Statistic	1.607 (df = 5; 432)	6.877*** (df = 5; 432)	3.171*** (df = 5; 432)	2.464** (df = 5; 427)	2.246** (df = 5; 428)	7.686*** (df = 5; 389)	0.910 (df = 5; 425)

$^{***}p < .01$; $^{**}p < .05$; $^{*}p < .1$

Table 8: Heterogeneous treatment effects: Cyber Knowledge

	Likelihood of cyber attacks against the government	*Likelihood of cyber attacks against civilians*	*Likelihood of becoming a victim of cyber attacks*	*Higher likelihood of becoming a victim of cyber attacks*	*Support for increased budget*	*Safer online behavior*	*Support for cybersecurity policies*
National	-0.056	-0.014	0.015	0.005	0.044	0.053	0.004
	(0.060)	(0.060)	(0.066)	(0.067)	(0.054)	(0.049)	(0.048)
Personal	-0.033	0.042	0.053	0.049	0.020	0.016	0.010
	(0.057)	(0.057)	(0.062)	(0.062)	(0.052)	(0.047)	(0.046)
Cyber knowledge	-0.035	-0.003	0.155	0.344***	0.124	0.263***	0.213**
	(0.113)	(0.113)	(0.124)	(0.124)	(0.102)	(0.092)	(0.089)
National X Cyber knowledge	0.191	0.109	-0.058	-0.030	-0.005	-0.089	0.105
	(0.177)	(0.177)	(0.195)	(0.194)	(0.160)	(0.142)	(0.139)
Personal X Cyber knowledge	0.244	-0.080	-0.069	-0.244	0.084	-0.080	0.120
	(0.161)	(0.162)	(0.178)	(0.176)	(0.146)	(0.133)	(0.128)
Constant	0.716***	0.641***	0.462***	0.207***	0.658***	0.482***	0.481***
	(0.041)	(0.041)	(0.045)	(0.045)	(0.038)	(0.034)	(0.033)
N	297	298	298	278	293	282	278
R-squared	0.019	0.005	0.011	0.046	0.027	0.053	0.095
Adj. R-squared	0.002	-0.012	-0.006	0.028	0.010	0.036	0.078
Residual Std. Error	0.282 (df = 291)	0.283 (df = 292)	0.311 (df = 292)	0.303 (df = 272)	0.254 (df = 287)	0.225 (df = 276)	0.218 (df = 272)
F Statistic	1.122 (df = 5; 291)	0.288 (df = 5; 292)	0.655 (df = 5; 292)	2.603** (df = 5; 272)	1.567 (df = 5; 287)	3.107*** (df = 5; 276)	5.712*** (df = 5; 272)

