CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING
Volume 20, Number 2, 2017

DOI: 10.1089/cyber.2016.0338

ORIGINAL ARTICLE

How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks

Daphna Canetti, PhD,[1,*] Michael Gross, PhD,[1,*] Israel Waismel-Manor, PhD,[1,*]
Asaf Levanon, PhD,[2] and Hagit Cohen, PhD[3]

Abstract

Do cyberattacks fuel the politics of threat? By what mechanism does it do so? To address these questions, we employ a technological and physiological experiment (2×2) involving a simulated cyberattack. Participants were randomly assigned to ''cyberattack'' (treatment) or ''no attack'' (control) conditions. We find that cyberattacks make people more likely to express threat perceptions; we suggest salivary cortisol, a measure of stress, as the mechanism bridging cyber and the politics of threat. Contrary to existing evidence, salivary cortisol is the mechanism that translates simulated exposure to cyberattacks into political threat perceptions.

Keywords: cyberterror, terrorism, threat perception, stress, exposure, cortisol

Introduction

JUST AS 9/11 highlighted the need to understand how exposure to terrorism affects citizens' psychological reactions and sense of threat,[1,2] cyberattacks across the globe call on experimentalists to study their impact. As these attacks grow in frequency, the politics of threat—how threat perceptions impact political attitudes and therefore a state's political reality—and cyber threat in particular, will become an ever more important area of study.[3]

This study is one of the first experimental investigations of cyberattacks based upon a comprehensive psychological model. Moreover, it is, to our knowledge, the first study to examine salivary cortisol as an indicator of stress responses to cyberattacks. Cyberattacks employ malware, viruses, and other forms of computer technology to further political, religious, or ideological goals by harming civilians physically or psychologically. Cyberattackers hope to terrify and demoralize their victims by undermining digital and financial resources and social networks, and/or by threatening physical harm. While there are fears that as cyberattacks grow they will undermine well-being across society,[4,5]

There are *no* experimental designs to substantiate this argument. To investigate the effects of cyberattacks, we exposed subjects to *simulated* cyberterror attacks. Integrating a stress-based model of exposure to terrorism[6] and a biomedical measurement of salivary cortisol to assess stress and related threat perceptions, our findings suggest that individuals exposed to cyberattacks show an increase in cyber-induced stress, which exacerbates perceptions of violent threat and personal insecurity.

Cyberattacks and the Politics of Threat

In the absence of realistic experimental data on the psychological effects of cyberattacks, we turn to cybercrime and kinetic (high explosive) terrorism for analogous data. Victims of identity theft and cyberbullying report moderate or severe emotional distress,[7] indicating a sense of ''moral panic,''[8] anger, fear, anxiety, mistrust, and loss of confidence.[9] The effects of kinetic terrorism include posttraumatic stress, depression, and anticipatory anxiety.[6,10,11] These consequences of kinetic terrorism undermine one's sense of security, increase feelings of vulnerability, foster a threatening worldview, and increase support for hard-line policies.[12,13] Studies demonstrate how individuals exposed to terrorism (9/11 and Oklahoma City bombing, respectively) show significantly greater levels of reactivity, particularly stress, as measured by the stress hormone cortisol, than the nonexposed subjects.[2,14,15]

We expect victims of cyberattacks to respond similarly; subjects exposed to cyberattacks will show greater levels of stress than nonexposed subjects. Although cyberattacks have yet to cause physical harm, fears of future catastrophic cyberattacks multiply. Cyberattacks raise concerns about online safety that spill into the victim's offline physical life

[1]School of Political Science and [2]Department of Sociology and Anthropology, University of Haifa, Haifa, Israel.
[3]Head, anxiety & Stress Research Unit, Division of Psychiatry, Ben-Gurion University of the Negev, Beer-Sheva, Israel.
*These authors contributed equally.

and, indeed, into the life of the community, thereby translating into fears of personal and collective security. Because cyberattacks often occur as an adjunct to protracted conflict, they amplify the stress, insecurity, and perceptions of threat associated with identity theft and cyberbullying. In this environment, we suggest that exposure to a simulated attack will induce stress, as measured by the stress hormone cortisol.[16]

The Cortisol Experiment

We implemented a panel design (a controlled randomized pre–post experiment) to investigate the effect of cyberterror on peoples' perception of cyberthreats in response to cyberattacks and their sense of personal security. We examined cortisol reactivity by exposing participants to stress-eliciting events that directly affect perceptions of security, vulnerability, and threat. A statistical power analysis was conducted to determine the optimal sample size. Because this study is the first to examine the impact of exposure to cyberterror on physiological and psychological responses, we based our calculation on prior studies examining the impact of kinetic terror.[2] Specifically, we assumed a one-sided test with 0.95 power for a comparison of two groups ($M_1 = 0.34$, $SD_1 = 12$; $M_2 = 24$, $SD_2 = 16$), which yielded a minimal sample size of 45 participants per group.

