JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 3(1), 2017, 49–58
doi: 10.1093/cybsec/tyw018
Advance Access Publication Date: 15 February 2017
Research paper

Research paper

Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes

Michael L. Gross*, Daphna Canetti and Dana R. Vashdi

School of Political Science, The University of Haifa, Mt. Carmel, Haifa, Israel

*Corresponding author. E-mail: mgross@poli.haifa.ac.il

Received 30 December 2016; accepted 30 December 2016

Abstract

Does exposure to lethal and non-lethal cyberterrorism affect psychological well-being, public confidence and political attitudes? By what mechanisms do they do so? While cyberterrorism most often raises concerns about national security, its effects on individuals' psyche and cognition are overlooked. To address these questions we carried out three studies between 2013 and 2016 ($n = 1124$, 909 and 592). Utilizing experimental manipulations (video clips) subjects were exposed to simulated lethal and non-lethal cyberterrorism. Our findings demonstrate a stress-based 'cyber terrorism effect'. Exposure to cyberterrorism is not benign and shares many traits with conventional terrorism: stress, anxiety, insecurity, a preference for security over liberty, a reevaluation of confidence in public institutions, a heightened perception of risk and support for forceful government policies. In the cyber realm, this translates into support for such policies as Internet surveillance, government regulation of the Internet and a forceful military response to cyberterrorism (including conventional, kinetic retaliation). These attitudes may impinge upon the tolerance and confidence necessary for a vibrant civil society. This effect is associated with non-lethal cyberterrorism that causes economic loss as well as with cyberterrorism that causes death and injury.

Key words: cyberterrorism; cyberwar; cybersecurity; threat perception; stress; exposure; public confidence

Introduction

A primary goal of conventional terrorism is to undermine civilians' resilience by instilling a sense of fear and vulnerability that erodes confidence in the ability of the government and law enforcement agencies to protect citizens against future attacks [1]. What about cyberterrorism? Are the psychological ramifications of conventional and cyberterrorism identical? Does the threat of conventional or cyberterrorism affect confidence in government and support for forceful security policies in the same way? To address these questions, we advanced three multiple scenario-based empirical studies for testing what happens when the public experiences cyberterrorism that causes mass casualties and/or severe economic losses with the avowed goal of undermining the public's morale and its confidence in economic and political institutions.

Our findings draw on three large n studies conducted from 2013 to 2016 and suggest that cyberterrorism aggravates stress and anxiety, intensifies feelings of vulnerability and hardens political attitudes. In these ways, we demonstrate that cyberterrorism causes responses similar to conventional terrorism. These responses highlight the human dimension of cyberterrorism that is often neglected as policymakers focus on national security interests and the protection of frontiers, critical infrastructures and military capabilities. Both are important and as the threat of cyberterrorism grows, policymakers will have to direct their attention to the emotional distress that cyberterrorism causes just as they strive to bolster deterrent and offensive cyber capabilities. In the sections below, we draw out the similarities between the psychology of conventional and cyberterrorism that inform our empirical research,

present the details of our findings and discuss their implications for public policy.

Conventional and cyber terror: mirror images?

Conventional terrorism employs kinetic means (e.g. suicide bombers or improvised explosive devices) and works in many ways. Accompanied by death, injury and property destruction, terrorism generates fear and anxiety in the target population. Terrorists may, therefore, use terrorism to demoralize a civilian population to pressure their government to undertake or refrain from a specific policy. Sometimes terrorists are effective. Witness the sudden departure of Spanish troops from Iraq following terror bombings in Madrid that killed 191 people in 2004. More commonly, however, the civilian population proves exceptionally resilient [2–4]. Terrorism hardens their hearts as they demand and often receive a forceful response from their government. Armed groups, such as Hamas, may also resort to terrorism to scuttle prospects of peace [5]. Alternatively, terrorism is theater, specifically designed to seize centre stage and provoke a disproportionate response from the government of terror victims with the hopes of turning world opinion. For nearly a decade, Israel avoided any massive response to Hamas' crude missile attacks on Southern Israel. Although the attacks disrupted everyday life, few people lost their lives. Eventually, though, security concerns and domestic pressure led to a full-scale invasion of the Gaza Strip in 2008 and again in 2014. Apart from achieving a short and fragile ceasefire, Israel faced a storm of international condemnation following the deaths of more than 1000 Palestinians in each encounter. In this way, terrorism sometimes creates a no-win situation for states [6]. Finally, terrorism may produce relatively few immediate casualties but undermine public confidence more broadly. Airplane hijackings such as those of 9/11, undermined faith in the air transportation system until governments introduced rigid controls [7]. Generally, however, conventional terrorism does not regularly affect confidence in major government institutions. This is attributable to a 'rally around the flag' effect and to the growing dependence on government institutions to provide security ([8–12], but see Baldwin *et al.* [13] and Berry *et al.* [14] for contrary data).

In contrast to conventional terrorism, cyberterrorism employs malicious computer technology rather than kinetic force. But like conventional terrorism, cyberterrorism aims to further political, religious, or ideological goals by harming civilians physically or psychologically. By contrast, 'cyberwar' uses malware and viruses to disable military targets while 'cybercrime' aims for pecuniary gain or personally motivated harm to others (e.g. revenge, bullying) unrelated to political conflict. Sometimes these categories overlap and the differences are difficult to discern. Cyber-terrorists and nation states may, like criminals, steal money, data or identities or, like hacktivists, mount DDoS strikes to shut down major systems. Much depends upon the intention and identity of the actors that are not always known. In our cases, Hamas and Anonymous are the perpetrators and each publically announced its intent to terrorize Israeli citizens. In Europe and the USA, on the other hand, attribution may be more difficult as ISIS and proxy hacktivists have reason to sometimes conceal their identities.