$^{***}p < .01$; $^{**}p < .05$; $^{*}p < .1$

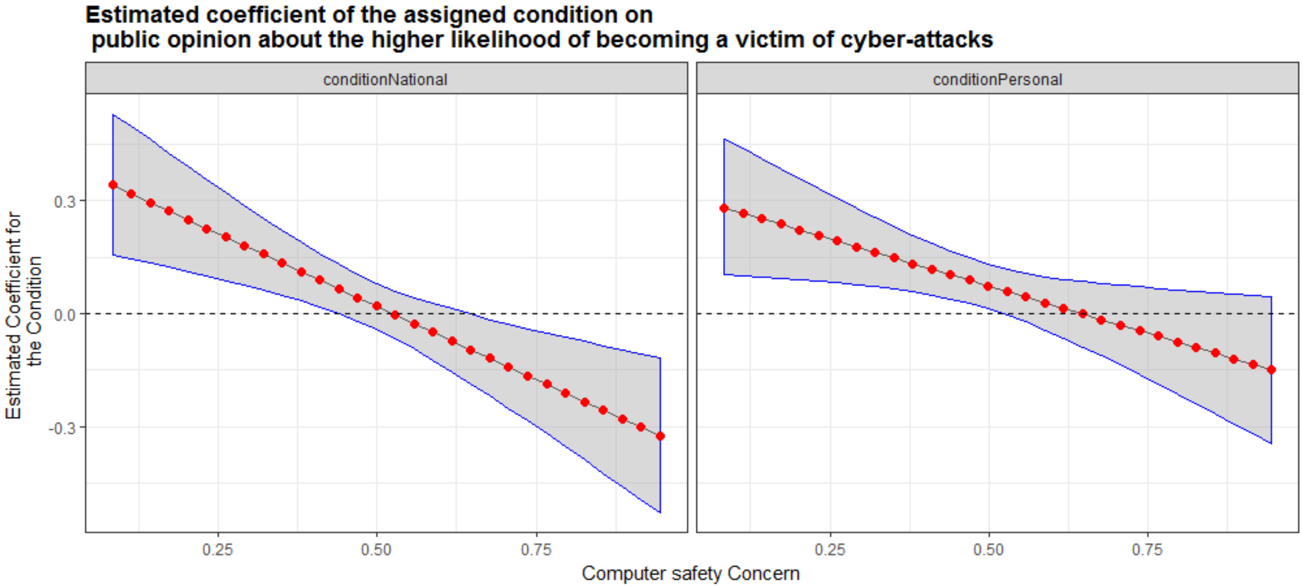

Figure 13: *Marginal Plot: Computer Safety & Condition*

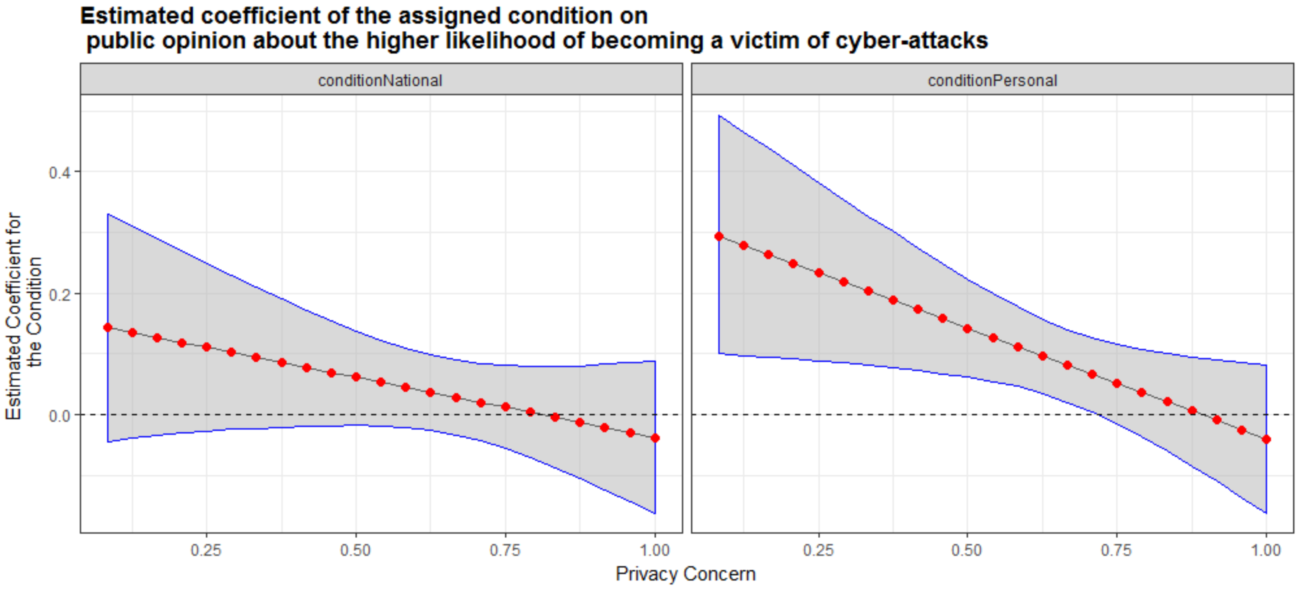

Figure 14: *Marginal Plot: Privacy Concern & Condition*

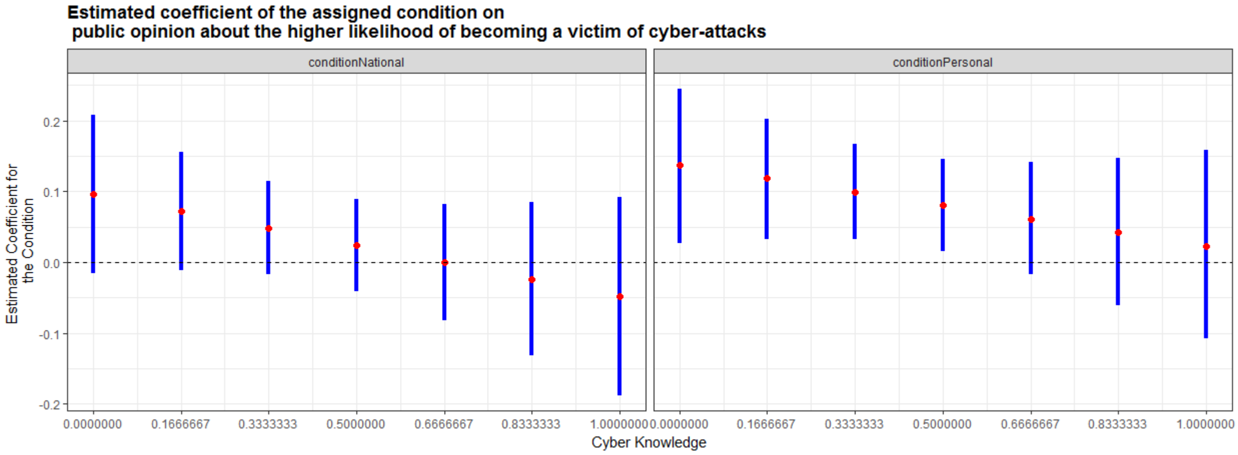

Figure 15: *Marginal Plot: Cyber Knowledge & Condition*