HHS Public Access

Author manuscript

Bull At Sci. Author manuscript; available in PMC 2017 August 04.

Published in final edited form as:

Bull At Sci. 2016 ; 72(5): 284–291. doi:10.1080/00963402.2016.1216502.

The psychological effects of cyber terrorism

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

Abstract

When ordinary citizens think of cyber threats, most are probably worried about their passwords and banking details, not a terrorist attack. The thought of a shooting in a mall or a bombing at an airport is probably more frightening than a cyber breach. Yet terrorists aim for mental as well as physical destruction, and our research has found that, depending on who the attackers and the victims are, the psychological effects of cyber threats can rival those of traditional terrorism.

Keywords

cyber security; cyber terrorism

Cyber aggression has become a daily fact of life in the 21st century, yet for most people it's still only a reality in the form of cyber crime—hackers targeting financial information or other personal details. Politically motivated attacks might threaten them as well, but they tend to be the concern of governments and corporations rather than ordinary citizens. The thought of a terrorist shooting in a mall or bombing in an airport probably seems far more frightening to the average person than Russian hackers disrupting government networks in Estonia or Anonymous breaking into the police department of Ferguson, Missouri. Cyber terrorists, after all, have yet to actually kill or injure anyone. Yet our research has found this perception of cyber aggression might not be entirely accurate. The aim of terrorism, after all, is not just physical destruction, and depending on who the attackers and the victims are, the psychological effects of cyber terrorism can be just as powerful as the real thing.

Defining cyber terrorism

People face cyber aggression on an almost daily basis. Hackers appropriate, erase, or ransom data, defraud bank customers, steal identities, or plant malevolent viruses. In many cases, hackers are criminals out for pecuniary gain. But sometimes their motives are political. Some are "hacktivists," or cyber activist groups, like Anonymous, others are terror groups like Hamas or Islamic State, and still others are agents of national states like Iran, North Korea, or Russia. They are not usually after money but pursue a political agenda to foment for social change, gain political concessions, or cripple an enemy. Sometimes their means are peaceful but other times they are vicious and violent. The lines often blur. Anonymous will hack the Ferguson police department just as it will initiate an "electronic Holocaust"

Corresponding author: Michael Gross < mgross@poli.haifa.ac.il>.

Disclosure statement

No potential conflict of interest was reported by the authors.

against Israel in support of the Palestinian cause (Rogers 2014). Islamic activists will not only use the Internet to recruit members and raise funds for social welfare projects but also to steal money for terrorist activities or disseminate information to stoke fear and demoralize a civilian population. States will pursue online espionage but also wreak havoc by crashing multiple systems—as did the Russians, allegedly, in Estonia in 2007, with mass denial-of-service attacks on government sites, and in Ukraine in 2016, with cyber attacks on the airport and power grid (Polityuk 2016).

Underlying many of these attacks is terrorism: an attempt to extract political concessions by instilling fear in the civilian population. In this way, cyber terrorism is no different from conventional terrorism. Yet cyber terrorism is far more subtle. To date, cyber terrorists have neither killed nor injured anyone. Nor have cyber terrorists successfully destroyed any critical infrastructures. Whether this is due to the offensive inadequacies of the terrorists or the superior defensive capabilities of the United States and its allies, experts have yet to decide.

But as the war on cyber terrorism continues, it is increasingly clear that protecting vital national interests is only half the battle. Security experts rightly worry about defending transportation networks, refineries, dams, military installations, hospitals, banks, and government offices from cyber attack just as they worry about defending the same facilities from terrorist bombs or ballistic missiles (Lewis 2002). Yet lost in the haze of cyber warfare is the human dimension. While scholars and policy makers raise concerns about the dangers that cyber terrorism holds for national security, we know little about its effects on human security.

Human security emphasizes the conditions necessary for a vibrant civil society (Tadjbakhsh 2014). At the most basic level, people must be able to live free of undue fear, anxiety, and trepidation. At a more developed level, civil society requires energetic public discourse, judicious public policy, and respect for human dignity. Following 9/11, we now recognize that conventional terrorism undermines human security even more than national security. It is a common truism that terrorists want a lot of people watching, not a lot of people dead (Jenkins 1975; Lerner et al. 2003). The dead are few; it is the living whose daily lives are transformed by the constant fear of impending doom. Conventional terrorism exacerbates feelings of insecurity and perceptions of threat that prompt public cries for protective and militant government policies that can short-circuit public discourse, intensify intolerance for dissident views, and infringe on human rights (Boggs 2002; Hirsch-Hoefler et al., 2014). Does cyber terrorism cause similar effects?

At first glance, it seems that it cannot. In their attempts to formulate the law of cyber warfare, the framers of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* remain unconvinced that cyber attacks that block e-mail, deny service, employ economic coercion, undermine confidence in the government or economy, or, in their example, “cause panic by falsely indicating that a highly contagious and deadly disease is spreading through the population” cause sufficient mental suffering to rise to the level of a terrorist attack (Schmitt 2013, §11.2, 3; 30.12; 36.3; 59.9). Unfortunately, these assumptions are untested and in a series of field experiments we studied how cyber terrorism affects

psychological well-being and political attitudes that impinge upon human security by causing stress, anxiety, and fear—all of which radicalize political attitudes and push people to exchange privacy for security to prevent cyber terror in the future.

