Journal of Experimental Criminology
https://doi.org/10.1007/s11292-022-09515-z

Ransomware and the Robin Hood effect?: Experimental evidence on Americans' willingness to support cyber-extortion

Murat Haner[1] · Melissa M. Sloan[2] · Amanda Graham[3] · Justin T. Pickett[4] · Francis T. Cullen[5]

Accepted: 5 May 2022

Abstract

Objectives Ransomware attacks have become a critical security threat worldwide. However, existing research on ransomware has largely ignored public opinion. This initial study identifies patterns in the American public's support for the use of ransomware, specifically when it is framed to provide benefits to others (i.e., in-group members). Drawing on the Robin Hood decision-making literature and Moral Foundations Theory, we offer theoretical predictions regarding ransomware support.

Methods In a survey of 1013 Americans, we embedded a split-ballot experiment in which respondents were randomly assigned to indicate their level of support or opposition to one of two sets of six ransomware scenarios. We manipulated the nationality, authority level, and political affiliation of the actors.

Results We find that people are more supportive of ransomware use when the actors are from their own in-group, and the outcomes benefit their in-group members. Also, the more strongly participants endorsed the moral foundations of authority and harm/care, the more supportive they were of the use of ransomware that may benefit others from their in-group.

Conclusions These findings suggest political actors may be able to generate public support for morally questionable actions by emphasizing in-group benefits and the Robin Hood nature of an attack (e.g., outcome-based morality).

Keywords Ransomware · Cyberattacks · Extortion · Robin Hood effect · Public opinion · Outcome-based morality

✉ Murat Haner
mhaner@asu.edu

[1] Arizona State University, Phoenix, AZ, USA

[2] University of South Florida, Tampa, FL, USA

[3] Georgia Southern University, Statesboro, GA, USA

[4] University at Albany, Albany, NY, USA

[5] University of Cincinnati, Cincinnati, OH, USA

Published online: 13 June 2022

Ransomware—a type of malware attack launched by hackers to encrypt and exfiltrate data on electronic systems until a ransom is paid for their release—is not new. In fact, the use of ransomware to extract financial benefits and exploits by criminals has been around for many decades, with early examples dating back to the late 1980s (Brooks, 2021). Yet, it has grown rampant today and has become a critical threat to the national security and economic stability of many countries around the world (Craig, 2021). This spread and impact has occurred mostly because, in today's world, technology has become embedded into every aspect of our lives (from homes to businesses to government), and the gains that can be accrued from ransomware can be substantial. Unlike in the past, when attackers would encrypt files to steal hundreds of dollars from random individual consumers, they are now targeting large organizations, demanding millions of dollars, and bringing down critical infrastructures such as hospitals, power grids, police stations, banks, and telecommunication systems, until their demands are met (Hugget, 2021; Telang, 2021; Welburn & Hodgson, 2021). Cybercriminals have learned how lucrative the ransomware business can be, and they have developed increasingly sophisticated victimization techniques, making it harder for organizations to protect their assets (Cook, 2021; Fung, 2021).

The complexity of ransoming, however, is that it is possible for an attack to be construed as an act for the public good—what we term the "Robin Hood Effect." This is a case where the ends might be seen as justifying otherwise untoward means. For example, in August 2021, a cyberattack on the totalitarian government of Belarus compromised dozens of police and interior ministry databases. The hackers leaked official documents indicating the unlawful surveillance, torture, and arrest efforts of the government and threatened to leak sensitive information about President Lukashenko and his inner circles unless the Belarusian government stopped its human rights violations (CSIS, 2021; Marks, 2021). During the same month, a group of hackers targeted a high-profile prison housing political prisoners in Tehran, Iran, and shared several videos and images showing the violent treatment of prisoners. The group threatened to leak even more disturbing footage that would embarrass Iran in the international arena unless the Iranian government made efforts to reform the conditions at this infamous prison (Gambrell, 2021).

There are countless other examples of cyberattacks and ransoming for what many may argue are good deeds, such as retaliating against child pornography websites by publishing the names of individuals who subscribe to these outlets (BBC, 2011), targeting the webpages of hate groups (e.g., Anonymous' hack of Nazi website after the Charlottesville White Nationalist rally) (Griffin, 2017), and destroying the electronic databases of corrupt governments to force dictators to resign (e.g., Operation Free Korea's effort to have South Korea's controversial leader resign by threatening to release the usernames and passwords of government web services) (Love, 2013). In what circumstances (and for what ends) cyberattacks are deemed socially acceptable, then, remains an open question and one of growing importance.

Even the United States has repeatedly used its cyber capabilities to achieve certain goals by crippling another country's infrastructure. For example, Stuxnet, the extremely sophisticated computer worm created during the Bush and Obama administrations, prevented a high-scale regional war in the Middle East by destroying the Iranian centrifuges at Natanz nuclear facility that produce enriched uranium to power atomic weapons (Fruhlinger, 2017; Rosenbaum, 2012). This attack (Operation Olympic Games) was seen as a nonviolent alternative to a traditional war, as it stopped

Israel from launching a heavy-scale airstrike, which could potentially prompt a regional conflict (Broad et al., 2011; Nakashima & Warrick, 2012). It also sent a clear message to Iran that the United States had the capability to disable or even destroy the country's nuclear program if they used it for any purposes other than supporting its energy needs (Sanger, 2012).

The Robin Hood effect and support for extortion

Ransoming is clearly a moral issue and a form of deviance. However, moral psychology research indicates that humans frequently engage in and justify deviant behavior when the results benefit themselves or other in-group members (Babu et al., 2020; Brelnes, 2020; Cadsby et al., 2016; Shalvi et al., 2015). As Sykes and Matza (1957) describe in their techniques of neutralization typology, this "appeal to higher loyalties" technique justifies deviant behavior as a service to others. More colloquially, this may be described as a Robin Hood effect, after the classic tale in which Robin Hood and his friends steal from rich noblemen and distribute their spoils to the poor. Although branded as an outlaw by opposing authorities, Robin Hood and his supporters rationalized his transgressions as justice in the name of serving a greater purpose: helping the impoverished public.

A large body of experimental research on Robin Hood types of deviant decision-making has focused on the conditions under which people are willing to lie or cheat and their justifications for doing so (Klein et al., 2017; Pierce & Balasubramanian, 2015; Shalvi et al., 2015; Wiltermuth et al., 2017). For example, research suggests that individuals may be motivated to engage in dishonest behavior (cheating) to help or hurt another person when the outcome will restore equity or result in a beneficial outcome (Gino & Pierce, 2010). However, to the best of our knowledge, research has not examined these processes in the context of cyber ransoming and the complex cases that may arise. As the threat and impacts of ransomware have grown in recent years, understanding public opinion on this matter will provide insights relevant to national security policy.

Considering this gap in the literature, we use experimental survey data to examine Americans' willingness to support ransoming, and we offer theoretical suggestions regarding possible predictors of such support. Based on the extant literature and the ransoming scenarios that we developed to reflect real-world experiences, we expect three factors to be important in determining support or opposition to cyber ransoming. First, we explore whether the nationality of the attacker influences Americans' support or opposition to the act of cyber ransoming. As we note below, ransomware is often an international issue, with individual and national-level actors and victims. We theorize that, when attacks cross national boundaries, the nationality of the attacker should matter for public support, regardless of the characteristics of the actors (i.e., government vs. civilian). More specifically, we expect that the American public will show more support for ransoming when the actor is American, and the victims are foreign than when the actor is another nation and the victims are American.

Second, because the act of ransoming is a moral issue, Moral Foundations Theory (MFT) may provide insight into the psychological underpinnings of differential responses to it. According to MFT, people have moral intuitions that structure their views about deviance (Graham et al., 2013; Silver & Silver, 2021). These intuitions (or foundations) include those that center on protecting individuals ("individualizing foundations")—having compassion for others and defending civil liberties—and those that locate moral concerns at the group level ("binding foundations")—sacrificing the self for group order, showing obedience to authority, and maintaining normative behaviors (Haidt & Graham, 2007). Of particular relevance to this study, the binding moral foundation of "authority" assesses the extent to which people believe it is morally important to obey authorities (i.e., to accept their government's decisions, whatever they may be). Thus, applied to the case of ransomware, we expect that people who endorse the moral foundation of authority will be particularly supportive of ransoming when the actor is the U.S. government. In contrast, when the actor is an ordinary American (i.e., family members), emphasis on obedience to authority should matter little.

Third and finally, we examine whether the existing political cleavages within the United States affect public support for the use of ransomware against other Americans. That is, are Americans willing to support the use of ransomware against fellow American political opponents, to benefit the political agenda of their in-group? We expect that, given the current political polarization apparent in the United States (which is often described as destructive negative partisanship), members of the public will be most likely to support ransomware use when the actor is from their political in-group (Drutman, 2020; Iyengar et al., 2012; Miller & Conover, 2015).

The impacts of ransomware on Americans

The current reality is that dozens of high-profile ransomware cases have directly affected the lives of millions of Americans and caused the issue of ransomware to emerge as one of the nation's most serious security problems (McMillan, 2021). For example, in 2013, the nation's major retail chain, Target, suffered the largest ever data breach (at the time) when hackers from Ukraine stole the financial data of 40 million customers through the heating, ventilation, and cooling (HVAC) systems of the company (Welburn and Hodgson, 2021). Four years later, in early 2017, four Chinese hackers (members of the Chinese Army) stole the private records of more than 140 million Americans (almost half of the nation) from the credit monitoring company, Equifax. In the same year, the U.S. shipment company FedEx was attacked by WannaCry 2.0 global ransomware, which caused the company to lose more than $300 million in ransom payments and system downtimes (Cook, 2021). The WannaCry outbreak, which was suspected to be sponsored by a terrorist organization supported by the North Korean government, caused even more damage in other countries—in the UK alone, the malware shut down the computer systems in more than 80 National Health Service organizations, blocked access to patient records, and forced hospitals to postpone surgeries and cancel patient appointments (Collier, 2017).