Participants were Jewish students from various fields of study at the humanities and social sciences at a public university in Israel. They were bachelor and masters students, who were offered either extra credit or a small monetary compensation. One hundred and sixteen participants completed the study. As we report in the Supplementary Data (Supplementary Data are available online at www.liebertpub.com/cyber), 16 subjects were excluded because of insufficient saliva samples, resulting in a sample of hundred participants (54 percent female, $M_{age} = 32.3$, $SD = 9.1$). Participants are politically and gender balanced, mostly secular and reporting relatively high levels of income, education, and computer usage, and average levels of computer knowledge.

Although participants were told that the study investigated the impact of social media on Oxytocin, it actually evaluated the psychological and physiological effects of a simulated cyberattack in a fully controlled randomized experiment—that is, pre–post-treatment-control.

Collection of saliva cortisol is a simple, noninvasive, and stress-free procedure that can be accomplished by the volunteers, without the need of paramedical staff. The assessment of cortisol in saliva has recently become a valuable alternative to blood-borne analysis.[17] There is a high correlation between salivary cortisol levels and unbound free cortisol levels in plasma and serum, which remain high during the circadian cycle and under different dynamic tests, such as dexamethasone suppression and ACTH stimulation.[18–20] In addition, cortisol in blood is largely bound to plasma proteins (such as transcortin, cortisol binding globulin, and albumin[21]), whereas saliva cortisol has been shown to be directly correlated with plasma-free (nonprotein bound) cortisol, the biologically active fraction.[22] Since free cortisol represents the biologically active hormone fraction, salivary cortisol measures have early been considered to be a better measure of adrenocortical function than serum cortisol.[23] In light of the above, we feel that salivary measures are the method of choice in stress research, at least for the assessment of free cortisol levels.[24]

Because diurnal cortisol levels decrease considerably in the first few hours after awakening, following prior cortisol studies,[25] we scheduled no sessions in the early morning hours. Furthermore, participants were instructed not to eat or drink, smoke, or chew gum 1 hour before their participation and upon arrival were asked to leave their cell phones on the table on vibrate mode.

To obtain a relaxed neutral environment, participants completed the study in a university faculty office, where only one participant and the research assistant (RA) were present at a time. They were instructed to complete the online survey on the office computer, while the RA sat at the opposite side of the table, working on a second computer. Participants were randomly assigned to either a treatment or a control condition. Following questions about exposure to kinetic terrorism, psychological distress, political trust, and computer use and knowledge, participants in both groups filled a small assay with saliva (pretest measurement).

Upon completion of several attitude and affective questions, only the treatment group was exposed to a multistage cyberattack. The treatment was composed of a sequence of three consecutive cyber threats perpetrated by Anonymous, sequenced at about two-minute intervals from each other. Anonymous is a well-known hacktivist organization whose political agenda includes support for radical political groups, and whose methods include disruption of Internet services, disclosure of confidential information, destruction of property, and an "electronic Holocaust" campaign against Israel.[26] Their avowed purpose, to make Israel "feel fear tingling in their servers"[27] is to terrorize a civilian population. Subjects first saw a pop-up screen with a message from Anonymous (Fig. 1A), announcing an imminent cyberattack against the participant's computer and cell phone ("We don't forget and don't forgive. In a few seconds we will hack your cell phone."). If questioned, the RA told participants to ignore the

FIG. 1. Cyberterror first manipulation **(A)** and second manipulation **(B)**.

message as a ''fluke'' that may happen when working on a public, university computer. After two minutes, a Skype-like screen appeared on the screen where subjects could see themselves live, and see and hear a suspicious-looking person typing (Fig. 1B). Again, the RA reassured the participants that it was a fluke. Finally, following a few more questions, about two minutes later, participants received a personalized anonymous phone text message stating that their personal contacts data had been hacked. Most participants picked up the phone when it vibrated to check the message themselves, however, if they did not, the RA was instructed to tell them following the vibration sound that they can check it out, which they did. At no point did the experimenter admit that the intrusions experienced by subjects in the treatment group had anything to do with the study. In fact, the RA was instructed to say that she has been running this study for weeks, with dozens of participants, and that she never saw anything like it. Participants were asked to disregard the incidents and continue with the study. Control group participants completed the exact same questions, but without the cyberattack component.

Since salivary cortisol reaches its stress-induced peak about 25 minutes after the initial stressor, participants in both conditions were asked to complete a long question battery completely orthogonal to the study, whose sole purpose, unbeknown to participants, was to pass the time. Upon completion of the long battery questionnaire, all participants provided a second saliva sample (posttest measurement) and subsequently answered threat perception and demographic questions. Pursuant to IRB instructions, all participants signed informed consent agreements and were debriefed at the end of the experiment. All participants in the treatment group reported that they were certain the cyberattack was real.