Simulating cyber terrorism

In our field survey experiments, we first interviewed 522 individuals following Anonymous's well-publicized attempt to perpetrate an "electronic Holocaust" in April 2015, when the hacktivist group promised to take down servers and "erase Israel from cyber space." In a second study, in January 2016, 907 subjects viewed various film clips describing hypothetical Hamas attacks on Israel's national water company. In one scenario, cyber terrorism was fatal; terrorists poisoned the water supply with an overdose of chlorine that killed two and injured many more. In other scenarios, cyber terrorism was not lethal; no one suffered physical harm but hackers appropriated the bank account numbers of the company's customers and successfully transferred money to Hamas. A third group of subjects viewed a fatal but conventional mass-casualty terrorist attack, while a control group viewed a neutral film depicting the dedication of a water treatment plant. Following these screenings, we surveyed respondents on measures fundamental to human security. These included stress, anxiety, insecurity and threat perception, political militancy, and a willingness to relinquish privacy and civil liberties in favor of security.

In some ways, Israelis are a unique population for such a study. The ongoing conflict between Israelis and Palestinians (and Palestinian allies like Hezbollah and Iran) is a constant feature of everyday life. Terrorism, too, simmers beneath the surface. Since January 2015, terrorists have taken 23 civilian lives in Israel. Yet Israelis know their enemy, know what they want and can imagine the way to peace. This puts terrorism and cyber terrorism in the context of a political struggle that has, in many ways, fixed and acceptable costs. Like a couple of wary boxers, each side circles the other, constantly poking and provoking. This leaves Israelis, who score very high on the UN's world happiness index, weary but resilient.

In contrast, the West's confrontation with radical Islam is enigmatic and exceptionally violent. In the same period since the start of last year, 67 Americans and 197 Europeans have lost their lives in terrorist attacks. Unlike Israelis, Americans and Europeans don't know their enemy, have no clear idea what they want or how to confront their demands. Islamic State attacks are brutally violent for their own sake. Americans and especially Europeans will find resilience elusive as terrorism and cyber terrorism fuel an inescapable cycle of fear. Learning from the Israeli case and understanding the effects of cyber terrorism for other Western nations is crucially important.

Measuring stress and insecurity

Not surprisingly, exposure to cyber terrorism is stressful. Figure 1 uses the State-Trait Anxiety Inventory (STAI) to show how stress and anxiety grow as attacks become more deadly. With a score of 4.00, conventional mass-casualty terrorism (e.g., suicide bombings) evokes a level of anxiety at the top of the scale. The stress scores for lethal and non-lethal cyber terrorism are not far behind, and all the scores significantly surpass the control group.

But the interesting point is this: Individuals were equally disturbed by lethal and non-lethal cyber terrorism, meaning there is no significant difference between the two when it comes to stress. Both cause significant panic and anxiety and both, it seems, are equally capable of cracking the foundations of personal wellbeing and human security.

Cyber terrorism also left individuals insecure and wary of future cyber terrorist attacks. These judgments are measures of threat perception and gauged by such questions as: “To what extent do cyber attacks undermine your sense of personal security?” and “To what extent do you feel threatened by cyber terrorism?” Like stress, threat perception increased steadily as attacks grew more severe (Figure 2). But even in our control group, Israelis are on edge and exposure to non-lethal cyber terrorism did not appreciably increase perceptions of threat. Lethal attacks, on the other hand, did trigger a significant jump in threat perception and it didn’t matter much whether they were cyber or conventional terrorist attacks. These findings show how stress and threat perception are two different phenomena. Stress is emotional while threat perception is cognitive. And while lethal *and* non-lethal cyber attacks evoke feelings of stress, only terrorism accompanied by injury and loss of life nurtures a serious preoccupation about the next attack. If a person’s reaction to cyber terrorism has both an emotional and cognitive dimension, it is also sensitive to circumstance and the identity of the perpetrator. After it was clear that Anonymous’s threat of an “electronic Holocaust” was empty, threat perception fell by 10 percent. People were still fearful, but not so much. But many Israelis do fear Hamas. and when that group, rather than Anonymous, was the perpetrator, threat perceptions increased by 20 percent, from a mean score of 2.9 to a score of 3.5. Hamas is a far more frightening adversary than Anonymous, even as they perpetrate similar attacks.

Stress, anxiety, insecurity, and perceptions of threat do not stand alone. Instead, we know that studies of conventional terrorism show how stress, anxiety, and heightened perceptions of threat radicalize political attitudes and draw individuals away from concerns about civil liberties to worries about national security (Verton and Brownlow 2003). In the wake of mass-casualty terrorism, individuals turn inward, disparage outgroups, move to the right on security and privacy issues, and call upon their government to take strong military action (Canetti et al. 2013; McDermott 2010). The effects can have a chilling effect on civil society and political discourse in many democratic nations, as debates about torture, rendition, due process, military belligerency, and surveillance show. We were not surprised to see similar effects from cyber terrorism.