Despite the devastating effects of the past ransomware attacks, many organizations and local governments in the United States have done little to invest in employee training on cybersecurity or pay for new measures to protect their networks from unwanted intrusions and dangerous attacks (Cook, 2021). Hence, a string of cybersecurity incidents seriously impacted the country in 2021, elevating the threat of ransomware to a top national security concern, again. First, the Russian-based group Darkside breached the computer systems of the largest fuel pipeline in the U.S., Colonial Pipeline, and shut down the East Coast's main supply artery for about a week. This resulted in panic buying, gas shortages, and eventually the closure of thousands of gas stations in the South (Fung, 2021; Gatlan, 2021). The company was able to resume its operations only after agreeing to pay a hefty sum of nearly $5 million (Siegel, 2021). Shortly after this incident, one of America's largest meat producers, JBS, was attacked by a group called REvil, slowing down global meat production (Sanger, 2021). REvil stopped its attack after JBS paid the equivalent of $11 million in cryptocurrency as a ransom (McMillan, 2021). More recently, the first case of a ransomware-related death occurred in the United States, when computer outages from a cyberattack led the hospital staff to miss troubling heartbeat signs, resulting in a newborn's death at Springhill Medical Center in Alabama (Poulsen et al., 2021). The navigation company Garmin, IT service provider Kaseya, Microsoft, Apple, T-Mobile, Washington D.C. Metropolitan Police, and New York City Metro are just some other examples of the large organizations that have suffered from ransomware attacks in 2021—along with thousands of schools, county governments, universities, hospitals, and retail businesses (Aslanian, 2021; Brooks, 2021; Shaban, 2021; Winder, 2021).

The risk is now even greater for Americans. As acknowledged in 2012 by then-President Obama, "No country's infrastructure is more dependent on computer systems, and thus more vulnerable to attacks, than that of the United States" (Sanger, 2012). In fact, according to official reports, there were more than 305 million ransomware attacks in the world during the first half of 2021 alone, and approximately 228 million of those attacks occurred in the United States (Burt, 2021). The economic consequences of these attacks have been severe. Compared to 2020, the average ransom paid in the United States during the first half of 2021 increased by 82%, to a record high of almost 600 thousand dollars per incident (Crothers, 2021). To put this into context, the overall cost of ransomware damages in 2021 is estimated to be 20 billion dollars, 60 times the total from 2015, which was around $325 million (Braue, 2021; Theis, 2021). Experts estimate that ransomware costs in the United States are to reach more than $265 billion by 2031 (Braue, 2021).

Public opinion on ransomware

It is clear that ransomware attacks have had significant consequences for Americans, and will continue to do so as criminal groups, foreign nations, terrorists, and other actors have already started to use this tool for monetary gains and/or political advantage (Hugget, 2021; Sanger, 2012). Indeed, a search of the scholarly literature indicates that academic attention to the issue of ransomware accelerated

beginning in 2016. However, the majority of the extant research focused solely on the technical aspects of the problem (e.g., software and hardware security, threat and detection systems, recovery, tracking, and deployment methods) (Connolly & Wall, 2019; Humayun et al., 2021; Maigida et al., 2019; McIntosh et al., 2021; Richardson et al., 2021) and ignored public opinion on this important security matter.

From more general polling data, we do have some evidence that the American public is aware of the threat of cybercrime more generally. For example, although not specific to ransoming, Gallup's 2021 World Affairs Survey found that cyberattacks/cyberterrorism ranks atop a list of 11 perceived potential "critical threats" to the United States. Whereas 82% of respondents saw cyberattacks/cyberterrorism as a critical threat, fewer felt this way about nuclear weapon attacks from North Korea and Iran (77%), international terrorism (72%), the spread of infectious diseases (72%), China's growing economic power (63%), and global warming (58%) (Brenan, 2021). In other words, cyber attacks appear to be salient to the public, despite the lack of research on the extent or sources of attitudes toward ransoming specifically.

The current study

As noted above, the existing public opinion data on cyberattacks suggests that Americans are fearful of this threat and believe that it poses a growing risk to national security. Nevertheless, from Americans' perspective, this may mostly be an international issue, one that usually involves adversaries of the United States (e.g., Russia, China, Iran, and North Korea), attacking the nations' computer networks and stealing U.S. economic information and technology or crippling critical infrastructures for economic gains. In other words, the public likely sees the threat as foreign, especially given the recent major cyberattacks on the nation, such as the Colonial Pipeline incident, which was suspected to be conducted by a Russian group (Rutherford, 2021).

From this perspective, the act of cyber ransoming should be something that Americans generally oppose. However, to date, no studies have explored the American public's opinion on the use of ransoming by the U.S. government for what may be perceived as good deeds. Thus, would the American public approve of the use of cyber-attacks to force foreign governments to comply with its requests by threatening to cause physical destruction in their industrial control systems (e.g., Stuxnet)? Does public opinion differ based on the actor using this technology (one's own country vs. a foreign country)? Furthermore, since Robin Hood use of ransomware is a moral issue, do moral foundations, in particular, endorsement of authority matter in predicting support for ransomware use by governmental authorities? Regarding intra-national attacks, would Americans support political in-groups using ransomware against political out-groups? Through a survey-based experimental study of 1013 Americans, we determine whether the willingness to excuse an act of cyber ransoming varies based on the outcomes that are to be achieved, the identity of the actor, or the moral foundations and political views of the respondent.

Methods

Data to explore this topic come from a nationwide online opt-in survey fielded in 2021 using Amazon's Mechanical Turk (MTurk). This platform allows for "workers" (i.e., respondents) to complete tasks for a small financial incentive—in this case, USD $1.65. Compared to other data collection methods, MTurk and other opt-in online surveys have become common in social science research due to several advantages, including their diversity and nationwide reach, increased attentiveness of respondents, reduction of satisficing and social desirability bias, and elimination of interviewer effects (Anson, 2018; Barnum & Solomon, 2019; Chang & Krosnick, 2009; Hauser & Schwarz, 2016; Weinberg et al., 2014). Notably, articles using data from MTurk have appeared in first-tier journals such as *Criminology* and *Justice Quarterly* (Herman & Pogarsky, 2020; Pickett et al., 2018). In order to increase the quality of the sample, respondents were limited to MTurk workers who had completed over 500 HITs (Human Intelligence Tasks) and had a 95% or higher rating for completing those tasks (Peer et al., 2014). Additionally, the sample was limited to those who were 18 years of age or older and living in the United States.

From the initial 1013 respondents, the sample was reduced to an analytic sample of 1012 based on the listwise deletion of one case for missing values. Compared to data from the 2019 American Community Survey (ASC), this sample underrepresents females and overrepresents married individuals and those with a bachelor's degree or higher, which is typical for MTurk surveys (Thompson & Pickett, 2020; Weinberg et al., 2014). Because of randomization, however, these sample-population differences are not a threat to the internal validity of our experimental findings. Additional descriptive statistics can be found in Table 1.

Experimental procedure

At the beginning of the survey, all respondents were provided with the following definition of ransomware:

> RANSOMWARE is a type of malware that encrypts files on a device (e.g., computer), making the files inaccessible and any system that relies on the files unusable. It then BLOCKS ACCESS to those files until a ransom is paid for decryption. (Sometimes, the files are released publicly if the ransom is not paid.)

To examine whether support for ransomware attacks varies depending on the nationality, authority, and political orientation of the actor, we used a split-ballot experimental design in which respondents were randomly assigned to indicate their level of support or opposition to one of two sets of six scenarios. All items are presented in Table 2. To manipulate nationality and authority, three of the items in each set (items 1, 2, and 3 in Table 2) described similar actions but varied the actors and targets across the experimental groups, with one group receiving scenarios with American actors and foreign targets (group A, $N = 505$) and

Table 1 Sample descriptives ($N = 1012$)

	Mean (SD)/%	Range	Alpha	Factor loadings
Moderators				
Authority	3.48 (.95)	1–5	.839	.778-.844
Republican	26.80			
Democrat	53.30			
Independent/other	19.90			
Conservative views	2.84 (1.27)	1–5		
Sociodemographic controls				
Age	38.70 (10.89)	18–79	–	–
Female	34.29	0–1	–	–
White	72.83	0–1	–	–
Married	65.81	0–1	–	–
Education	4.83 (1.14)	1–7	–	–
Income	4.27 (1.43)	1–7	–	–
Religious	78.36	0–1	–	–
Ransomware knowledge	3.37	1–5	–	–
Online scam victim in household	45.8	0–1	–	–
Time spent online	4.31 (1.25)	0–6	–	–
Care/Harm	3.79 (.74)	1–5	.670	.643-.773

$^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$

the other group receiving scenarios with foreign actors and U.S. targets (group B, $N = 507$). Out of those three items in each group, two described scenarios in which the actor was the national government (items 1 and 2) and one described a scenario where the actor was a private citizen (item 3).