Despite its growth, cyberterrorism unlike conventional terrorism does not currently threaten life and limb. As a result, very little attention is paid to the effects of cyberterrorism on civilians [15]. The Tallinn Manual on the International Law Applicable to Cyber Warfare [16], for example, describes how cyber operations may rise to the level of an armed attack by threatening widespread loss of life or destruction of property. However, the Manual considers operations that block email throughout the country (section 30.12), involve 'mere economic coercion' (section 11.2), transmit tweets to cause panic by 'falsely indicating that a highly contagious and deadly disease is spreading through the population' (section 36.3) or comprise cyber psychological operations intended solely to undermine confidence in a government or economy (section 11.3) as insufficiently severe to constitute terror. We ask whether current events do not belie this equanimity. Claiming, 'The internet is not indispensable to the survival of the civilian population' (section 81.5) the framers of the Tallinn Manual seem unaware of the effects cyberterrorism may pose. As cyberattacks grow in frequency and intensity, they push beyond criminal acts to concerted attempts to disrupt airport and utility services in the Ukraine [17], perpetrate an electronic Holocaust in Israel (below), cripple DynDNS servers across important sectors of the USA and interfere with and possibly compromise the recent US elections. While not all the perpetrators or their goals are immediately obvious, they do not appear motivated by monetary gain. Rather it seems that they aim to impair public confidence, disrupt civil society and seed anxiety and insecurity by crippling digital and financial resources, undermining the institutions of governance and disrupting social networks. Given the growing threat of cyberterrorism, the question, 'How does non-lethal and lethal cyberterrorism affect individuals psychologically?' is pressing. In an attempt to shed some light on this question, we examined the effects of different kinds of cyberattacks on a person's sense of security and confidence.

Research design

Experimental overview

To evaluate the effects of different kinds of cyberattacks on a person's sense of security and confidence, we utilized two platforms: experimental manipulations and self-reported past exposure to cyberattacks. Focusing on emotional and political responses to cyberattacks and using original video clips, we conducted three online and panel studies.

Our experimental designs enabled randomization and full control of the researchers. While online surveys—particularly non-probability ones—may be slightly skewed towards the younger and the technology savvy, phone surveys tend towards older respondents, women and left leaning individuals. Because we were not conducting a correlational study seeking precise estimates of population values, we followed the recommendations of Baker et al. [18] that support the use of online studies for the purposes described in our studies [19]. Each study received University Institutional Review Board (IRB) approval. Participants signed a consent form at the beginning of the survey and we made provisions for psychological support with the survey company if needed. None was requested. Participants were debriefed and informed post-study that all the scenarios were simulated and not actual attacks.

Study 1 (September 2015)

This is an online survey experiment in which Israeli adults were randomly assigned to three treatments after which they answered a series of psychological and political questions. The control group received no experimental stimulus. In the 'high' treatment group, subjects viewed a video clip depicting civilian and military deaths following cyberattacks on missile systems and the electric company. In the 'low' treatment group, they viewed a video clip reporting a non-lethal cyberattack accompanied by damage to hardware, loss of

data and theft of funds ($n = 1124$). In neither case was the perpetrator identified.

Study 2 (January 2016)

This was also an online survey. Here, subjects were randomly assigned to a news report describing a cyberattack on Israel's water purification network by terrorists (Hamas). The news reports were identical with the exception of the losses suffered. In one clip, two people died and many were injured after terrorists released deadly amounts of chlorine into the water system. In the second clip, Hamas retrieved the financial information of the company's customers and successfully transferred substantial funds to its coffers overseas. Alternative manipulations included a conventional terror attack, that depicts a kinetic attack on a water facility that, like the kinetic attack, kills two and injures many and a control group that viewed a benign clip depicting the dedication of a new water desalinization plant ($n = 909$). Immediately after viewing the clip, subjects were asked to report risk perception, threat perception and confidence in government and to evaluate offensive cyber policies and cyber regulation practices.

Study 3

Using a two-wave panel design, we administered two surveys to the same panel of 522 experimental subjects—10 days apart, leading up to and following Anonymous' well-publicized 'electronic Holocaust' campaign against Israel in April 2015. Anonymous' language was belligerent and menacing but did not threaten physical harm. Rather they warned that 'elite cyber squadrons' would 'invade and attack your devices and personal data, take down your servers and erase Israel from cyber space' [20]. Pre- and post-attack questionnaires focused on the emotional and cognitive responses to the attacks and related policy choices ranging from cyber to kinetic retaliation.

Independent variables

Type of terrorism

This was manipulated in Studies 1 and 2 by the experimental condition as explained above. In Study 1, there were three conditions: (i) control, (ii) cyberterrorism, non-lethal and (iii) cyberterrorism, lethal. In Study 2, there was an additional condition: (iv) kinetic terrorism.

Previous exposure to a cyberattack

This was assessed in all three studies by asking subjects four questions on a scale of 1–6 regarding the extent to which they, their friends or their family suffered harm or loss from a cyberattack. An answer above 3 on any of these questions was regarded as previous exposure.

Dependent variables

Measures of well-being, stress and threat perception

In 'Study 1' (unidentified perpetrator) and 'Study 2' (Hamas), we used a four-point scale State–Trait Anxiety Index (STAI) [21]. STAI measures two types of anxiety—state (extrinsic) and trait (intrinsic) anxiety. State anxiety aligns with temporary feelings of fear, nervousness and discomfort. Trait anxiety aligns with almost daily feelings of stress, worry and discomfort. The questionnaire includes six items describing various feelings and emotions. The experimental subjects were asked to rate on a scale of 1–4 (1 = not at all; 4 = very much so) the extent to which their feelings 'at present' (both pre- and post experimental treatment) correspond to different items. Half of the items represent negative feelings and emotions (e.g. 'I feel upset', 'I feel nervous') and the other half represent positive feelings and emotions (e.g. 'I feel relaxed', 'I feel comfortable'). Because we were interested in negative affect, we created a variable constituting only the three negative emotions.

In addition to stress, perceptions of threat play a significant role in our understanding of the psychology of terrorism. Perceptions of threat reflect the extent to which thinking about a cyberattack undermines ones sense of personal security. Threat perception is an appraisal of the danger that an out-group poses to an individual and/or his/her political community [22–26, 56, 57, 58, 59]. To gauge threat perception in all three studies we asked 'To what extent do cyberattacks undermine your sense of personal security?' and 'To what extent do you feel threatened by cyber terrorism?' (Scale 1–5).

Measures of public confidence

To assess the effects of cyberattacks, Study 2 (Hamas) probed a range of confidence related questions. First, confidence in government, the army, police and supreme court were examined with separate items for each on a scale of 1 = not confident at all to 6 = extremely confident. Following each manipulation, we also asked a range of questions about confidence in the government's ability to safeguard information entrusted to government offices, prevent identity and data theft, credit card and bank fraud, and protect critical infrastructures (water, military, transportation, electric) from future attacks (1 = not confident at all; 6 = extremely confident). Of closer resolution, we asked about confidence in a bank, utility company or HMO (Health Maintenance Organization) that suffered a cyberattack. We also included two behavioural questions that address the public's confidence in the government assurances following a cyberattack on the national water supply by posing behavioural choices to gauge confidence:

1. 'Following a cyber-attack on the water system, the authorities advised drinking bottled water. How soon would you drink tap water?'
2. 'Following a cyber-attack on the water system the authorities suggested waiting 3 days before showering: After 3 days, would you . . .?'