Political reactions

Figures 3 and 4 depict an array of political attitudes that harden in the wake of terrorism. As noted, individuals in our first survey confronted an ongoing cyber attack by Anonymous and in the second, a simulated attack by Hamas. In each case, we asked individuals about their support for internet surveillance, government regulation, and military retaliation in the context of an unspecified cyber terror attack. Questions centered on surveillance and civil liberties (“Should the government monitor emails and social networks for suspicious phrases?”; “Are you willing to let the government read emails to improve personal and national security?”),[1] government regulation (“Should the government require businesses to

install cyber security systems?"), and military retaliation ("Following a cyber terrorism attack, should the government respond with a small-scale cyber attack against military targets, a large-scale cyber attack against military and civilian targets, a small-scale conventional (missiles, bombs, and artillery) attack against military targets, or a large-scale conventional attack attacks against military and civilian targets?")

Attitudes varied depending on the perpetrator. When Anonymous was the attacker, 54 percent of the respondents in our survey would allow the government to monitor e-mails for suspicious phrases, 48 percent would allow the government to monitor Facebook and Twitter, and 23 percent would allow the government to read e-mails. When the perpetrator was Hamas, support for government surveillance leaps to 67 percent in favor of monitoring e-mails, 46 percent in favor of monitoring social media, and 61 percent in favor of reading e-mails. Among Americans in general, by contrast, only 43% of the respondents would allow the US government to monitor the communications of US citizens (Shelton et al. 2015, 6). Among Israelis, support for surveillance depends on the identity of the perpetrator. And while the identity of the attacker did not affect calls for government regulation (74 percent of the respondents would require business to install cyber security software) fears of Islamic terrorism dominate the public's demand for military responses. As Figure 4 demonstrates, individuals facing Hamas terrorism were considerably more militant and supported conventional retaliation by a margin of nearly 2:1 compared to those facing the hacktivist group Anonymous. One reason may be greater fear of Hamas but another may be the recognition that Hamas, like Islamic State, has infrastructures and territory vulnerable to conventional attack. On the other hand, it is fear of Hamas rather than its vulnerability that drives greater support for surveillance. These data highlight the public's willingness to employ conventional military measures to quash cyber terrorism, strong attitudes that will no doubt influence political leaders as they weigh kinetic military responses to cyber threats (Libicki 2014).

From a psychological perspective, the data offer a curious finding. We expected to find a clear connection between exposure to cyber terrorism and militant, hardline attitudes. The harsher the terrorist attack our subjects experienced, the greater their militancy. But this is not what we discovered. Instead, we found that the greater one's *perception of threat*, the greater one's militancy. The odds were more than twice as high that individuals with high levels of threat perception will support surveillance, government regulation, and military retaliation compared to those whose threat perception is lower. We cannot explain why some individuals are more fearful than others. Past exposure to cyber attacks explains only a small part of the variance. Other personality factors, beyond the scope of our study to examine, are also probably at work. Nevertheless, it is clear that the threat of terrorism and how one perceives it are better determinants of militancy and hardline attitudes than the experience of an actual attack. And, indeed, this is how terrorism works. One need not suffer direct harm to be terrorized; it is enough that one *fear* direct harm to suffer the ravages of contemporary terrorism, whether cyber terrorism or conventional terrorism.

[1]"Reading" and "monitoring" are different. "Monitoring" suggests either the collection of metadata or only reading e-mails that trigger security concerns, while "reading" suggest scrutinizing every e-mail.

From Anonymous and Hamas to Islamic State

These results offer tantalizing evidence that cyber terrorism mirrors conventional terrorism even when its victims do not suffer injury or loss of life. We found that cyber terrorism increases stress, anxiety, fear, hardline attitudes, and political militancy. But circumstances matter, because the identity of the perpetrator helps explain the political attitudes related to cyber terrorism. Hamas is more threatening than Anonymous. When Hamas is at the wheel, Israelis see a brutal terrorist organization and do not much distinguish between cyber and conventional terrorism. Anonymous, on the other hand, still carries some cachet as a rogue hacktivist group that is unwilling or unable to harm anyone physically. Hamas, for the most part, poses no threat to Americans and Europeans. But Islamic State certainly does, and it will not be long before the group gains the capabilities to mount cyber-terrorism attacks. And, as with Hamas, the fact that these attacks might cause little physical harm may be irrelevant. Islamic State, like Hamas, will trade on its ruthless terrorist image. Leveraging its success at conventional terrorism, it will move seamlessly and effectively to cyber terrorism to produce outsized fear and panic. Marrying conventional and cyber terrorism will have chilling effects: Islamic State and other terrorist groups will be able to achieve the dramatic effects of suicide attacks and mass casualties at the relatively low cost and risk of cyber terrorism. There will be no need for suicide cyber bombers. Cyber terrorism is a force multiplier that can magnify the effects of limited, sporadic, and even failed kinetic terrorist attacks. In tandem, conventional and cyber terrorism can undermine human security in a most fundamental way.