For the government actor items, experimental group A was presented with the U.S. cyber attacking a foreign country to (1) force the release of American prisoners and (2) stop aid to terrorist organizations. Experimental group B was presented with two parallel scenarios with the actor being a "foreign government" and the target being the "United States" (see Table 2). Respondents were then asked to report their level of support or opposition to the statements provided (in random order), using a five-point Likert scale ranging from "Strongly Oppose" to "Strongly Support."

We merged responses to the parallel items across groups and then averaged responses to the two merged items to create the *Government Use* of ransomware measure. We use a dummy variable in the analyses to examine the impact of nationality (1 = U.S. actors [group A], 0 = foreign actors [group B]).

To examine the role of nationality when the actors are civilians, we utilized a *Civilian Use* of ransomware scenario, to which respondents indicated support using the same Likert scale described above (1 = strongly oppose to 5 = strongly support). Group A was presented with American citizens hiring hackers to threaten a foreign country for the release of their family members, and the other group responded to foreign civilians hiring hackers to threaten the United States. As with the

Table 2 Survey items (percentages reported)

Items	Total oppose	Neither support nor oppose	Total support
Group A ($n = 505$)			
1. The U.S. hacks a foreign country's electrical grid and demands that the country release American prisoners or suffer a shutdown of their grid	44.1	21.9	34.0
2. The U.S. hacks a foreign country's electrical grid and demands that the country stop aiding terrorist organizations or suffer a shutdown of their electrical grid	43.1	19.6	37.3
3. Family members of Americans being held in another country's prison hire hackers that threaten to collapse its government's computer systems unless the Americans are released	41.3	25.1	33.5
4. Human rights activists hack Syria's computers and threatening to undermine the country's banking system unless the government stops bombing raids against opponents	40.4	26.3	33.3
5. Health activists hack the computers of a large pharmaceutical company and threaten to disrupt their sales unless they reduce the cost of expensive life-saving drugs	45.9	22.8	31.3
6. Democratic advocates hack the Republican Party's headquarters and threaten to corrupt their mailing lists of donors unless they publicly announce that Donald Trump has lied about winning the 2020 presidential election	55.6	17.6	26.7
Group B ($n = 507$)			
1. A foreign country hacks the U. S. electrical grid and demand that the U.S. release foreigners being held in prison or suffer a shutdown of the grid	59.6	17.9	22.5
2. A foreign country hacks the U. S. electrical grid and demands that the U.S. stop counterterrorism operations overseas or suffer a shutdown of their electrical grid	59.2	17.0	23.8
3. Family members of foreigners being held in American prisons hire hackers to threaten the U. S. with the collapse of government computer systems unless they are released	59.1	19.3	21.5
4. Human rights activists hack Syria's computers and threaten to undermine the country's banking system unless the government stops bombing raids against opponents	41.0	25.0	34
5. Health activists hack the computers of a large pharmaceutical company and threaten to disrupt their sales unless they reduce the cost of expensive life-saving drugs	45.5	20.0	34.5
6. Republican advocates hack the Democratic Party's headquarters and threaten to corrupt their mailing lists of donors unless they publicly announce that there was voter fraud in the 2020 presidential election	61.4	15.6	23.1

government actor items, we merged responses across groups to produce one *Civilian Use* variable and include the actor nationality dummy variable described above in the analyses.

Beyond nationality, we also sought to determine whether in-group identification matters within nations—that is, when Americans cyberattack other Americans. To examine this, we used the social identity of political affiliation and presented each group with one item that described political actors within the United States targeting the political opponent. Group A reported their support or opposition to Democrats cyber attacking Republicans, and group B responded to Republicans cyber attacking Democrats (see Table 2). We merged responses to these two items across the groups to create the *Political Opponent Use* measure and created a dummy variable (1 = Democratic actors, 0 = Republican actors) to examine the influence of political group identification.

Finally, as a check on the success of the randomization, we included two items that were worded identically across the experimental groups. In each group, the items asked about (1) human rights activists' use of ransomware to end bombings in Syria and (2) health activists' use of ransomware to reduce the cost of life-saving drugs. We examine whether the experimental groups held otherwise similar attitudes when asked identical items. Thus, a comparison of responses to these two items will provide a test of whether respondents in the two experimental groups differed attitudinally even when asked the same questions (selection bias). If they did not, then we can be more confident that the groups were attitudinally similar, and thus that any group differences observed in responses to the other, experimentally varied question stems reflect the causal effect of question-wording.

Moderators

As discussed above, we expect that the effects of the experimental conditions (U.S. actors versus foreign actors and Democratic actors versus Republican actors) on support for ransomware will be moderated by the characteristics of the respondents. In the case of governmental use of ransomware, we predict that respondents' endorsement of the moral foundation of authority, a binding foundation according to Graham et al. (2009), will interact with nationality to predict ransomware support. That is, persons who emphasize obedience to authority should be particularly supportive of the actions of their own governmental leaders. To measure authority, we use Graham et al.'s (2020) updated version of the moral foundations *Authority* subscale. Respondents were asked to rate their level of agreement to four items that tap into their emphasis on obedience and duty (e.g., respect for authority is something all children need to learn) on a five-point Likert scale, ranging from "Strongly Disagree" to "Strongly Agree." The Cronbach's alpha for *Authority* is 0.839, with factor loadings between 0.778 and 0.884.

For the case of the intra-governmental political use of ransomware, we predict that support for political advocates' use of ransomware will depend on both the party of the actor and the political views of the respondents. We use two measures of respondents' political leaning, conservative political views and political party, both of which are standard in the political science literature (see, e.g., Kinder & Kalmoe,

2017). For *Conservative Views*, respondents were asked how they would describe their political viewpoint, with response options ranging from (1 = very liberal to 5 = very conservative). *Political Party* is measured with a set of dummy variables to indicate Democrat, Republican, or Independent.[1]

Sociodemographic controls

To increase explanatory power and improve the precision of the estimates, additional sociodemographic controls were included in the multivariate analyses. These variables include: *age* (in years), sex (1 = *female*, 0 = male), race (1 = *White*, 0 = non-White), marital status (1 = *married*, 0 = other), education (measured ordinally from 1 = *less than a high school degree*, to 7 = *doctoral degree*), 2020 household income (measured ordinally from 1 = *0-$9999* to 7 = *$100,000+*), and religious affiliation (1 = *Religious* (Protestant, Roman Catholic, Mormon, Eastern or Greek Orthodox, Jewish, Muslim, Buddhist, Hindu, Something else), 0 = not religious (Atheist, Agnostic, nothing in particular)).

Furthermore, to control for baseline levels of knowledge about ransomware, we include the variable *Ransomware Knowledge* in all models. *Ransomware Knowledge* was assessed by the first question in the survey, which asked, "How much do you know about ransomware?," with response options ranging from 1 (not much) to 5 (a great deal). In addition, to account for the impact of online victimization, respondents were asked to report whether anyone in their household had been the victim of an online scam in the last 5 years (1 = *Yes*, 0 = No). Likewise, to control for internet exposure, which may influence the actual or perceived risk of victimization, respondents were asked to report how much time they spent online each day, using a six-point scale ranging from "None" to "More than 6 h." (Detailed sample frequencies for these items are provided in Table 6.)[2]

Finally, we also control for the MFT individualizing foundation, *Care/Harm*. The *Care/Harm* subscale seeks to capture respondents' emphasis on protecting individuals, empathy, compassion, altruism, and prosocial behavior (e.g., it can never be right to kill a human being; Graham et al., 2009). The Cronbach's alpha for *Care/Harm* is 0.670, with factor loadings between 0.643 and 0.773. As there are no existing empirical examinations of the role of moral foundations in predicting support for the use of ransomware, the inclusion of *Care/Harm* provides us with a comparison between the influence of binding and individualizing foundations (Graham et al., 2009). Furthermore, as an initial investigation of public opinion on ransomware use, the examination of the associations between these control variables and ransomware support is an additional contribution of our analyses. (Please see Table 7 for a table of all interaction effects without the control variables.)

[1] Respondents who reported "not sure" or "other" for political party were coded as independents.

[2] As an additional check on the influence of knowledge on our findings, we repeated all analyses with sample split by knowledge ("some" or more vs. "a little" and "not much"). We found no substantive difference in the patterns of results by knowledge group. These results are available upon request.

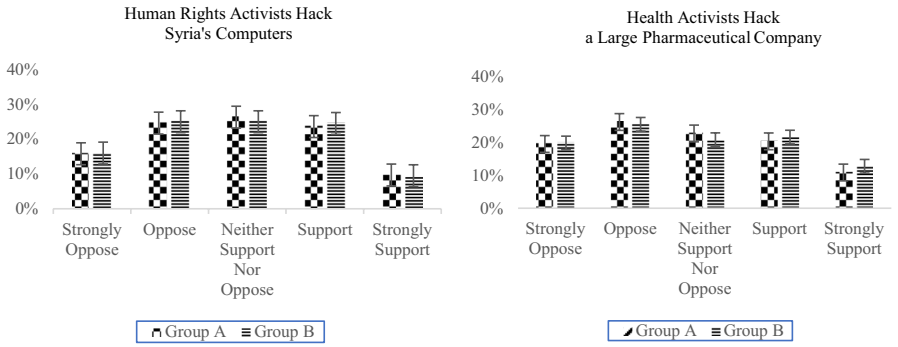

Fig. 1 Percentage comparison by experimental group for the "test" items-the identical survey items. Note: Figures show support for ransomware use by condition with 95% confidence interval

Analytic plan

We begin our analysis by descriptively assessing participants' support for the use of ransomware in each Robin Hood scenario within each experimental group. Next, we use ordinary least squares regression (OLS) to predict our three dependent variables: support for government use, support for civilian use, and support for political opponent use of ransomware. We examine three models for each variable. First, we assess the effect of the experimental manipulation of the ransoming actor (i.e., experimental group A versus B), net of the control variables. Second, we add our measures of authority (for government and civilian use) or rightward views (for political opponent use) to the model. Finally, we add the interaction term to determine whether authority (in the case of government versus civilian use) and political views (in the case of political opponent use) moderate the relationship between the ransoming actor (U.S. versus foreign; Democrat versus Republican) and support for ransomware. We examined the models for multicollinearity and found no VIFs above the recommended threshold (Belsley et al., 2005).