Following each question, subjects were asked to choose one of four modes of behavior that reflect various degrees of compliance (full responses are provided below).

Measures of attitudes towards government policies

In all three studies, we asked subjects to consider government surveillance of the Internet and emails, government regulation of the businesses and military retaliation in response to cyberattacks. Questions about government surveillance asked whether the government ought to read emails and monitor social networks for security threats. Regulation of the business sector reflected answers to 'Should the government require businesses to maintain a mandated level of cyber security.' Retaliatory policy offered four options: (i) a 'limited cyberattack' to disable enemy military cyber capabilities (servers, switches, computers, cables); (ii) a 'large scale cyberattack' to disable enemy military and civilian cyber capabilities; (iii) a 'limited conventional attack' (missiles or bombs) to disable enemy military cyber capabilities; and (iv) a 'large scale, conventional attack' (missiles or bombs) to disable enemy military and civilian cyber capabilities. All questions were rated on a scale of 1 (not at all) to 6 (most definitely).

Table 1. Stress/anxiety measures following experimental cyberterror attacks. Scale: 1 (low) to 4 (high)

	State/trait anxiety measure STAI	
	Study 1[a], $n = 1027$	Study 2[a], $n = 907$
PerpetratorTreatment group	Unidentified	Hamas
Control: no terrorism	2.3	2.7
Cyberterrorism, non-lethal: asset and data loss (Study 1); disclosure of account information, loss of funds (Study 2)	3.5	3.4
Cyberterrorism, lethal: deaths and injuries	3.6	3.6
Conventional (kinetic) terrorism, lethal: deaths and injuries		4.0
Significance	$P < 0.001$	$P < 0.001$
ANOVA (Analysis of Variance)	$F_{2,1035} = 139.65$	$F_{3,942} = 34.23$

[a]In *post hoc* tests using the Tukey statistic there is a significant difference between all treatment groups except for the difference between non-lethal and lethal cyberterrorism that is not significant for any of the stress/anxiety measures.

Table 2. Threat perception measures following experimental cyberterror attacks. Scale 1 (low) to 5 (high)

Experiment Perpetrator treatment group	Study 1[a], $n = 1027$ Unidentified	Study 2[b], $n = 907$ Hamas
Control: no terrorism	2.9	3.1
Cyberterrorism, non-lethal: disclosure of account information and loss of funds		3.4
Cyberterrorism, non-lethal: asset and data loss	3.4	
Cyberterrorism, lethal: deaths and injuries	3.5	3.6
Conventional terrorism, lethal: deaths and injuries		3.8
Significance	$P < 0.001$	$P < 0.001$
ANOVA	$F_{2,1029} = 21.60$	$F_{3,937} = 11.12$

[a]In *post hoc* tests using the Tukey statistic for the data of Study 1, there was no significant difference between non-lethal and lethal cyberterrorism, but both were significantly different than the control group.

[b]In *post hoc* tests using the Tukey statistic for the data of Study 2, there was no significant difference between the control group and non-lethal cyberterrorism, no significant difference between non-lethal and lethal cyberterrorism and no significant difference between lethal cyberterrorism and conventional terrorism. Lethal cyberterrorism and conventional terrorism were significantly different than the control group and conventional terrorism was significantly different than non-lethal cyberterrorism.

Measures of risk perception

Following Slovic [27], we distinguish between risk assessment and risk perception: 'Whereas technologically sophisticated analysts employ risk assessment to evaluate hazards, the majority of citizens rely on intuitive judgments typically called risk perceptions.' To assess risk perception we posed 16 questions that asked the experimental subjects in Study 2 (Hamas) to assess the risk posed by a cyberterror attack (1 = no risk; 6 = a very high risk). Responses loaded on four factors: bodily harm (risk of injury or loss of life); material loss (credit card and bank fraud, data theft, theft of confidential medical information); damage to critical infrastructures (transportation, refineries, water) and damage to state facilities (military, stock exchange, government offices) Alpha Cronbach 0.70, 0.91, 0.81 and 0.94, respectively.

Demographic variables

We asked respondents about their political orientation on a scale ranging from very right-wing to very left-wing.

Results

Our findings suggest that the effects of 'non-lethal' and 'lethal' cyberterrorism track those of conventional terrorism. Overall, experimental subjects exhibit marked signs of stress, personal insecurity and heightened perceptions of cyber threat. Heightened perceptions of threat, in turn, lend support for forceful cyber government policies, a finding consistent with the effects of kinetic terrorism [28–31].

Stress and anxiety

Table 1 describes how anxiety increases as attacks become more severe. Compared to the control group, every form of terrorism, whether cyber or kinetic, lethal or non-lethal, increased anxiety and other negative emotions. Conventional (kinetic) terrorism had the greatest effect upon all measures of negative affect and anxiety followed by lethal and non-lethal cyberterrorism. However, the effects of lethal and non-lethal cyberterrorism were not statistically distinguishable. Each affected STAI measures similarly, their effects significantly more severe than those seen in the control group. Each kind of cyberterrorism generated increasing levels of anxiety. As an ongoing feature of Israeli life, conventional terrorist attacks provoke anxiety more readily than cyberterror attacks. Nevertheless, it appears that all remain points on the same terrorist spectrum. Non-lethal cyberterrorism is no exception.

Threat perception

Both exposure to past cyberattacks and exposure to simulated cyberattacks increased perceptions of threat. As noted above, we gauged exposure to past cyberattacks by asking subjects whether they, their friends or family suffered harm or loss from a cyberattack. Of the respondents, 18% in the Study 3 (Anonymous) reported harm or loss from cyberattack as did 19% in Study 2 (Hamas). Among our subjects, perceptions of threat were 3–9% stronger among those previously exposed to a cyberattack than among those who were not exposed. The experimental manipulations affected threat perception similarly (Table 2).