Restoring human security

Human security thrives when societies are open, tolerant, peaceful, and vibrant, and when they offer citizens the conditions necessary to flourish economically, intellectually, physically, and emotionally (Tadjbakhsh and Chanoy 2007). Physical security is a necessary condition for human security but not sufficient if civil society fails to allow its members to thrive. To thrive, individuals must maintain tolerance and social discourse. By inducing stress and anxiety, cyber terrorism endangers psychological wellbeing and increases perceptions of threat even if individuals suffer no physical harm. Once cyber terrorism successfully breaches a critical infrastructure to kill and injure (as in our film clips), these effects are more pronounced. Threat perception is not all bad. Reasonable perceptions of threat are essential to protect individuals and their communities from dangerous surprises but become disabling when they foster insecurity and prompt visions of an inescapable cycle of violence (Canetti-Nisim et al. 2009). It is the nature of cyber terrorism to target civilians (Gross 2015, 153–183). Some of this is mere efficiency: Civilian targets are softer than military targets or critical infrastructures, which states take great pains to protect. But part is strategic: Targeting civilians is a way to demoralize and terrorize. This is precisely what Anonymous, Hamas, and Islamic State promise to do.

In response, civilians are increasingly willing to jettison privacy and support military retaliation. Neither outcome bodes well for human security. Privacy embraces the right to keep secrets and preserves a domain for individuals to build their personal identities and communicate without interference or duress. Surveillance inhibits free speech, discourages

political opposition, prevents dissenters from organizing or publishing anonymously, and disrupts the flow of information necessary for a well-functioning civil society. Surveillance threatens privacy but not without cause. Surveillance can strengthen physical security. Gaining access to the content of e-mails and social media may allow law enforcement authorities and intelligence agencies to co-opt and cripple hostile organizations. Physical security is as important for human security as privacy. Balancing the two will be exceptionally challenging in the shadow of cyber terrorism, and cyber security experts and policy makers cannot unilaterally fortify the former at the expense of the latter.

Political militancy is equally problematic. Facing cyber terrorism and the threat it poses to national and human security, governments consider a range of tempered policies that include criminal prosecution, counter espionage, and active cyber defenses. Because most offensive cyber attacks fall far short of war, each of these retaliatory responses is freighted with fears of escalation that the United States and other nations wish to avoid. Nations must be careful as they weigh their responses to hostile cyber operations (Hathaway et al. 2012). Civilians, particularly those who already find themselves in the midst of an armed conflict, are less restrained and may push their governments in unwarranted and dangerous directions as they call for harsh military retaliation following cyber attacks. Human security does not demand pacifism but it thrives best in a society that is cautious about the use of armed force. Cyber terrorism, like conventional terrorism, upends judicious decision making.

Eliminating the toxic effects of cyber terrorism is not simply a matter of cyber security. It is not enough to thwart or reduce the incidence of cyber-terror attacks. Protecting facilities is only half the battle. Fear, insecurity, anxiety, and militancy are often the product of perceived, not actual, threats. Cyber terrorists lurk in the background, and individuals will not be mollified unless they are eliminated. Despite their best efforts, however, no government will ever eradicate cyber terrorism, and people will always be driven by their outsized fears. Mitigating these fears is as equally important as reducing the incidence of attack. But the means are entirely different. Perceptions depend crucially on information and, as a result, risk assessment and communication are of crucial importance is the war against cyber terrorism. Individuals who misunderstand the nature of cyber terrorism and the threat it poses are most likely inclined to greater fear, insecurity, and militancy than those whose assessment is sober. Experts, to be sure, remain divided over the risk of cyber terrorism. Nevertheless, the cyber security community must address the fears of everyday citizens by cogently assessing the danger of cyber terrorism and the protective measures necessary to maintain secure networks. Risk communication is sorely lacking; properly implemented, it can reduce insecurity and perceptions of threat. Finally, there is also room to think about psychological intervention and cognitive behavior therapy to treat cyber terrorism–induced anxieties, just as it is used to treat the effects of conventional terrorism.[2] Risk assessment and psychological treatment protocols address the human dimension of cyber terrorism and should not be neglected as nations work to fend off cyber terrorists of all stripes.

[2]For example, see Somer et al. 2005.

Cyber terrorism has many faces, as does the psychology of the masses. Our research demonstrates how even non-lethal, seemingly banal forms of cyber terrorism have a considerable impact on the attitudes of victimized populations. Our experiments show a "cyber terrorism effect" that enables terrorists to foster fears akin to kinetic terrorism and pursue similarly ideological goals. In this way, cyber terrorism pushes well beyond cyber crime even when its methods—identity theft, destruction of data, and disruption of service—are sometimes similar. When Anonymous threatens an electronic Holocaust by corrupting data or stealing identities, they are taking sides in violent, armed conflict, and their actions are far more than criminal. They are attacking innocent civilians, not bilking an easy mark. Victims know the difference. Under attack, they react with not only fear and trepidation, as do victims of crime, but with demands for protection from the enemies of the state via harsh military retaliation, surveillance, and strong government. This is the psychology of terrorism.

Acknowledgments

Funding

This research was made possible, in part, by grants awarded to Daphna Canetti from the US 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 Michael L. Gross from the Israel Science Foundation (156/13).