Results

As a check on our randomization, we first compare responses to the identical, non-manipulated items in each group. As shown in Fig. 1, levels of opposition and support for ransomware use are nearly identical in each response category across the two experimental groups. In addition, the mean support for ransomware does not differ significantly across groups for either item (for human rights activists: group A $\bar{x}=3.13$, $s=1.22$; group B $\bar{x}=3.14$, $s=1.27$; $t=0.045$, $p<0.964$ and for health activists: group A $\bar{x}$ 3.23, $s=1.28$; group B $\bar{x}=3.17$, $s=1.31$; $t=0.883$, $p<0.377$). The lack of significant differences by group on the identically worded items indicates that the experimental groups responded similarly when asked the same questions, denoting attitudinal balance. As such, this suggests that any differences found between the remaining manipulated items are a result of the experimental

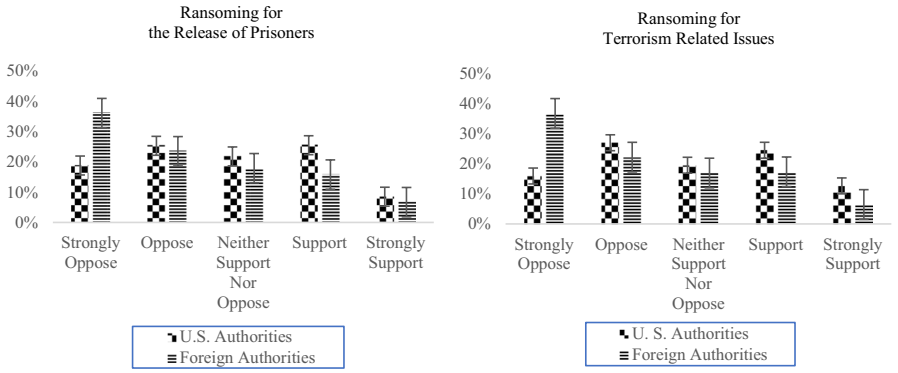

Fig. 2 Percentage of support for the U.S. vs. Foreign Government use of ransoming. Note: Figures show support for ransomware use by condition with 95% confidence intervals

conditions (i.e., ransoming actors) viewed by respondents based on the split ballot methodology.

Next, we evaluate levels of support for the use of ransomware within our sample. Along with each ransomware survey item, Table 2 reports the percentages of the sample that oppose (including "strongly oppose" and "oppose"), neither support nor oppose, and support (including "strongly support" and "support") the use of ransomware. Overall, a complex picture emerges. There is a clear sentiment against the use of ransomware in each scenario, even to achieve possibly desired ends. Opposition to the use of ransomware in general ranges from 41 to 61%, with a large portion of the sample, 15 to 26%, indicating ambivalence on the matter. Thus, while there is substantial opposition to the use of ransomware among our respondents, the large "neither support nor oppose" response illustrates that a substantial minority of the sample does not reject the use of ransomware for "Robin Hood" purposes. In comparison, support for the use of ransomware ranges from 22 to 37%.

Furthermore, looking from group A (which includes U.S. actors in international scenarios for items 1–3) to group B (which includes foreign actors in international scenarios for the same items), there is a pattern of stronger opposition in group B. In fact, for items 1–3 in group A, more than half of the sample does not reject the use of Robin Hood ransomware in international situations with American actors.

We present these patterns in greater detail in Figs. 2 and 3. Figure 2 displays responses to the use of ransomware by governmental actors, U.S. and foreign. While most of the sample opposed the use of ransomware, consistent with our expectations, participants showed greater support for ransomware use when the actor is their own nation, and the victim is foreign. In particular, participants report greater support when the actor is the U.S. government (34% versus 22.5% for the release of prisoners and 37.3% versus 23.8% for terrorism-related issues), and more participants "oppose" or "strongly oppose" ransomware use when the actor is a foreign government than when the actor is the United States (59.6% versus 44.1% for release of prisoners and 59.2% versus 43.1% for terrorism-related issues). This is notable given that the attack behavior is the same and only the actor varies across

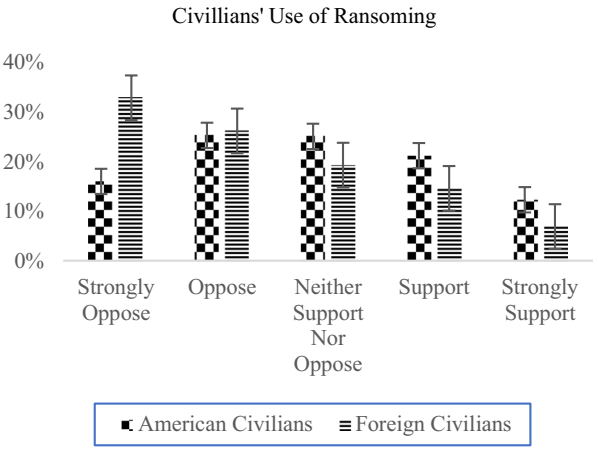

Fig. 3 Percentage support for the use of ransoming by "Civilians". Note: Figures show support for ransomware use by condition with 95% confidence intervals

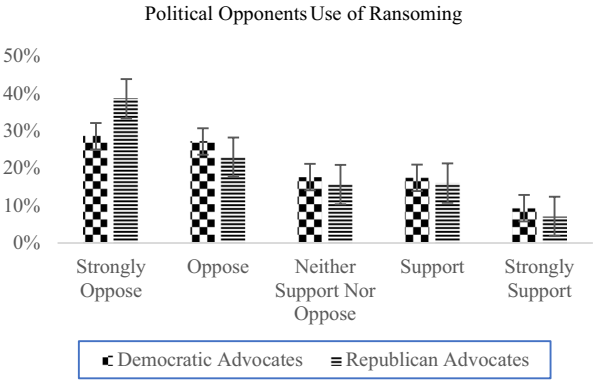

Fig. 4 Percentage support for the use of ransoming by political opponent. Note: Figures show support for ransomware use by condition with 95% confidence intervals

scenarios—people are more approving of the same behavior when done by their own country. These results are suggestive of a Robin Hood effect—a solid minority of the respondents appear to endorse cyber-deviance to achieve desired ends—winning the release of international prisoners and stopping aid to terrorists—especially when the actor is the United States.

Figure 3 illustrates that this Robin Hood effect extends to non-governmental (i.e., civilian) actors. As in the case of governmental actors, participants show more support for American citizens' use of ransomware to release family members imprisoned in foreign countries than the reverse, with 33.5% in support of U.S. citizens' ransoming (versus 21.5% for foreign actors). Also, participants are most opposed to civilians ransoming when the actors are foreign (59.1%) than when the actors are American (41.3%). Once again, because the ransoming action is the same and only the nationality of the civilian attacker varied between the groups, this pattern suggests that people are more accepting of deviant behavior by in-groups.

Finally, as indicated in Fig. 4, the use of ransomware by Americans to target other Americans for political reasons is opposed by a majority of the sample. We do see

stronger opposition, however, when the actors are Republicans compared to Democrats (61.4% oppose or strongly oppose Republican actors while 55.6% oppose or strongly oppose Democratic actors), which is likely due to a greater proportion of Democrats in our sample (53%) compared to Republicans (27%).

Given these findings, we move on to the regression analysis. Table 2 reports the OLS regressions of governmental use of ransomware and families' use of ransomware. Here, we expect that people will be more supportive of Robin Hood use of ransomware when the actor and beneficiaries are in-group members (i.e., Americans), and the earlier findings were consistent with this expectation. We also expect that participants who believe that it is morally important to obey authorities should be more likely to support their government's actions, in this case ransoming. Thus, authority should moderate the relationship between actor nationality and governmental use of ransomware. To test these predictions, we present our analyses in three steps. For both dependent variables, an initial model (models 1 and 4, respectively), estimates the effects of respondents viewing U.S. attackers (coded as 1) as opposed to foreign attackers (coded as 0) on support for ransomware, while controlling for sociodemographic characteristics. Then, in the second model for each dependent variable (models 2 and 5, respectively), we include the authority moral foundation measure. In the final model for each outcome (models 3 and 6, respectively), we include the interaction term.

As shown in Table 3, across all models, there is a consistent effect of nationality. Participants are significantly more likely to support the use of ransomware when the actor is American—either government or private citizen (Cohen's $d = 0.437$ for government use, 0.407 for civilian use). Furthermore, models 2 and 5 reveal that, regardless of condition, respondents with stronger moral foundations in authority are more supportive of the use of ransomware ($b = 0.189$, $p < 0.001$ and $b = 0.248$, $p < 0.001$, respectively). Thus, persons who emphasize respect for authority tend to be more supportive of the use of ransomware by both governmental and non-governmental actors when the outcome can benefit others. Likewise, and unexpectedly, the moral foundation of care/harm is also positively associated with ransomware support ($b = 0.173$, $p < 0.01$ and $b = 0.182$, $p < 0.01$). Taken together, these results suggest that persons who emphasize moral foundations, whether they be "binding" or "individualizing," show heightened support the use of ransomware to benefit others, although the reasons (mediating mechanisms) likely differ.