Simulated exposure to lethal attacks, whether cyber or kinetic, evoked perceptions of threat 16–22% stronger than those unexposed to terrorism in the control group. Among those exposed to non-lethal cyberterrorism, perceptions of threat were 10–17% stronger than among those in the control group. These results varied relative to the nature of non-lethal cyberterrorism. Perceptions of cyber threat were strongest when non-lethal cyberattacks resulted in the loss of 'assets and data' (Study 1, unidentified perpetrator), rather than the loss of 'funds' (Study 2, Hamas). While loss of data and other digital assets might be irreplaceable or costly to replace, banks and other financial institutions usually reimburse customers for funds lost to hackers. Our results indicate that the fact that the perpetrator was Hamas, a hostile agent that one might expect to induce threat perception, did not change this assessment. Indeed, when non-lethal cyberterrorism is defined in terms of

Table 3. Confidence measures, Study 2 (Hamas). Scale 1 (not confident) to 6 (extremely confident) $n = 907$

Condition confidence measure	Control	Cyberterrorism non-lethal	Cyberterrorism lethal	Conventional terrorism	Sig. ANOVA
Confidence in government to protect infrastructures (water, electric, transportation, stock exchange, classified military data)	4.1	4.1	4.2	4.2	NS
Confident in government to protect personal data	3.6	3.6	3.5	3.5	NS
Confidence in public/private institutions (army, scientific community, high-tech sector, government, police) to prevent a serious cyberterror attack	4.4	4.6	4.5	4.5	NS
Confidence in those responsible for cybersecurity to know what they are doing	4.8	5.1	5.0	5.0	0.01 $F_{3,904} = 2.68$[a]

[a]In *post hoc* tests using the Tukey statistic the significant difference lies only in the difference between the control group and the non-lethal cyberterrorism (NS = not significant).

financial loss alone, its effects on threat perception were not statistically different than among those in the control group (see notes, Table 2). Further data are necessary to substantiate the relationship between perceptions of threat and non-lethal cyber-terrorist attacks.

The data in Tables 1 and 2 clearly suggest that cyberattacks, whether lethal or non-lethal, cause stress, anxiety and insecurity. In their wake, threat perception rises to a level very close to conventional terrorism when cyberterrorism turns deadly. These data demonstrate how cyberterrorism, like conventional terrorism, impairs psychological well-being and increase perceptions of threat. The fear stemming from threat perception may lead to incorrect assessments of risk and risk-averse attitudes that, in turn, impinge upon confidence in government institutions.

Cyberterrorism and public confidence

Confidence in the government's ability to protect critical infrastructures and data or to prevent a cyberattack did not vary as manipulations presented increasingly dangerous and life-threatening forms of terrorism. And, the slight effect we found (item 4) shows an 'increase' in confidence only following a non-lethal cyber-terrorist attack. The data appear in Table 3.

Two other questions posed behavioural choices to gauge confidence:

Option	Percentage agreeing
a. When the authorities say it is OK	70
b. 3 months after the authorities say it is OK	24
c. 1 year after the authorities say it is OK	5
d. Never	6

(1) Following a cyberattack on the water system, the authorities advised drinking bottled water: How soon would you drink tap water? ($n = 909$)

a. Shower?	63
b. Wait 1 week	19
c. Install a filter that doubled your water bill	8
d. Install a filter that tripled your water bill	4

(2) Following a cyberattack on the water system, the authorities suggested waiting 3 days before showering: After 3 days, would you? ($n = 909$)

Table 4. Political action following cyberattack on selected facilities, $n = 907$

Response (% agreeing)	Electric Co.	HMO	Bank
Complain to the facility	30	25	22
Find a different HMO/bank		7	15
File a lawsuit	12	14	18
Complain to the city	4		
Turn to the press	4	3	3
Participate in a demonstration	14	4	4
File a complaint with the ombudsman		10	7
Complain to the police		12	11
Other or none	37	24	18

In each case, 30–37% of the respondents do not trust the authority's instructions. Rather, they preferred to take additional measures to protect themselves. The answers to these two questions were unaffected by the manipulations.

To further investigate the behavioural dimensions of confidence, we asked subjects how they would publically react to cyberterrorism? Would they be quiescent or would they take to the streets in a way that might undermine political stability and foment unrest in the way terrorists often hope? Table 4 portrays public political behaviour in the wake of three kinds of cyberterror attacks: an attack on the national electric company, a private HMO and a private bank. In each case, subjects were asked to choose the most likely political action they would take.

While these questions did not specify whether the attack on the facility was lethal or non-lethal, few people are sufficiently riled to take to the streets. A substantial minority (22–30%) would complain to the authorities and some would join a lawsuit (12–18%), but few would demonstrate. None of the attacks prompted outrage or lack of confidence in the government. On the contrary, the manipulations prompted support for greater government intervention to assure security. It is no surprise then, that confidence in the government is generally unaffected by cyberterrorism and may even increase in its wake.

Cyberterrorism and political attitudes: security, civil liberties, government regulation and military retaliation

Confronted with the threat of lethal and non-lethal cyberterrorism, our data suggest that individuals will support strong government measures to police and regulate cyberspace and to respond forcefully

Table 5. Support for domestic and retaliatory cyber policy

Perpetrator policy	Study 1, $n = 1027$ Unidentified (% agreeing[a])	Study 2, $n = 907$ Hamas (% agreeing[a])	Study 3, $n = 522$ Anonymous (% agreeing[a])
Domestic cyber policy			
Surveillance			
Monitor for suspicious expressions		67	54
Read emails		46	23
Monitor Facebook Twitter		61	48
Regulation of business to maintain cybersecurity	69	62	78
Willingness to give up privacy for security	54	44	
Retaliatory policyfollowing a hostile cyber attack			
Cyberattack on military facilities		84	86
Cyberattack on military and civilian facilities		78	69
Conventional attack on military facilities		60	37
Conventional attack on military and civilian facilities		65	31

[a]% who agree, very much agree or absolutely agree

to cyberattacks. In all three studies, we asked subjects to consider government surveillance of the Internet and emails, government regulation of the businesses and military retaliation in the wake of cyberattacks. These results appear in Table 5.

Overall, the high percentages of support reflect widespread backing for these policies. Well over 50% support government monitoring of emails for suspicious expressions and roughly 50% are willing to give up privacy for security and allow the government to monitor social media (Facebook, Twitter). At the same time, 23% will permit the government to read emails, a figure that doubles to 46% when the perpetrator is Hamas. These numbers are higher than in the USA where, in a recent PEW Survey [32] in the USA, 43% of the subjects said it is acceptable for the government to monitor the communications of US citizens (compare 48–67% in our survey).