Biographies

Michael L. Gross is a professor in and the head of the School of Political Science at the University of Haifa, Israel. His recent books include *The Ethics of Insurgency* (Cambridge 2015) and *Moral Dilemmas of Modern War* (Cambridge 2010).

Daphna Canetti is a professor of political science at the University of Haifa and the director of the university's graduate program in Democracy Studies. Canetti's research examines the psychological challenges and policy implications of terrorism, warfare, and political violence. Her publications appear in political and psychological outlets including the *Lancet*, the *American Journal of Political Science*, the *British Journal of Political Science*, and *Political Psychology*. Her commentary has been featured in media outlets including NPR and the *Washington Post*.

Dana Vashdi is the head of the Division of Public Administration and Policy at the University of Haifa, Israel. Her research focuses on the well-being of citizens in general and of employees in particular as well as on teams in public organizations, organizational learning, and healthcare policy. She has published articles in a wide variety of academic journals including the *Academy of Management Journal*, the *British Medical Journal, Human Resource Management*, and *Public Administration Review*.

References

Boggs C. Militarism and Terrorism: The Deadly Cycle. Democracy & Nature. 2002; 8(2):241–259.

Canetti-Nisim D, Halperin E, Sharvit K, Hobfoll SE. A New Stress-Based Model of Political Extremism Personal Exposure to Terrorism, Psychological Distress, and Exclusionist Political Attitudes. Journal of Conflict Resolution. 2009; 53(3):363–389. [PubMed: 22140275]

Canetti D, Hall BJ, Rapaport C, Wayne C. Exposure to political violence and political extremism: A stress-based process. European Psychologist. 2013; 18(4):263.

Gross, M. The Ethics of Insurgency: A Critical Guide to Just Guerrilla Warfare. Cambridge: Cambridge University Press; 2015.

Hathaway OA, Crootof R, Levitz P, Nix H, Nowlan A, Perdue W, Spiegel J. The Law of Cyber-Attack. California Law Review. 2012; 100(4):817–885.

Hirsch-Hoefler S, Canetti D, Rapaport C, Hobfoll SE. Conflict will harden your heart: Exposure to violence, psychological distress and peace barriers in Israel and Palestine. British Journal of Political Science. 2014:1–15.

Jenkins, BM. Will terrorists go nuclear?. Santa Monica, CA: The RAND Corporation; 1975. (P-5541 in the RAND Paper Series)

Lerner JS, Gonzalez RM, Small DA, Fischhoff B. Effects of fear and anger on perceived risks of terrorism: A national field experiment. Psychological Science. 2003; 14(2):144–150. [PubMed: 12661676]

Lewis JA. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies. 2002 Dec.

Libicki, MC. Cyberspace in Peace and War. Vol. Chap. 32. Annapolis, MD: Naval Institute Press; 2014. From the Tallinn Manual to Las Vegas rules. 2016 (forthcoming)

McDermott, R. Proceedings of a Workshop Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, National Research Council. Washington, DC: The National Academies Press; 2010. Decision Making under Uncertainty; p. 227-241.

Polityuk P. Ukraine Sees Russian Hand in Cyber Attacks on Power Grid. Reuters. 2016 Feb 12. http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E.

Schmitt, MN., editor. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press; 2013.

Somer E, Tamir E, Maguen S, Litz BT. Brief cognitive behavioral phone-based intervention targeting anxiety about the threat of an attack: A pilot study. Behaviour Research and Therapy. 2005; 43(5): 669–679. [PubMed: 15865920]

Shelton M, Rainie L, Madden M. Americans' Privacy Strategies Post-Snowden. Pew Research Center. 2015 Mar 15. http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf.

Rogers A. What Anonymous is Doing in Ferguson. Time. 2014 Aug 21. http://time.com/3148925/ferguson-michael-brown-anonymous/.

Tadjbakhsh S. Human security twenty years on. Norwegian Peacebuilding Resource Centre (NOREF). 2014 Jun. http://www.peacebuilding.no/var/ezflow_site/storage/original/application/540cb240aa84ac7133bce008adcde01f.pdf.

Tadjbakhsh, S., Chanoy, AM. Human Security: Concepts and Implications. Abingdon, UK: Routledge; 2007.

Verton, D., Brownlow, J., editors. Black Ice: The Invisible Threat of Cyber-Terrorism. Emeryville, CA: McGraw-Hill/Osborne; 2003.