Furthermore, although we expected authority to moderate the relationship between actor nationality and support for government use of ransomware, model 3 in Table 3 shows that this is not the case. Persons with strong moral foundations in authority do not show elevated levels of support for their own government's use of ransomware ($b = -0.038$, $p = 0.598$). Also, as a comparison, model 6 in Table 3 also shows a non-significant interaction term ($b = -0.068$, $p = 0.383$). Again, these findings illustrate that the relationship between moral foundations and support for ransomware attacks does not vary by the nationality of the actor, which is inconsistent with our expectations.

Of the control variables, models 2 and 5 of Table 2 indicate that age is negatively associated with support for ransomware use in both cases, government use and civilian use ($b = -0.007$, $p < 0.05$ and $b = -0.011$, $p < 0.01$, respectively). In addition, experiencing previous online victimization corresponds to higher levels of support

Table 3 OLS models predicting support for ransomware, by attacker ($N = 1012$)

	Government use						Civilian use					
	Model 1		Model 2		Model 3		Model 4		Model 5		Model 6	
	b	*SE*	*b*	*SE*	*b*	*SE*	*b*	*SE*	*b*	*SE*	*b*	*SE*
Experimental manipulation												
US actors	**.524*** **	.069	**.509*** **	.068	**.641***	.258	**.534*** **	.075	**.520*** **	.073	**.756****	.280
Theoretical variable												
Authority	–	–	**.189*** **	.047	**.206*** **	.057	–	–	**.248*** **	.051	**.279*** **	.062
Interactions												
US Actors × authority	–	–	–	–	-.038	.071	–	–	–	–	-.068	.078
Sociodemographic controls												
Age	−.005	.003	**−.007***	.003	**−.007***	.003	**−.010****	.004	**−.011****	.003	**−.011****	.003
Female	.092	.074	.056	.072	.055	.072	.125	.080	.081	.078	.078	.079
White	−.021	.078	.023	.077	.022	.077	−.012	.085	.040	.083	.038	.083
Married	**.180***	.087	.102	.087	.101	.087	**.239****	.095	.127	.094	.125	.094
Education	−.021	.034	.002	.034	.002	.034	.014	.037	.035	.037	.035	.037
Income	−.012	.026	−.008	.025	−.008	.025	−.012	.028	−.006	.028	−.006	.028
Religious	**.306****	.100	.170	.104	.171	.104	.095	.109	−.084	.113	−.082	.113
Ransomware knowledge	**.067***	.071	.030	.033	.030	.033	**.083****	.036	.038	.036	.038	.036
Online victim	**.269*** **	.077	**.241****	.076	**.240****	.076	**.293*** **	.084	**.256****	.082	**.255****	.082
Time spent online	**−.183*** **	.032	**−.178*** **	.031	**−.178*** **	.031	**−.173*** **	.034	**−.167*** **	.034	**−.166*** **	.034
Care/harm	–	-	**.173****	.053	**.173****	.053	-	-	**.182****	.057	**.183*** **	.057
Conservative views	–	–	.031	.030	.032	.030	–	–	.032	.042	.034	.042
Democrat	–	–	-.037	.087	-.036	.087	–	–	.068	.094	.070	.094
Independent	–	–	.093	.107	.092	.107	–	–	.038	.116	.036	.116
Adjusted R^2	.170		.208		.207		.142		.188		.187	

Republican is the reference category for political party; *$p < .05$, **$p < .01$, ***$p < .001$

for ransomware use in both cases ($b = 0.241$. $p < 0.01$ and $b = 0.256$, $p < 0.01$) while greater time spent online is associated with decreased levels of support for both government and civilian use of ransomware ($b = -0.178$, $p < 0.001$ and $b = -0.167$, $p < 0.001$).

Our final set of analyses examines the case of ransomware use in intra-governmental disputes. Recall, the political scenarios involved political actors hacking a political opponent's headquarters for concessions related to the 2020 presidential election results. In this case, while the experimental condition (Democratic versus Republican actors) may matter overall, its effect on ransomware support should be dependent on the respondent's political orientation. For example, people with conservative views should be most supportive of Republican actors targeting the Democratic headquarters. Following our previous analysis, Table 4 presents the OLS regression of political opponent use of ransomware in three steps. First, we examine the effect of the experimental condition (1 = *Democratic actors*), net of the control variables. Second, we add our key independent variables, conservative views and political party, to the model. Finally, we include the interaction terms.

Models 1 through 3 of Table 4 show a consistent effect of actor party on ransomware support. Even while controlling for respondents' political views and political party, people are more supportive of Democratic advocates hacking the Republican party's headquarters to force them to announce that Donald Trump has lied about winning the 2020 presidential election than of Republican advocates forcing Democrats to announce that there was voter fraud in the 2020 election. It may be the case that a greater proportion of the public believes that former President Trump lied about winning the election than believes that there was voter fraud. Furthermore, while *Conservative Views* does not exert a main effect on support for political opponent use of ransomware, model 2 of Table 4 reveals that Democrats report greater support of political uses of ransomware than Republicans ($b = 0.224$, $p < 0.05$). Model 2 also shows a pattern of associations among the control variables that is similar to that reported in Table 3, with age, ransomware knowledge, prior internet victimization, and authority being significant predictors of support for ransomware use. In addition, persons who are married and those whit higher levels of education are more supportive of a political opponent's use of ransomware ($b = 0.277$, $p < 0.01$ and $b = 0.088$, $p < 0.05$, respectively), while income is negatively associated with ransomware support ($b = -0.056$, $p < 0.05$).

Turning to model 3 of Table 4, as expected, *Conservative Political Views* does moderate the effect of actor identity on ransomware support. Although there is greater support for the Democratic advocates' use of ransomware in general, holding conservative political views tempers this support ($b = -0.149$, $p < 0.05$). The interactions between actor and political party, however, are not significant.[3]

[3] Because conservative political ideology is correlated with Republican party identification ($r = .365$, $p < .001$), we ran additional analyses with a variable, Rightward Political Views, which we constructed by standardizing and combining self-reported political party affiliation and political ideology. Analyses with this variable also showed a significant negative interaction between Rightward Political Views and Democratic actor ($b = -.280$, $p < .01$).

Table 4 OLS models predicting support for political ransomware Use ($n = 1012$)

	Political Opponent Use					
	Model 1		Model 2		Model 3	
	b	*SE*	*b*	*SE*	*b*	*SE*
Experimental manipulation						
Democratic actors	**.241*****	.073	**.229*****	.071	.164	.145
Theoretical variables						
Conservative views	–	–	.044	.032	**.121****	.043
Democrat	–	–	**.224***	.091	.127	.126
Independent	–	–	.113	.112	.205	.157
Interactions						
Democratic actors × Conservative views	–	–	–	–	**−.149***	.060
Democratic actors × Democrat	–	–	–	–	.181	.182
Democratic actors × Independent	–	–	–	–	−.162	.215
Sociodemographic controls						
Age	**−.011*****	.003	**−.012*****	.003	**−.012*****	.003
Female	.044	.077	.017	.076	.002	.076
White	.106	.082	.138	.081	.127	.081
Married	**.376*****	.092	**.277****	.092	**.283****	.091
Education	**.071***	.036	**.088***	.036	**.088***	.036
Income	**−.062***	.027	**−.056***	.028	**−.055***	.027
Religious	**.368*****	.105	.190	.109	.200	.109
Ransomware knowledge	**.104****	.035	**.072***	.035	.068	.035
Online scam victim in household	**.402*****	.081	**.368*****	.080	**.364*****	.080
Time spent online	**−.216*****	.033	**−.206*****	.033	**−.201*****	.033
Care/harm	**–**	–	.044	.056	.053	.055
Authority	–	–	**.249*****	.049	**.248*****	.049
Adjusted R^2	.241		.269		.276	

Republican is the reference category for political party; *$p < .05$, **$p < .01$, ***$p < .001$

To examine the support for the political use of ransomware by political views, we disaggregated the sample by *Conservative Views* and ran separate OLS regressions for those with liberal views ("Very Liberal" or "Liberal) and those with conservative views ("Very Conservative" or Conservative"). As shown in model 1 of Table 5, among those with liberal political views, support for political opponents' use of ransomware is significantly higher when the actor is a Democrat compared to Republican ($b = 0.492$, $p < 0.001$). In contrast, the political affiliation of the ransoming actor is not a significant predictor of support for ransomware use among conservative respondents ($b = -0.019$, $p = 0.948$). Paternoster et al.'s (1998) slope-difference test indicates that the difference between the Democratic actor coefficients from models 1 and 3 is statistically significant ($z = 3.15$, $p < 0.000$). Thus, those with liberal views, in particular, are significantly more supportive of Democratic actors' use of ransomware to coerce Republicans into admitting that Donald Trump lied

about winning the election than of Republican actors' use of ransomware to force Democrats to admit voter fraud.