Looking beyond surveillance to retaliatory policy we see how military strikes, particularly cybernetic but also kinetic, command significant support from the public. In response to cyberterrorism, the vast majority (69–89%) support retaliatory cyberattacks against military and civilian targets while a significant number (31–65%) support conventional, 'kinetic' counter attacks. These attitudes remain unstudied in the USA, but there is little doubt that they will play a significant role as public officials and scholars weigh the merit of responding to cyberwar and cyberterrorism with kinetic force [33, 34].

To explain why individuals hold different attitudes about surveillance and military retaliation, we looked at a number of factors. The experimental manipulations within each study had no direct effect on political attitudes as they did on anxiety and did not affect the extent to which individuals supported different types of retaliation. That is, support for surveillance, regulation or military action was not affected by exposure to a simulated cyberattack (With the exception of Study 1, (unidentified perpetrator), where the willingness to give up privacy increased as the manipulation grew more severe.). Similarly, self-reported exposure to cyberattacks did not affect attitudes towards these policies. Instead, variables that explain greater support for government interference include political and religious conservatism, threat perception and the identity of the perpetrator. Support from right-wing religious conservatives is consistent with the right's traditional demand for security and their support for the current right-wing government. Among our subjects, the odds that right-wing conservatives would support militant policies were up to two times higher than those on the left. Beyond the role of political orientation, however, lie the effects of threat perception. As threat perception (in contrast to direct exposure to cyber violence) grows, individuals demand greater security from their government. Here, the odds were 1.3–2.2 times higher that individuals with high levels of threat perception will support surveillance, government regulation and military retaliation compared to those with lower perceptions of threat.

Our data also suggest that the identity of the perpetrator matters. Note how support for government surveillance and, in particular, retaliatory 'military' strikes is appreciably greater when the manipulation focused on a known terrorist group, Hamas, (Study 2) rather than on a hacktivist group, Anonymous (Study 3). Our question was framed generally and asked whether subjects would support military retaliation following a cyberattack. We did not ask whether they would support an attack against Hamas or Anonymous or their sponsors. Nevertheless, and as Table 5 demonstrates, subjects participating in the Hamas experiment favoured government surveillance far more than those in Study 3 (Anonymous) and supported conventional military attacks of either sort (limited or large scale) by a margin of nearly 2:1. One reason may be that the manipulation triggered fears of Hamas and burgeoning Islamic radicalism. Another reason may be the recognition that Hamas, like ISIS, has infrastructures and territory vulnerable to conventional attack. Because our study found a relationship between threat perceptions and support for surveillance and military retaliation it seems that it is not Hamas' material vulnerability but the fear related to threat perception that better explains why those exposed to Hamas cyberterrorism are more likely to support surveillance and military retaliation than those facing Anonymous. Nevertheless, this may change. In a phenomenon, George Lucas [35] describes as 'state sponsored hacktivism', nations recruit hacktivist groups to mount cyberattacks on their behalf. As they do, fears of such groups may grow accordingly as might the willingness to retaliate against their sponsors.

Cyberterrorism and risk perception

Researchers of risk perception have long noted how individuals' perceptions of the risk of common hazards [27] or disease [36] are often markedly different from the assessments of experts. The result is to make it more difficult to manage risk effectively. How, then, does the public understand the risk of cyberterrorism? If cyberterrorism, unlike conventional terrorism, disease or natural disasters, has yet to harm anyone, there is good reason to suspect that the public does not understand the risk it poses. Experts are themselves divided [37]. Some remain sceptical about the capabilities of terrorist groups

Table 6. Risk Assessment, Study 2(Hamas). Scale 1 (very low) to 6 (very high).

What are the chances of a cyberattack causing:	Control	Cyber terror non-lethal	Cyber terror lethal	Conventional terrorism	Sig. ANOVA	Total average[a]
1. Theft of data, assets, identity	3.0	3.1	3.1	3.2	NS	3.1
2. Attacks on state facilities: military, stock exchange, government offices	3.7	3.7	3.5	3.8	NS	3.6
3. Destruction/damage of critical infrastructures[b]	4.4	4.7	4.6	4.8	<0.001 $F_{3,907} = 5.9$	4.6
4. Loss of life or limb[c]	2.7	2.7	3.1	3.2	<0.001 $F_{3,908} = 19.22$	2.9

[a]A repeated measures ANOVA with a Greenhouse-Geisser correction was statistically significant ($F2.908, 2640.671 = 904.457$, $P < 0.001$). All the mean scores between the all the different categories of risk assessment were significantly different from each other.

[b]In *post hoc* tests using the Tukey statistic, there was no significant difference between the the non-lethal cyberterrorism group, the lethal cyberterrorism group and the conventional terrorism group. These three groups were all significantly different from the control group.

[c]In *post hoc* tests using the Tukey statistic, there was no significant difference between the control group and the non-lethal cyberterrorism group and no significant difference between the lethal cyberterrorism group and the conventional terrorism group. Significant differences were found between lethal cyberterrorism and the control and non-lethal cyberterrorism and between the conventional terrorism and the control and non-lethal cyberterrorism.

or violent hacktivists to mount offensive, catastrophic cyberattack [38–40] while others describe how cyberterrorism may seriously compromise electrical infrastructures [41], disable military defense systems [42] and, ultimately, 'undermine conventional and nuclear stability' [43]. Divisions among experts might only confound risk perceptions among the lay population.

In our study, risk perceptions varied with the manipulations of Study 2 (Hamas). Those exposed to increasingly severe manipulations assess some cyber threats more severely than the control groups (Table 6).