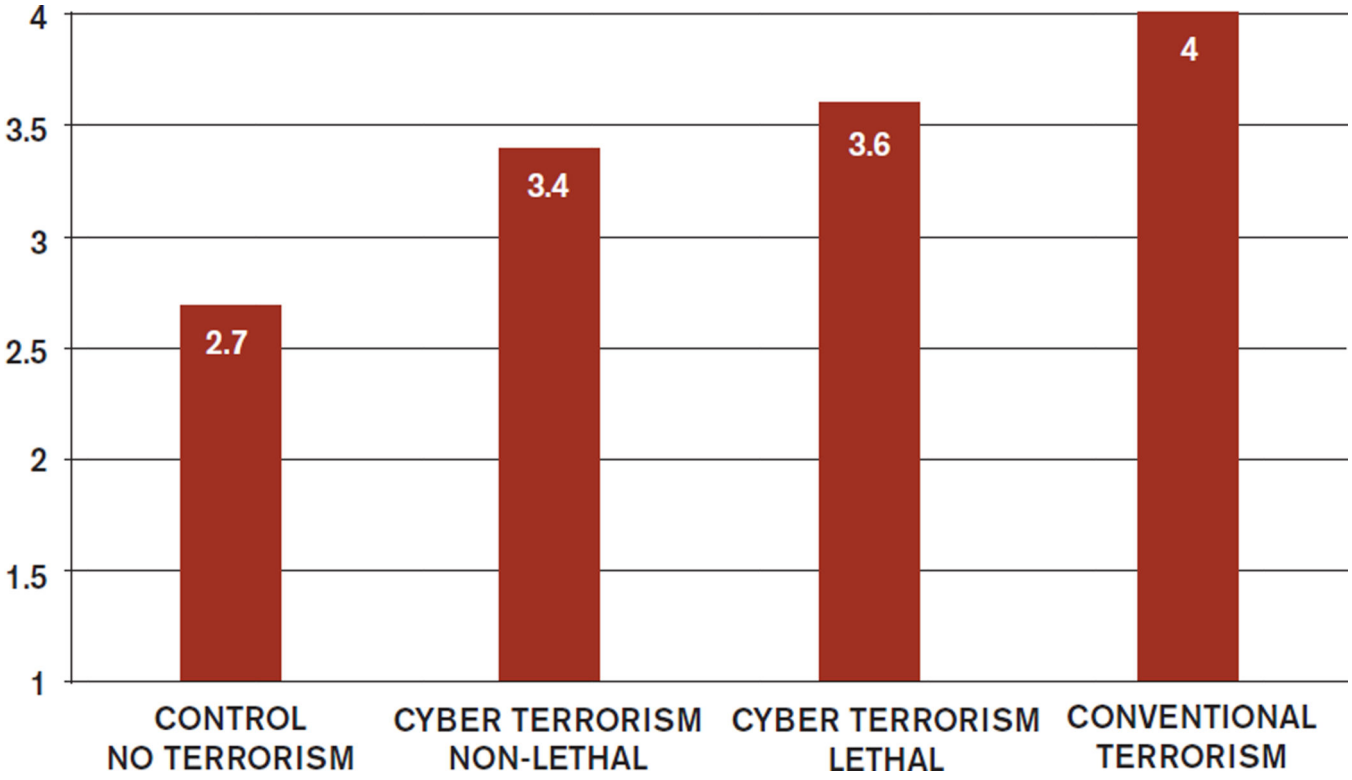

Figure 1.
Anxiety in the Wake of Terrorism

CONTROL: No terrorism

CYBER TERRORISM, NON-LETHAL: Disclosure of account information, loss of funds

CYBER TERRORISM, LETHAL: Deaths and injuries

CONVENTIONAL TERRORISM, LETHAL: Deaths and injuries

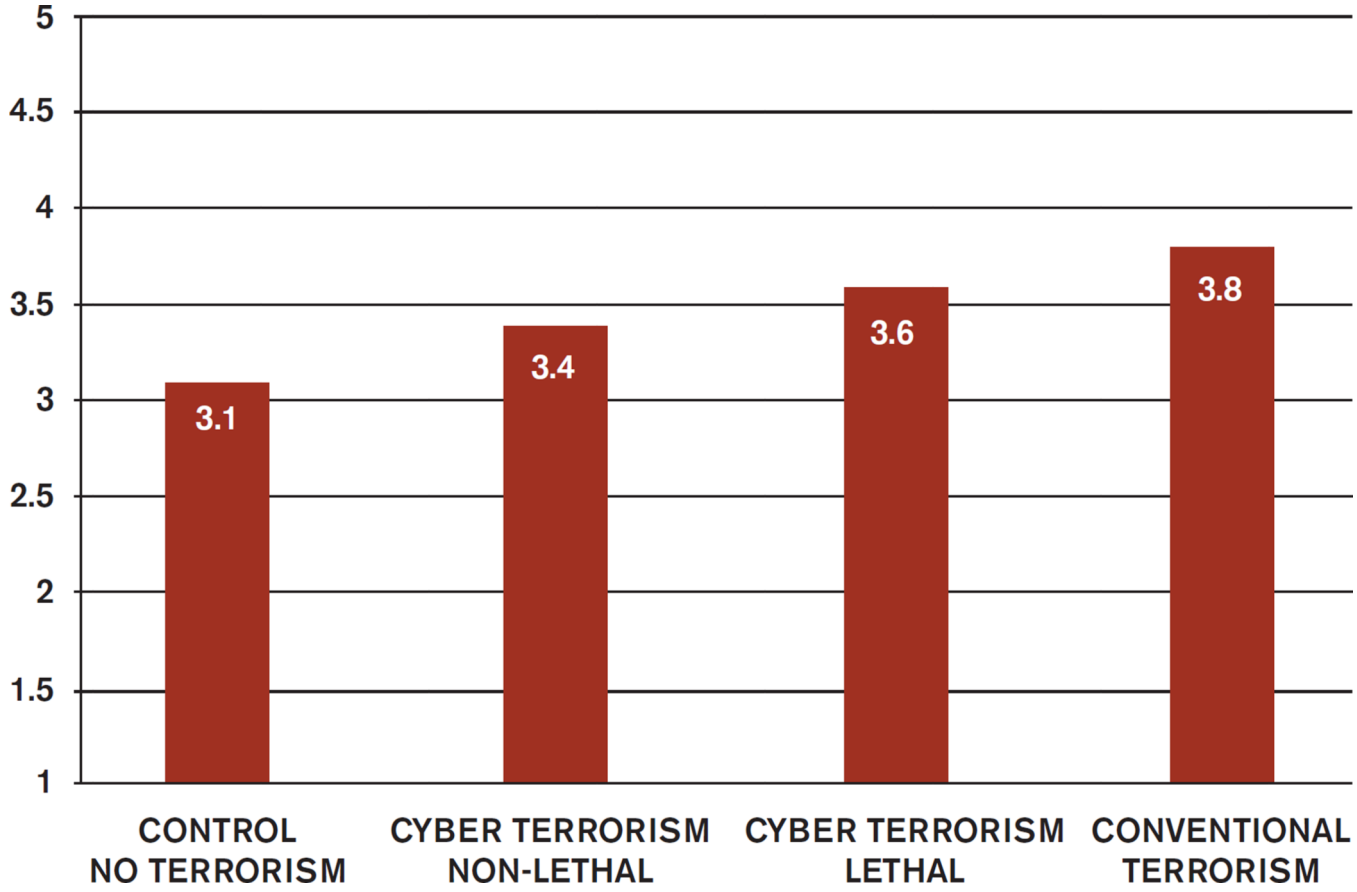

Figure 2.
Threat Perception and Insecurity
CONTROL: No terrorism
CYBER TERRORISM, NON-LETHAL: Disclosure of account information, loss of funds
CYBER TERRORISM, LETHAL: Deaths and injuries
CONVENTIONAL TERRORISM, LETHAL: Deaths and injuries