However, we find a non-significant coefficient for actor affiliation among those with conservative views. This lack of effect of actor party among those with stronger conservative views across conditions may indicate an ambivalence on their part in supporting Republicans advocating for admittance of voter fraud. It may be the case that more conservative persons are more generally opposed to the use of ransomware than those on the left. Or, our results may be a function of the outcome of ransoming—most persons holding liberal views may believe that Donald Trump lied about the election results, but many persons holding conservative views may disagree with the claim of voter fraud in the 2020 presidential election.

Discussion

The issue of ransomware has emerged as one of the most serious threats to the national security of the United States in recent years (McMillan, 2021). Some of these large-scale attacks conducted against government agencies and corporations (including the theft of cutting-edge technology such as the intellectual property on Covid-19 vaccine development from the U.S. companies and universities) were linked to nation-state actors, namely Russia and China (Myre, 2021). In fact, as we were writing this manuscript, President Biden warned Russian President Vladimir Putin that there would be "real consequences for Russia" should they commit future attacks on American soil (McGuire, 2021; Miller, 2022). He further commented that "if we end up in a war—a real shooting war with a major power—it's going to be as a consequence of a cyber-attack" (Bose, 2021).

Thus, as nation states have become increasingly bold in their use of cyber capabilities against the United States, a serious debate has begun around the issue of developing an official retaliatory policy concerning cyberattacks. The question of what kind of retaliation would be appropriate is a difficult one, though. Experts and politicians question whether the United States is ready to escalate counterattacks against its adversaries' infrastructure, potentially causing injuries and death. Some argue that a retaliatory attack by the United States can cause more damage than good, as any counterattack may lead to a dangerous standoff between the country and other major nuclear powers (Collinson, 2021). Others, on the other hand, favor the use of aggressive military and cyber capabilities. For example, Congressman Michael Waltz stated, "An attack on U.S. oil infrastructure or food supply is an attack, whether it's from a plane dropping a bomb or a cyberattack" (Nakashima, 2021).

Given the recent developments and the pressing threat of cyberattacks, understanding the factors that influence public opinion and thus generate policy support for the use of ransomware is critical. Do American support the use of ransomware by the United States, suggesting a belief that the ends justify the means? That is, do they support the U.S. government acting like Robin Hood, using ransomware to address international matters? Or is this support limited, regardless of the actor

Table 5 OLS models predicting support for political ransomware use, by political views

	Political opponent use			
	Liberal views ($N=497$)		Conservative views ($N=332$)	
	Model 1		Model 2	
	b	*SE*	*b*	*SE*
Experimental manipulation				
Democratic actors	**.492*** **	.098	-.019	.129
Sociodemographic controls				
Age	−.009	.005	**−.014***	.006
Female	−.137	.106	.175	.134
White	**.335** **	.113	−.032	.145
Married	.192	.126	.332	.177
Education	.060	.049	**.179***	.069
Income	.004	.036	−.109	.050
Religious	.226	.149	.098	.239
Ransomware knowledge	.039	.049	.120	.064
Online scam victim in household	**.305** **	.112	**.301***	.139
Time spent online	**−.172*** **	.047	**−.254*** **	.057
Care/harm	−.110	.080	**.264***	.101
Authority	**.329*** **	.064	.122	.110
Adjusted R^2	.324		.269	

Republican is the reference category for political party; *$p<.05$, **$p<.01$, ***$p<.001$

wielding the ransomware? We initiated an experimental examination of public support for ransomware use.

As we discussed above, the previous ransomware attacks on the United States have illustrated the danger of these attacks to the American public, as they have caused serious disruption and even death. Thus, we expect that many Americans would oppose these deviant acts of cyber ransoming. However, the use of ransomware may be framed in a positive way—as a means to provide a benefit to others, and the literature on the Robin Hood effect in decision-making suggests that people may support deviant behavior when it will provide benefits to in-group members. Thus, in our effort to understand support for ransomware, we focus specifically on the Robin Hood effect, in which actions are justified by their potential benefits to others. Based on the limited existing research on the topic, we identified three key features of a ransomware scenario to vary: in international cases, the (1) nationality of the actor (U.S. vs. foreign) and (2) authority of the actor (government vs. civilian), and, in domestic cases (3) the political affiliation of the actor (Democrat vs. Republican). Our analyses generated four key insights.

First, support for the use of ransomware is a complex issue that varies by actor and beneficiary in the scenario. Overall, even when the United States is victimizing

a foreign entity, more than 4 in 10 do not support its use. Thus, even when the ends are possibly seen as positive or even noble, the use of illegal means to blackmail even an opponent or bad actor into changing their behavior is not endorsed by the majority of the sample. This may be because ransomware likely has a negative connotation generally, which may result in it being seen as a morally questionable way to achieve goals. Or, Americans in our sample may see the use of ransomware by anyone as simply poor public/international policy (i.e., they may prefer more diplomatic responses to threats than the creation of/escalating cyber-arms race). However, more than a third of the sample did indicate support for the use of ransomware by U.S. actors to do good—clearly demonstrating a Robin Hood effect. Most instructive, another fifth to a fourth of the sample is unsure—saying that they neither support nor oppose its use. Depending on the circumstances, it is likely that Americans might split almost evenly about using ransomware. Support might vary, for example, by who "gets hurt" by the action—foreign evil-doers or "innocents" living in another country. The reaction might be similar to the use of other methods to serve U.S. interests—such as drone or missile attacks—that target enemies of the United States but risk having "collateral damage" to civilians.

Second, consistent with the Robin Hood decision-making research that shows people tend to support morally questionable actions when they or members of their in-group may benefit, the nationality of the actor is a key predictor of support for the use of ransomware. People are more supportive of ransomware use when the actors are from their own country, and the outcomes benefit their in-group members. This effect holds for both government actors and civilian actors. Thus, we see national in-group support for cyber-Robin Hood actions. This finding is particularly important, as the notable recent cyberattacks have been international in origin. Should the U.S. engage in counter cyberattacks against Russia, as the Biden administration has warned, our experimental results suggest the U.S. government may generate support among a sizeable minority of the American public if the attacks are framed to emphasize the benefits that they may bring to in-group members (Americans).

Third, contrary to our expectations, support of ransomware use by U.S. government officials did not depend on participants' endorsement of the moral foundation of authority. Rather, both of the moral foundations examined—authority and harm/care—exhibited additive, positive associations with support for ransomware use by both governmental actors and civilian actors. The more strongly participants endorsed these moral foundations, the more supportive they were of the Robin Hood use of ransomware, regardless of the actor type. Indeed, subgroup analyses show that within both experimental groups (U.S. actors and foreign actors), endorsement of authority and harm/care are positively associated with support for ransomware use (for U.S. actors $r=0.291$, $p<0.000$ for authority, and $r=0.162$, $p<0.000$ for harm/care and for foreign actors $r=0.350$, $p<0.000$ for authority, and $r=0.161$, $p<0.000$ for harm/care). The outcome of a potential benefit to others, regardless of who those "others" are, appears to resonate with individuals who feel strongly about moral concerns—whether they be binding (i.e., authority) or individualizing (i.e., harm/care).

Fourth, our analysis of an intragroup (within the United States) attack on political opponents revealed that political views matter for support of ransomware use. While

participants were most supportive of ransomware use by Democratic actors, this support depended on participants' political affiliation. Support for ransomware use by Democratic actors was lowered by holding conservative political views. More specifically, our split sample analysis revealed in-group support among those with liberal views but no effect of actor party on ransomware support among conservative participants. We expect that this finding is due to the goal of the ransoming in this specific scenario—to force Democrats to publicly announce that there was voter fraud in the 2020 presidential election. This particular outcome may test the limit of political party support. Indeed, a poll conducted by Monmouth University indicated that 40% of Republicans believe that Donald Trump lied about his 2020 election loss (Greenwood, 2021). Similarly, another national poll conducted by Reuters/Ipsos also indicated that while more than half of Republicans believe that the presidential election was stolen from Donald Trump, 40% of Republicans believe that Trump attempted to overthrow valid election results (Durkee, 2020). Thus, there is a substantial division among Republicans on the results of the 2020 presidential election. Our findings suggest that individuals may need to support both their party and the goal of the attack. Future research might examine political opponent attacks with less contentious outcomes to determine whether those with rightward views simply oppose the use of ransomware or if it is the outcome (admitting voter fraud) that they just do not support.

Overall, while our study provides an initial experimental examination of support for the use of ransomware, our findings must be interpreted as responses to hypothetical scenarios. Although we designed realistic scenarios, particularly with the growing threat of ransomware, we cannot confirm whether Americans would have similar responses to actual cases of cyber ransoming. That said, there is evidence that responses to hypothetical vignettes mirror real-world behavior, at least in the case of voting (Hainmueller et al., 2015). Also of note, we provided all respondents with a definition of ransomware at the start of the survey, and this definition may have influenced responses in a way that persons may not experience with an actual (real-world) case of ransoming. However, responses to our question about ransomware knowledge that preceded the definition in the survey revealed that only 4.3% of the sample reported "not much" knowledge of ransomware. Thus, we believe our sample already had some understanding of ransomware, and this was expected given the recent media attention in the United States to major cyberattacks (e.g., Colonial Pipeline, JBS).

Furthermore, our analyses were limited to the five different ransoming scenarios we presented, and, building on existing theory, we focused on three key predictors. In particular, the outcomes we examined were all of the "Robin Hood" type. Would we still see the effects of support by nationality if the outcomes were not so clearly positive? For example, would Americans support the U.S. government's use of its cyber capabilities solely to gain military power and economic benefits (as in the case of Russia and China)? Or, would the public agree with retaliatory cyberattacks against Russia's oil and gas pipelines, knowing that it would cause civilian deaths and suffering? Given the worldwide expansion of cyberattacking abilities, the need for international and national security policy concerning cyberattacks and ransomware use is clear. Understanding the drivers of support for various uses of cyber threats is thus critical, as support is essential for policy development and implementation.