These data demonstrate how experimental manipulations exacerbate some assessments of risk from cyberterrorism. After viewing video clips of cyber or conventional terror attacks with lethal consequences, subjects' perceptions of risk to life, limb and infrastructures were significantly greater than of those viewing the more benign clips (rows 3, 4). When asked to assess the chances of a cyberattack-causing destruction of critical infrastructures the average response rose from 4.4 in the control group to 4.8 in the conventional terrorism group. Similarly, when asked to assess the chances of a cyberattack-causing loss of life and limb the average response rose from 2.7 in the control group to 3.2 in the conventional terrorism group. On the other hand, the manipulations did not affect the risk associated with data theft or attacks on the stock exchange or government offices (rows 1, 2). These stayed constant across the manipulations. These attitudes reflect concerns about the future threat of cyberterrorism. The risk associated with identity theft, asset loss and attacks on the government offices is stable, while the risk associated with significant bodily or infrastructural harm is not. Individuals seem to think they understand the risks of non-lethal cyberterrorism but seem unsure about the risks of lethal cyberterrorism when, in fact, our data indicate much the opposite. They underestimate the danger of non-lethal cyberterrorism while often overestimating the danger of lethal terrorism particularly when the perpetrator is a known terrorist organization. As such, it is important to notice that the perception of threat, in part, contradicts reality. For many subjects, the risk of an attack that destroys or damages critical infrastructures, which has yet to materialize to any significant degree (average 4.6), is significantly 'greater' than the risk of an attack on stock exchanges, government offices, personal computers, banks and credit cards that are clear and present dangers (average 3.6). While these outcomes might be partially explained by a manipulation that primes subjects for threats to infrastructures, our control group viewed no attack and still assessed some risks unrealistically high. At the same time the average perception of risk associated with the theft of data, assets and identity (average 3.1) was little different from a risk that a cyberattack would bring death or injury (average 2.9). They perceive the risk of these hazards equally despite the fact that the former is relatively common and the latter non-existent.

Discussion: the psychological effects of cyberterrorism

Our results show that cyberterrorism, even when non-lethal, impacts the civilian population in several ways. First, cyberterrorism aggravates anxiety and personal insecurity. Secondly, lethal and non-lethal terrorism exacerbate perceptions of threat and personal insecurity. Thirdly, many people, particularly those with high levels of threat perception, are willing to support strong government policies. These policies split along two lines and include foreign policy (e.g. cyber and/or kinetic military responses to cyberattacks) and domestic policy (e.g. tolerance of government surveillance and control of the Internet). As threat perception increases, individuals take increasingly stringent political views. Like conventional terrorism, cyberterrorism hardens political attitudes as individuals are willing to exchange civil liberties and privacy for security and support government surveillance, greater regulation of the Internet and forceful military responses in response to cyberattacks. And while these measures are meant to ensure national security, such foreign and particularly domestic policies may adversely affect the unfettered discourse necessary for a vibrant and open democratic society [44].

Nevertheless, cyberterrorism does not significantly undermine confidence in the national government or its institutions any more than conventional terrorism does. This was evident from our confidence measures comparing a control group to those exposed to depictions of conventional and cyberterrorism. As noted at the head of this article, such broad measures of confidence are not always affected by terrorism or other traumatic events. On the contrary, such events often strengthen public confidence as occurred in the USA post 9/11 [11, 9]. These findings about confidence go hand in hand with demands for greater security. As individuals, particularly those with heightened levels of threat perception, demand more government oversight, they cannot express a lack of confidence in the

government without unease. Supporters of intrusive government regulation and surveillance must be confident that the authorities will do their jobs effectively and without abusing the greater authority they now enjoy.

This does not mean governments can remain quiescent. This is true for governments in Israel, whose population was the subject of these studies, and just as important for governments in the USA, Europe and elsewhere. Just as 20th-century studies of the psychology of terrorism in Israel informed post 9/11 research, the effects of cyberterrorism in Israel are equally relevant. Cyberterrorism is a transnational phenomenon and we see that agents like Anonymous are as equally prepared to disrupt American networks (as they did in Ferguson, MO in 2014 [46]) as they are Israeli systems. In fact, the effects of cyberterrorism may prove weaker in Israel than elsewhere as research develops. For Israelis, Hamas is a known quantity, a partner to a long simmering but, to date, manageable conflict that occasionally erupts into sustained violence. To pursue its goals Hamas must publicize its demands and attacks. Attribution is not an issue. For ISIS and the proxies of hostile nations, on the other hand, this is not necessarily true. Attacks are difficult to attribute with certainty and hacktivist demands are often unknown, thereby allowing foreign governments to conduct offensive cyber operations by proxy. Such attacks trade on uncertainty and disruption that may exacerbate anxiety, threat and risk perception in many Western nations to a greater extent than we have seen in Israel.

The outsized risk attributed to threats to life, limb and infrastructure track previous studies that ascribe relatively high levels of risk perception to hazards associated with uncertainty and dread risk, i.e. events 'perceived by lack of control, dread, catastrophic potential and fatal consequences' [27]. Lichtenstein *et al.* [36] describe how media exposure, particularly sensational media coverage, catastrophic outcomes and lack of direct experience skew assessments of risk. To some extent, cyberterrorism fits these models. Although there are only hypothetical lines between cyberattacks and mass casualties, the great risk attributable to infrastructure damage and loss of life and limb might be explained by their possible catastrophic effects, the benefits that they provide (thereby making them a likely target as well as a significant source of concern if threatened), the inability to always identify perpetrators or their motives, and the division of opinion among experts that only exacerbates uncertainty. The role of media coverage remains unstudied but may provide insight into the high risks that many people associate with cyberterrorism. Slovic [60] also reminds us that a kinetic terrorist attack comes with significant 'signal value', the perception that an event will reverberate in the future and generate further death, destruction and mayhem [47]. The result is to overestimate risk. On the other hand, and in contrast to the studies cited, cyberterrorism has never caused death or injury. As such, cyber risk, with is peculiar counterfactual (if we protect ourselves nothing will continue to happen), is likely to be the next frontier of risk perception theory.

Finally, our data suggest that threat perception and not only actual cyber events drive the cognitive effects of cyberterrorism. While individuals demand Internet surveillance and regulation, and forceful military responses to cyberattack following the experimental manipulations, many people are responding to their fears rather than to specific cyber events. In other words, it does not take exposure to actual events to trigger anxiety, rather the perception of threat alone. These results are consistent with studies that document how simply raising and lowering terror threat alerts can increase anxiety and depression and foster a willingness to 'accept both restrictions on their personal freedoms … and violent actions against others' [48]. Here, too, there is no actual attack in the offing, only the fear of an attack. Threat perception, not an actual attack is sufficient to unsettle individuals to the extent many terrorists desire. As a result, authorities will need to recognize that they cannot reduce fears of cyberterrorism and its pervasive effects solely by eliminating cyberattacks that will, quite possibly, only grow more severe. Rather, policymakers must think about ways to enhance resilience in much the way they have in the context of kinetic terrorism and other disasters.