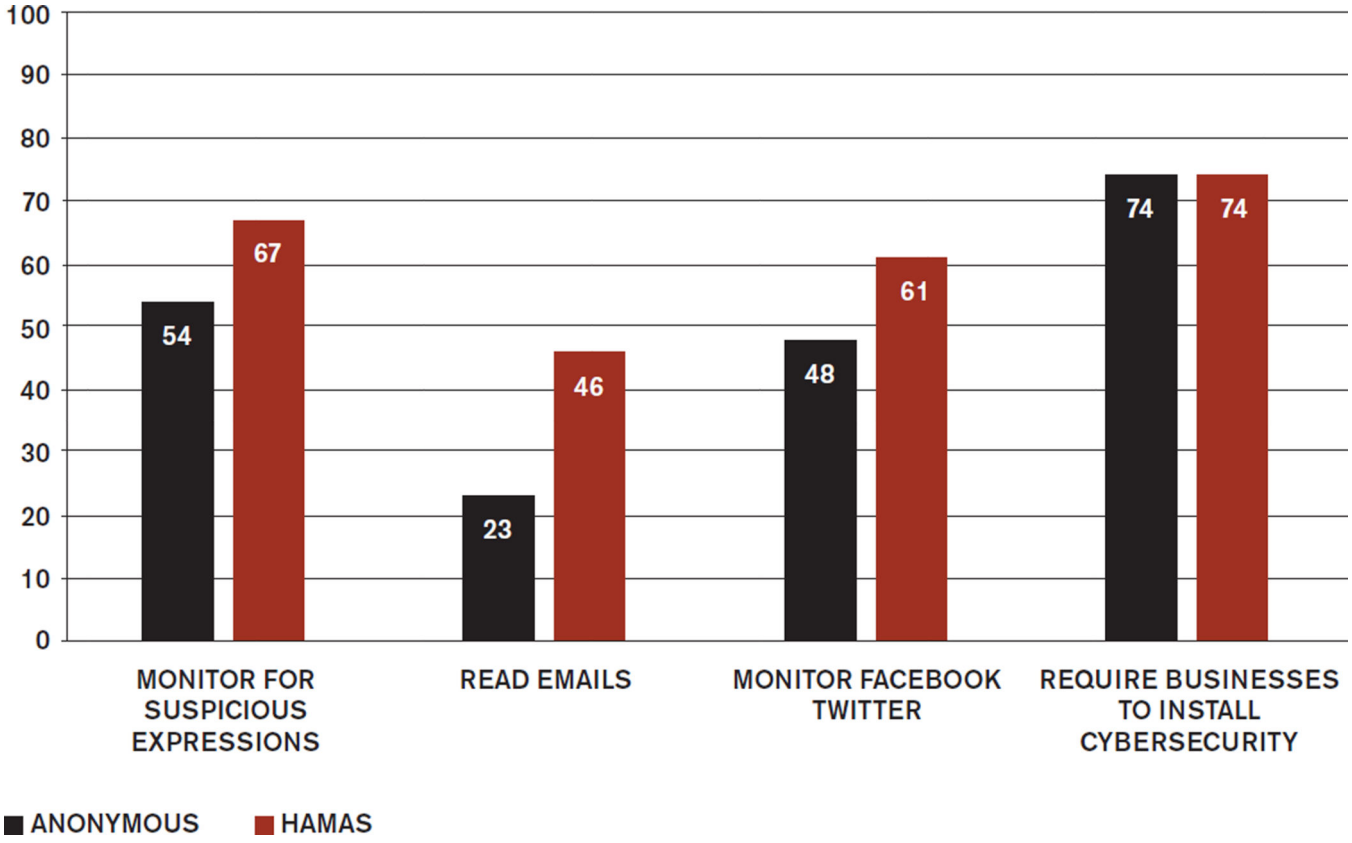

Figure 3.
Percent Favoring Surveillance and Government Regulation

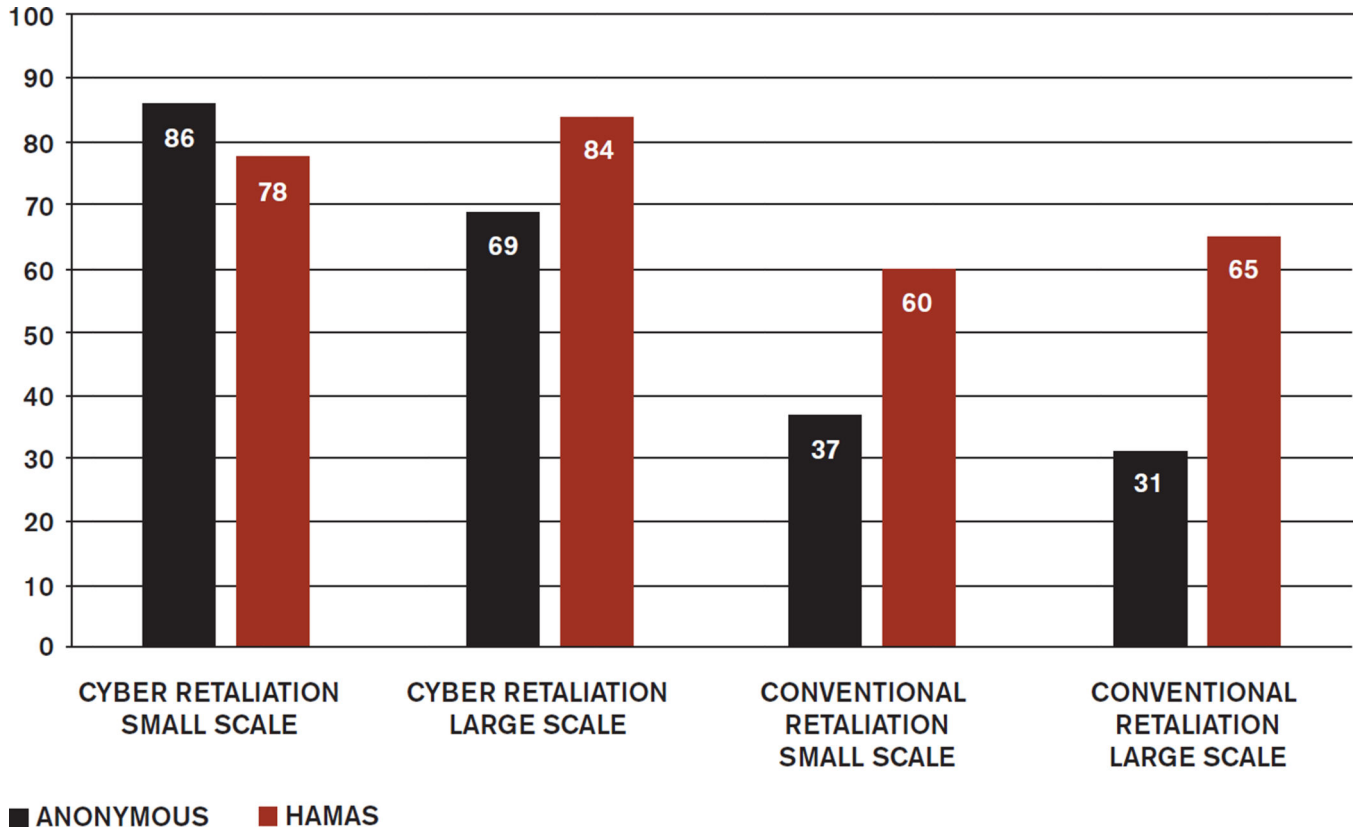

Figure 4.

Percent Favoring Small-Scale and Large-Scale or Conventional Retaliation

CYBER RETALIATION SMALL SCALE: Cyber attacks against military targets

CYBER RETALIATION LARGE SCALE: Cyber attacks against military and civilian targets

CONVENTIONAL RETALIATION SMALL SCALE: Kinetic attacks against military targets

CONVENTIONAL RETALIATION LARGE SCALE: Kinetic attacks against military and civilian targets