Appendix

Table 6 Sample background knowledge of ransomware and internet usage

Variables	Percent (%)
Ransomware knowledge	
Not much	4.3
A little	18.7
Some	30.3
Quite a bit	29.5
A great deal	17.2
Time spent online each day	
None	.3
Less than 30 min	6.4
30 min up to 1 h	22.5
Between 1 and 3 h	26.5
More than 3 h but less than 6 h	21.2
More than 6 h	23.1

Table 7 Interactions without control variables

Variables	DV = government use		DV = civilian use		DV = political opponent use	
	Model 1		Model 2		Model 3	
	b	SE	*b*	SE	*b*	SE
Interactions						
US actors × authority	− .060	.074	− .091	.080	—	—
Democratic actors × Conservative views	—	—	—	—	**− .147***	.069
Democratic actors × Democrat	—	—	—	—	.274	.200
Democratic actors × Independent	—	—	—	—	− .193	.247
Moderators						
US actors	**.696****	.267	**.812****	.288	—	—
Authority	**.427*****	.050	**.458*****	.054	—	—
Democratic actors	—	—	—	—	.513	.295
Conservative views	—	—	—	—	**.191*****	.048
Democrat	—	—	—	—	− .028	.144
Independent	—	—	—	—	− .209	.177
Adjusted *R*-squared	.143		.133		.038	

Republican is the reference category for political party; *$p < .05$; **$p < .01$; ***$p < .001$ (two–tailed) $N = 1012$

Data availability The dataset generated during and/or analyzed during the current study is not publicly available due to other research studies in progress, but a replication file is available from the corresponding author on request.

References

Anson, I. G. (2018). Taking the time? Explaining effortful participation among low-cost online survey participants. *Research & Politics*, *5*(3). https://doi.org/10.1177/2053168018785483

Aslanian, A. (2021). The cyber war on our critical infrastructure and how to win. *Info Security Group*. https://www.infosecurity-magazine.com/opinions/cyber-war-critical-infrastructure/. Accessed 26 August 2021.

Babu, N., De Roeck, K., & Raineri, N. (2020). Hypocritical organizations: Implications for employee social responsibility. *Journal of Business Research, 114*, 376–384.

BBC. (2011). Hackers take down child pornography sites. *BBC*. https://www.bbc.com/news/technology-15428203. Accessed 26 August 2021.

Barnum, T. C., & Solomon, S. J. (2019). Fight or flight: Integral emotions and violent intentions. *Criminology, 57*(4), 659–686.

Belsley, D. A., Kuh, E., & Welsch, R. E. (2005). *Regression diagnostics: Identifying influential data and sources of collinearity* (Vol. 571). John Wiley & Sons.

Bose, N. (2021). Biden: If U.S. has 'real shooting war' it could be result of cyber attacks. Reuters. Retrieved from https://www.reuters.com/world/biden-warns-cyber-attacks-could-lead-a-real-shooting-war-2021-07-27/

Braue, D. (2021). Global ransomware damage costs predicted to exceed $265 billion by 2031. *Cybercrime Magazine*. Retrieved from https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/. Accessed 26 August 2021.

Brelnes, J. (2020). Six common ways people justify unethical behavior. *Psychology Today*. https://www.psychologytoday.com/us/blog/in-love-and-war/202008/six-common-ways-people-justify-unethical-behavior. Accessed 26 August 2021.

Brenan, M. (2021). Cyberterrorism tops list of 11 potential threats to U.S. *GALLUP*. https://news.gallup.com/poll/339974/cyberterrorism-tops-list-potential-threats.aspx. Accessed 26 August 2021.

Broad, J. W., Markoff, J., Sanger, D. (2011). Israeli test on worm called crucial in Iran nuclear delay. *New York Times*. Retrieved from https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html. Accessed 26 August 2021.

Brooks, C. (2021). Ransomware on a rampage; A new wake-up call. *Forbes*. Retrieved from https://www.forbes.com/sites/chuckbrooks/2021/08/21/ransomware-on-a-rampage-a-new-wake-up-call/?sh=6c0e09972e81. Accessed 26 August 2021.

Burt, J. (2021). Ransomware groups look for inside help. *E Security Planet*. Retrieved from https://www.esecurityplanet.com/threats/ransomware-groups-look-for-inside-help/. Accessed 26 August 2021.

Cadsby, C. B., Du, N., & Song, F. (2016). In-group favoritism and moral decision-making. *Journal of Economic Behavior & Organization, 128*, 59–71.

Chang, L., & Krosnick, J. A. (2009). National surveys via RDD telephone interviewing versus the Internet: Comparing sample representativeness and response quality. *Public Opinion Quarterly, 73*(4), 641–678.

Collier, R. (2017). NHS ransomware attack spreads worldwide. *CMAJ, 189*(22), E786–E787.

Collinson, S. (2021). Ransomware attacks saddle Biden with grave national security crisis. CNN. Retrieved from https://www.cnn.com/2021/06/07/politics/president-joe-biden-cyber-attacks-russia-putin-trump-economy/index.html

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security, 87*. https://doi.org/10.1016/j.cose.2019.101568

Cook, S. (2021). 2021 Ransomware statistics and facts. *Comparitech*. https://www.comparitech.com/antivirus/ransomware-statistics/. *Accessed 26 August 2021.*

Craig, T. (2021). HVAC industry needs to prevent ransomware from entering systems. *The News*. https://www.achrnews.com/articles/145402-hvac-industry-needs-to-prevent-ransomware-from-entering-systems. Accessed 26 August 2021.

Crothers, B. (2021). Ransomware "criminals' demands rise as aggressive tactics pay off. *Fox Business.* https://www.foxbusiness.com/technology/ransomware-criminals-demands-rise-aggressive-tactics-pay-off. Accessed 26 August 2021.

CSIS (2021). Significant cyber incidents. *Center for Strategic & International Studies*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed 26 August 2021.

Durkee, A. (2020). More than half of republicans believe voter fraud claims and most still support trump, poll finds. *Forbes*. https://www.forbes.com/sites/alisondurkee/2021/04/05/more-than-half-of-republicans-believe-voter-fraud-claims-and-most-still-support-trump-poll-finds/?sh=65d34c2d1b3f. Accessed 26 August 2021.

Drutman, L. (2020). How hatred came to dominate American politics. *FiveThirtyEight*. https://fivethirtyeight.com/features/how-hatred-negative-partisanship-came-to-dominate-american-politics/. Accessed 26 August 2021.

Fruhlinger, J. (2017). What is Stuxnet, who created it and how does it work? *Reuters.* https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html. Accessed 26 August 2021.

Fung, B. (2021). Colonial Pipeline says ransomware attack also led to personal information being stolen. *CNN*. https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html. Accessed 26 August 2021.

Gambrell, J. (2021). Leaked footage shows grim conditions in Iran's Evin prison. *Bloomberg*. https://www.bloomberg.com/news/articles/2021-08-23/leaked-footage-shows-grim-conditions-in-iran-s-evin-prison

Gatlan, S. (2021). Colonial Pipeline reports data breach after May ransomware attack. *Bleepingcomputer.* https://www.bleepingcomputer.com/news/security/colonial-pipeline-reports-data-breach-after-may-ransomware-attack/. Accessed 26 August 2021.

Gino, F., & Pierce, L. (2010). Lying to level the playing field: Why people may dishonestly help or hurt others to create equity. *Journal of Business Ethics, 95*(1), 89–103.

Graham, A., Cullen, F. T., Pickett, J. T., Jonson, C. L., Haner, M., & Sloan, M. M. (2020). Faith in Trump, moral foundations, and social distancing defiance during the coronavirus pandemic. *Socius, 6*, 2378023120956815.

Graham, J., Haidt, J., & Nosek, B. A. (2009). Liberals and conservatives rely on different sets of moral foundations. *Journal of Personality and Social Psychology, 96*(5), 1029.

Graham, J., Haidt, J., Koleva, S., Motyl, M., Iyer, R., Wojcik, S. P., & Ditto, P. H. (2013). Moral foundations theory: The pragmatic validity of moral pluralism. *Advances in Experimental Social Psychology, 47*, 55–130.

Greenwood, M. (2021). One-third of Americans believe Biden won because of voter fraud: Poll. *The Hill.* https://thehill.com/homenews/campaign/559402-one-third-of-americans-believe-biden-won-because-of-voter-fraud-poll. Accessed 26 August 2021.

Griffin, A. (2017). Daily stormer "'hacked': Nazi website "'taken over by anonymous hacking "group' after Charlottesville white nationalist rally. *Independent.* https://www.independent.co.uk/life-style/gadgets-and-tech/news/daily-stormer-anonymous-hack-charlottesville-white-supremacist-nazi-cyber-attack-a7891741.html. Accessed 26 August 2021.

Haidt, J., & Graham, J. (2007). When morality opposes justice: Conservatives have moral intuitions that liberals may not recognize. *Social Justice Research, 20*(1), 98–116.

Hainmueller, J., Hangartner, D., & Yamamoto, T. (2015). Validating vignette and conjoint survey experimenst against real-world behavior. *Proceedings of the National Academy of Sciences, 112*(8), 2395–2400.