Lessons gleaned from successful (and unsuccessful) efforts to improve disaster preparedness [49–53] suggest that the government, the private sector and the academic community should effectively communicate the risks of cyberterrorism and take steps that will help instill effective cybersecurity practices. Furthermore, if individuals feel they can communicate their concerns to their government and the authorities are attentive (i.e. citizens have a sense of political efficacy) then threat perceptions may be reduced (Canetti *et al.*, unpublished work [54]). These efforts are intertwined. Providing cybersecurity depends, in part, upon securing compliance with cybersecurity measures. Compliance, in turn, depends upon how accurately the public assesses the risk of cyberattacks and upon how successfully government and private agencies communicate cyber risks and the precautions that individuals must take.

To secure computer systems, we draw attention to the many programmes in schools and businesses to impart the knowledge and skills individuals need to maintain personal cybersecurity. Currently, it is our impression that the only evaluation tool is performative, i.e. how well end-users master and adopt the necessary skills to protect their online assets (e.g. recognizing malware, changing passwords, updating firewalls). To fully assess the benefits of these tools, further research is required to understand how these educational and intervention programmes might impart the fear/stress reducing skills to cope with cyberterrorism and to improve resiliency, i.e. withstand adverse psychological effects of cyberterrorism, overcome feelings of vulnerability and regain a sense of control. Experience with kinetic terrorism also points to the benefits of psychological intervention [55]. Mitigating the deleterious effects of cyberterrorism and strengthening resilience may diminish the impact of cyberterrorism and the chance it will spill over into militancy, kinetic war and protracted conflict.

Acknowledgements

This research was made possible, in part, by grants awarded to D.C. from the National Institute of Mental Health (R01 MH073687), from the Israel Science Foundation (594/15) and from the US-Israel Binational Science Foundation (2009460) and to M.L.G. from the Israel Science Foundation (156/13). An earlier version of this article was presented at Stanford University in March 2016 as part of the Cyber Policy Program Workshop on Strategic Uses of Offensive Cyber Operations. We wish to thank Herb Lin who organized the conference and provided valuable input during the early stages of this project and to the conference participants who commented on earlier drafts of this study during the workshop.

References

1. Sinclair SJ, Antonius D. *The Political Psychology of Terrorism Fears*. Oxford: Oxford University Press, 2013.
2. Luft B. *We're not Leaving: 9/11 Responders Tell Their Stories of Courage, Sacrifice, and Renewal*. New York: Greenpoint Press, 2011.
3. Hobfoll SE, Palmieri PA, Johnson RJ *et al*. Trajectories of resilience, resistance, and distress during ongoing terrorism: the case of Jews and Arabs in Israel. *J Consult Clin Psychol* 2009; 77:138–148.
4. Norris FH, Tracy M, Galea S. Looking for resilience: understanding the longitudinal trajectories of responses to stress. *Soc Sci Med* 2009;**68**:2190–98.

5. De Mesquita EB. Conciliation, counterterrorism, and patterns of terrorist violence. *International Organization* 2005; **59**:145–76.
6. Gross ML. *The Ethics of Insurgency: A Critical Guide to just Guerrilla Warfare*. Cambridge: Cambridge University Press, 2015.
7. Goodrich JN. September 11, 2001 attack on America: a record of the immediate impacts and reactions in the USA travel and tourism industry. *Tourism Manage* 2002;**23**:573–80.
8. Fierke KM. Terrorism and trust in Northern Ireland. *Critic Stud Terror* 2009;**2**:497–511.
9. Gross K, Brewer PR, Aday S. Confidence in government and emotional responses to terrorism after September 11, 2001. *Am Polit Res* 2009;**37**:107–28.
10. Smith TW, Rasinski KA, Toce M. *America Rebounds: A National Study of Public Response to the September 11th Terrorist Attacks*. Chicago, IL: National Opinion Research Center, University of Chicago, 2001.
11. Rasinski KA, Berktold J, Smith TW *et al*. *America Recovers: A Follow-up to a National Study of Public Response to the September 11th Terrorist Attacks*. Chicago, IL: National Opinion Research Center, University of Chicago, 2002.
12. Wollebæk D, Enjolras B, Steen-Johnsen K *et al*. After Utøya: how a high-trust society reacts to terror—trust and civic engagement in the aftermath of July 22. *PS: Polit Sci Politic* 2012;**45**:32–37.
13. Baldwin TE, Ramaprasad A, Samsa ME. Understanding public confidence in government to prevent terrorist attacks. *J Homeland Secur Emerg Manage* 2008;**5**:18–30.
14. Berry MS, Baldwin TE, Samsa ME *et al*. The effect of terrorism on public confidence: an exploratory study. Argonne National Laboratory, ANL/DIS-08/6, 2008.
15. Canetti D, Gross ML, Waismel-Manor I. Immune From Cyber-Fire? The Psychological & Physiological Effects of Cyberwar. In: Allhoff F, Henschke A, and Strawser BJ (eds). *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press, 2016, 157–76.
16. Schmitt, MN (ed). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.
17. Polityuk, P. 2016. Ukraine Sees Russian Hand in Cyber Attacks on Power Grid.Reuters 12 February. http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E
18. Baker R, Blumberg SJ, Brick JM *et al*. Research synthesis AAPOR report on online panels. *Public Opin Quart* 2010;**74**:711–81.
19. Callegaro M, Baker R, Bethlehem J *et al*. (eds). *Online Panel Research: A Data Quality Perspective*. West Sussex, UK: John Wiley and Sons, 2014.
20. Deardon L. Anonymous vows to wreak ′electronic holocaust′ on Israel for ′crimes in the Palestinian territories′. *The Independent*, 31 March 2015.
21. Marteau TM, Bekker H. The development of a Six-Item Short-Form of the State Scale of the Spielberger State—Trait Anxiety Inventory (STAI). *British Journal of Clinical Psychology* 1992;**31**:301–306.
22. Canetti-Nisim D, Ariely G, Halperin E. Life, Pocketbook, or Culture: The Role of Perceived Security Threats in Promoting Exclusionist Political Attitudes towards Minorities in Israel. *Political Research Quarterly* 2008;**61**:90–103.
23. Canetti D, Lindner M. Exposure to political violence and political behavior. In: Reynolds K, Branscombe N (eds), *Psychology of Change: Life Contexts, Experiences, and Identities*. New York: Psychology Press, 2014, 77–94.
24. Raijman R, Semyonov M. Perceived threat and exclusionary attitudes towards foreign workers in Israel. *Ethnic Racial Stud* 2004;**27**:780–99.
25. Hobfoll SE, Canetti-Nisim D, Johnson RJ *et al*. The association of exposure, risk, and resiliency factors with PTSD among Jews and Arabs exposed to repeated acts of terrorism in Israel. *J Trauma Stress* 2008;**21**:9–21.
26. Huddy L, Feldman S, Capelos T *et al*. The consequences of terrorism: disentangling the effects of personal and national threat. *Polit Psychol* 2002;**23**:485–509.
27. Slovic P. Perception of risk. *Science* 1987;**236**:280–85.
28. Davis DW, Silver BD. Civil liberties vs. security: public opinion in the context of the terrorist attacks on America. *Am J Polit Sci* 2004;**48**:28–46.
29. Echebarria-Echabe A, Fernández-Guede E. Effects of terrorism on attitudes and ideological orientation. *Eur J Social Psychol* 2006;**36**:259–65.
30. Getmansky A, Zeitzoff T. Terrorism and Voting: the effect of rocket threat on voting in Israeli elections. *Am Polit Sci Rev* 2014;**108**:588–604.
31. Lerner JS, Gonzalez RM, Small DA *et al*. Effects of fear and anger on perceived risks of terrorism a national field experiment. *Psychol Sci* 2003;**14**:144–50.
32. PEW *American's Privacy Strategies Post Snowden*, 2015 http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf
33. Libicki, C. From the Tallinn Manual to Las Vegas rules. In: *Cyberspace in Peace and War.* Annapolis MD: Naval Institute Press, 2016, chapter 32, forthcoming.
34. Farell H, Glaser CL. An effects-based approach to escalation and deterrence in cyberspace. In: *Stanford Cyber Policy Program Workshop on Strategic Uses of Offensive Cyber Operations.* Stanford, CA: Stanford University, March 3-4, 2016.
35. Lucas GR. State sponsored hacktivism. In: Gross ML, Meisels T. (eds), *Soft War, the Ethics of Unarmed Conflict*. Cambridge: Cambridge University Press, 2017.
36. Lichtenstein S, Slovic P, Fischhoff B *et al*. Judged frequency of lethal events. *J Exp Psychol* 1978;**4**:551–578.
37. Jarvis LS, Macdonald S, Nouri L. The cyberterrorism threat: findings from a survey of researchers. *Stud Conflict Terror* 2014;**37**:68–90.
38. Lewis JA. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, DC: Center for Strategic and International Studies, 2002.
39. Lucas GR. Cyber warfare. In: Johnson JT, Patterson, ED (eds), *The Ashgate Research Companion to Military Ethics*. London: Ashgate, 2015, 245–58.
40. Valeriano B, Maness RC. The coming cyberspace: the normative argument against cyberwarfare. *Foreign Affairs*, 13 May 2015.
41. Bronk C. Getting creative on what will do: cyber espionage, conflict and covert action. In: *Stanford Cyber Policy Program Workshop on Strategic Uses of Offensive Cyber Operations*. Stanford, CA: Stanford University, March 3-4, 2016.
42. Aucsmith D. Disintermediation, counterinsurgency, and cyber defense. In: *Stanford Cyber Policy Program Workshop on Strategic Uses of Offensive Cyber Operations*. Stanford, CA: Stanford University, March 3–4, 2016.
43. Gartzke E, Lindsay J. Cyberwar in a thermonuclear world. *Stanford Cyber Policy Program Workshop on Strategic Uses of Offensive Cyber Operations*. Stanford, CA: Stanford University, March 3-4, 2016.
44. Gross ML, Canetti D, Vashdi DR. The psychological effects of cyber terrorism. *Bull Atom Sci* 2016;**72**:284–91.
45. Gross K, Brewer PR, Aday S. Confidence in government and emotional responses to terrorism after September 11, 2001. *American Politics Research* 2009;**37**:107–28.
46. Kerr D, Ferguson M. Police site hit with DDoS attack. *CNET*, 15 August 2014.
47. Jenkin CM. Risk perception and terrorism: applying the psychometric paradigm. *Homeland Secur Affair* 2006;**ii**:1–14.
48. McDermott R, Zimbardo PG. The psychological consequences of terrorist alerts. In: Bongar B, Brown LM, Beutler LE *et al*. (eds), *Psychology of Terrorism*. Oxford: Oxford University Press, 2007, 357–70.
49. Barry MM, Sixsmith J, Infanti JJ. *A Literature Review on Effective Risk Communication for the Prevention and Control of Communicable Diseases in Europe*. Stockholm: ECDC, 2013.
50. Basolo V, Steinberg LJ, Burby RJ *et al*. The effects of confidence in government and information on perceived and actual preparedness for disasters. *Environment and Behavior* 2008;**43**:338–64.
51. Gray GM, Ropeik DP. Dealing with the dangers of fear: the role of risk communication. *Health Affair* 2002;**21**:106–16.
52. Fischhoff B, Gonzalez RM, Small DA *et al*. Evaluating the success of terror risk communications. *Biosecur Bioterror* 2003;**1**:255–58.
53. Wood MM, Mileti DS, Kano M *et al*. Communicating actionable risk for terrorism and other hazards. *Risk Anal* 2012;**32**:601–15.
54. Canetti D, Navot D, Vashdi D *et al*. Political resources effect? Evidence from a longitudinal study on exposure to violence and psychological distress in Israel (unpublished manuscript).

55. Canetti D, Hall BJ, Rapaport C *et al*. Exposure to terrorism and political extremism: a stress-based process. *Eur Psychol* 2013;**18**:263–72.
56. Canetti-Nisim D, Halperin E, Sharvit K *et al*. A new stress-based model of political extremism personal exposure to terrorism, psychological distress, and exclusionist political attitudes. *J Confl Resolut* 2009;**53**:363–89.
57. Hirsch-Hoefler S, Canetti D, Rapaport C *et al*. Conflict will harden your heart: exposure to violence, psychological distress and peace barriers in Israel and Palestine. *Brit J Polit Sci* 2014;**44**:1–15.
58. Huddy L, Feldman S. Americans respond politically to 9/11: understanding the impact of the terrorist attacks and their aftermath. *Am Psychol* 2011;**66**:455–67.
59. Rubin GJ, Brewin CR, Greenberg N *et al*. Enduring consequences of terrorism: 7-month follow-up survey of reactions to the bombings in London on 7 July 2005. *Brit J Psychiat* 2007;**190**:350–56.
60. Slovic P. The perception of risk. In: Sternberg RJ, Fiske ST, Foss DJ (eds), *Scientists Making a Difference*, Cambridge: Cambridge University Press, 2016, 179–82.