Hauser, D. J., & Schwarz, N. (2016). Attentive Turkers: MTurk participants perform better on online attention checks than do subject pool participants. *Behavior Research Methods, 48*(1), 400–407.

Herman, S., & Pogarsky, G. (2020). Morality, deterrability, and offender decision making. *Justice Quarterly, 39*(1), 1–25.

Hugget, C. (2021). Double-extortion ransomware: The new trend for businesses to prepare for. *Information Age.* https://www.information-age.com/double-extortion-ransomware-new-trend-prepare-for-123496666/. Accessed 26 August 2021.

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal, 22*(1), 105–117.

Iyengar, S., Sood, G., & Lelkes, Y. (2012). Affect, not ideology: A social identity perspective on polarization. *Public Opinion Quarterly, 76*(3), 405–431.

Kinder, D. R., & Kalmoe, N. P. (2017). *Neither liberal nor conservative: Ideological innocence in the American public*. University of Chicago Press.

Klein, S. A., Thielmann, I., Hilbig, B. E., & Zettler, I. (2017). Between me and we: The importance of self-profit versus social justifiability for ethical decision making. *Judgment and Decision Making, 12*(6), 563–571.

Love, D. (2013). 8 things that anonymous, the hacker ‘“”‘terrorist’ group, has done for good. *Business Insider*. Retrieved from https://www.businessinsider.com/good-hacks-by-anonymous-2013-4. Accessed 26 August 2021.

Maigida, A. M., Abdulhamid, S. I. M., Olalere, M., Alhassan, J. K., Chiroma, H., & Dada, E. G. (2019). Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. *Journal of Reliable Intelligent Environments, 5*(2), 67–89.

Marks, J. (2021). The cybersecurity 202: It’s cybersecurity day at the White House. *The Washington Post.* Retrieved from https://www.washingtonpost.com/politics/2021/08/25/cybersecurity-202-it-cybersecurity-day-white-hoyYuse/. Accessed 26 August 2021.

McGuire, M. (2021). Nation states, cyberconflict, and the web of profit. HP Development Company, L.P. Retrieved from https://press.hp.com/content/dam/sites/garage-press/press/press-releases/2021/web-of-profit/hp-bps-web-of-profit-report-april-2021.pdf

McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2021). Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys (CSUR), 54*(9), 1–36.

McMillan, R. (2021). Ransomware attack affecting likely thousands of targets drags on. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/ransomware-group-behind-meat-supply-attack-threatens-hundreds-of-new-targets-11625285071. Accessed 26 August 2021.

Miller, M. (2022). The hard truth behind Biden’s cyber warnings. Politico. Retrieved from https://www.politico.com/news/2022/03/27/bidens-cyber-warnings-00020638

Miller, P. R., & Conover, P. J. (2015). Red and blue states of mind: Partisan hostility and voting in the United States. *Political Research Quarterly, 68*(2), 225–239.

Myre, G. (2021). As Cyberattacks Surge, Biden Is Seeking to Mount A Better Defense. NPR. Retrieved from https://www.npr.org/2021/06/04/1003262750/as-cyber-attacks-surge-biden-seeks-to-mount-a-better-defense

Nakashima, E. (2021) Pressure grows on Biden to curb ransomware attacks. Washington Post. Retrieved from https://www.washingtonpost.com/national-security/ransomware-biden-russia/2021/07/06/ff52a9de-de72-11eb-b507-697762d090dd_story.html

Nakashima, E., & Warrick, J. (2012). Stuxnet was work of US and Israeli experts, officials say. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html. Accessed 26 August 2021.

Paternoster, R., Brame, R., Mazerolle, P., & Piquero, A. (1998). Using the correct statistical test for the equality of regression coefficients. *Criminology, 36*(4), 859–866.

Peer, E., Vosgerau, J., & Acquisti, A. (2014). Reputation as a sufficient condition for data quality on Amazon Mechanical Turk. *Behavior Research Methods, 46*(4), 1023–1031.

Pickett, J. T., Roche, S. P., & Pogarsky, G. (2018). Toward a bifurcated theory of emotional deterrence. *Criminology, 56*(1), 27–58.

Pierce, L., & Balasubramanian, P. (2015). Behavioral field evidence on psychological and social factors in dishonesty and misconduct. *Current Opinion in Psychology, 6*, 70–76.

Poulsen, K., McMillan, R., & Evans, M. (2021). A hospital hit by hackers, a baby in distress: The case of the first alleged ransomware death. *The Wall Street Journal.* Retrieved from https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116. Accessed 26 August 2021.

Richardson, R., North, M. M., & Garofalo, D. (2021). Ransomware: The landscape is shifting—A concise report. *International Management Review, 17*(1), 5–86.

Rosenbaum, R. (2012). Richard Clarke on who was behind the Stuxnet attack. *Smithsonian Magazine.* Retrieved from https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/. Accessed 26 August 2021.

Rutherford, L. (2021). Q&A: Understanding the rising threat of ransomware attacks. *USA Today*. Retrieved from https://news.virginia.edu/content/qa-understanding-rising-threat-ransomware-attacks. Accessed 26 August 2021.

Sanger, D. (2012). Obama ordered wave of cyberattacks against Iran. *The New York Times.* https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html. Accessed 26 August 2021.

Sanger, D. (2021). Russia's most aggressive ransomware group disappeared. It's unclear who made that happen. *The New York Times*. Retrieved from https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html. Accessed 26 August 2021.

Shaban, H. (2021). T-Mobile says hackers stole data of more than 40 million people. *The Washington Post*. Retrieved from https://www.wsj.com/articles/t-mobile-says-hackers-stole-details-on-more-than-40-million-people-11629285376. Accessed 26 August 2021.

Shalvi, S., Gino, F., Barkan, R., & Ayal, S. (2015). Self-serving justifications: Doing wrong and feeling moral. *Current Directions in Psychological Science, 24*(2), 125–130.

Siegel, B. (2021). Protect yourself against ransomware attacks. *Ohio University News*. Retrieved from https://www.ohio.edu/news/2021/08/protect-yourself-against-ransomware-attacks. Accessed 26 August 2021.

Silver, J. R., & Silver, E. (2021). The nature and role of morality in offending: A moral foundations approach. *Journal of Research in Crime and Delinquency, 58*(3), 343–380.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664–670.

Telang, R. (2021). Could ransomware attacks ultimately benefit consumers? *Harvard Business Review*. Retrieved from https://hbr.org/2021/08/could-ransomware-attacks-ultimately-benefit-consumers. Accessed 26 August 2021.

Theis, J. (2021). How should U.S. companies guard against the growing threat of ransomware? *Builtin.* Retrieved from https://builtin.com/cybersecurity/guard-against-ransomware. Accessed 26 August 2021.

Thompson, A. J., & Pickett, J. T. (2020). Are relational inferences from crowdsourced and opt-in samples generalizable? Comparing criminal justice attitudes in the GSS and five online samples. *Journal of Quantitative Criminology, 36*(4), 907–932.

Weinberg, J. D., Freese, J., & Mc Elhattan, D. (2014). Comparing data characteristics and results of an online factorial survey between a population-based and a crowdsource-recruited sample. *Sociological Science, 1*, 292–310.

Welburn, J. & Hodgson, Q. (2021). The US should deter ransomware computer attacks. *The Los Angeles Times.* https://www.latimes.com/opinion/story/2021-08-08/ransomware-attacks-defense-national-security. Accessed 26 August 2021.

Wiltermuth, S. S., Vincent, L. C., & Gino, F. (2017). Creativity in unethical behavior attenuates condemnation and breeds social contagion when transgressions seem to create little harm. *Organizational Behavior and Human Decision Processes, 139*, 106–126.

Winder, D. (2021). Ransomware reality shock: 92% who pay don't get their data back. *Forbes.* Retrieved from https://www.forbes.com/sites/daveywinder/2021/05/02/ransomware-reality-shock-92-who-pay-dont-get-their-data-back/?sh=97a09d4e0c75. Accessed 26 August 2021.

Murat Haner Murat Haner is an assistant professor in the School of Criminology and Criminal Justice at the Arizona State University. His current research is focused on examining the issue of radicalization into terrorist organizations and understanding public opinion on terrorism, counter-terrorism policies, and other pressing social issues. His research has been published in journals such as Justice Quarterly, British Journal of Criminology, Crime & Delinquency, and Terrorism & Political Violence.

Melissa M. Sloan Melissa M. Sloan is an Associate Professor of Sociology and Interdisciplinary Social Sciences at the University of South Florida. Her research interests include the sociology of emotion, with a particular focus on fear of terrorism and psychological well-being, and the interdisciplinary research process. Her research has been published in journals such as Social Psychology Quarterly, Socius: Sociological Research for a Dynamic World, and the American Review of Public Administration.

Amanda Graham Amanda Graham is an assistant professor in the Department of Criminal Justice and Criminology at Georgia Southern University. Her research interests focus on policing, fear of police brutality, the impact of race in police–community relationships, police legitimacy, and measurement.

Justin T. Pickett Justin T. Pickett is an associate professor in the School of Criminal Justice at the State University of New York at Albany. His research interests include survey research methods, public opinion, police–community relations, and theories of punishment.

Francis T. Cullen Francis T. Cullen is a distinguished research professor emeritus and senior research associate in the School of Criminal Justice at the University of Cincinnati. His research interests include offender rehabilitation and redemption, racial attitudes and criminal justice policy, social support theory, and the criminology of Donald Trump.