Biochemical measurement

Enzime linked immunosorbent assays (EIA-Diagnostic System Laboratories, Inc., Webster, TX) performed biomedical analysis of free cortisol in saliva using a competitive enzyme-linked immunosorbent assay method in accordance with the manufacturer's instructions. Cortisol assays, stored at −20°C, were performed in duplicate. The intra-assay and interassay coefficients of variation were 3.8 percent and of 5.1 percent, respectively. Sixteen samples were lost due to insufficient sample volume.

Anxiety

Spielberger State-Anxiety Inventory-6 (STAI-6) was used to measure anxiety following the cyberattack[28,29] and asked ''to what extent do you feel stressed/calm/angry/relaxed/satisfied/anxious?'' Each item was reported on a 4-point scale (1-*not at all* to 4-*very much*), both pretreatment and posttreatment (Cronbach's $\alpha = 0.72$ pretreatment and 0.81 posttreatment). Confirmatory factor analysis was conducted separately for pretreatment and posttreatment items. We created a scale for both pretreatment and posttreatment based on the factor score weights and subsequently computed the differences between the two scales (e.g., Supplementary Table S2). Hence, scores on this item represent changes in self-reported anxiety between the premanipulation and postmanipulation measurement.

Perception of cyber threat was measured with the following question: ''To what extent, if any, did cyberattacks on Israel undermine (or harm) your sense of personal security?''

Computer knowledge included four averaged items on a 5-point scale (*poor* to *excellent*) and measured participants' knowledge level with (a) a word processor, (b) browsing the Web, (c) e-mail, and (d) using a search engine (Cronbach's $\alpha = 0.89$).[30] (Supplementary Table S2).

Computer usage included three averaged items on a 5-point scale to (*not at all* to *more than 6 hours*) measure how many hours on a typical day participants (a) surf the Internet, (b) work on a computer, and (c) are connected to social networks (Cronbach's $\alpha = 0.67$)[30] (e.g., Supplementary Table S2).

Sociodemographic variables include gender (1 = female), self-reported income (1 = very low, 5 = very high), education level (two binary variables indicating if the participant has a postsecondary nonacademic education or academic education, with no postsecondary education as the reference category), political orientation (1 = right wing, 5 = left wing), and religiosity (1 = secular, with religious as a reference category).

Results

Before evaluating our hypothesis on the effect of exposure to a cyberattack on cyberthreat perception, cortisol, and

Table 1. Summary Statistics and Variable Descriptions ($N = 100$)

	Control group				*Experimental group*			
Variable name	M	SD	*Min.*	*Max.*	M	SD	*Min.*	*Max.*
Cyber threat	2.6	1.38	1	6	3.24	1.63	1	6
Pre–post cortisol gap	−0.93.68	48.17	−1,993.36	296.5	251.06	429.24	−1,656.93	4,103.71
STAI	−0.04	0.8	−2.55	2.24	0.04	0.79	−1.32	3.29
Computer usage	−0.08	0.94	−1.12	1.8	0.08	0.93	−1.59	1.8
Computer knowledge	−0.09	1.12	−4.18	1.01	0.09	0.78	−2.49	1.01
Gender	0.44				0.64			
Income	4.98	1.15	3	6	4.58	1.18	3	6
Postsecondary nonacademic education	0.16				0.22			
Postsecondary academic Education	0.08				0.12			
Religiosity	0.7				0.68			
Political orientation	3.22	0.84	2	5	3.12	0.82	1	5

STAI, Spielberger State-Anxiety Inventory.

STAI, we present descriptive information regarding the research variables, as well as differences between the control and experimental groups on three main indicators of stress and threat. Table 1, below, presents the descriptive statistics, as well as the *ex-ante* balance checks of our outcome variables and controls, standard demographic indicators, and political orientation. Participants are politically balanced, mostly secular, and report relatively high levels of income, education and computer usage, and average levels of computer knowledge. With respect to gender, the control group had a greater representation of men, while the treatment group had a greater representation of women. As is evident, there is *ex ante* covariate imbalance—an expectation of our model—thus we cannot reject the null hypothesis that there is a difference in means across our baseline data. We address this imbalance by using a propensity score matching treatment effects model in the robustness check section.

Next, we examined differences between the control and experimental groups on three main indicators. The results generally confirmed our expectations. First, cortisol, our biochemical measure, did not differ greatly between the control (M = 1,375.35, SD = 61.04) and treatment group (M = 1,534.85, SD = 64.63) pretreatment (t = 1.794, p = 0.08; Cohen's d: 0.35; 95% CI for the difference = [–335.92, 16.92]), but differed between the control (M = 1,281.65, SD = 56.07) and treatment group (M = 1,785.92, SD = 113.34) posttreatment (t = 3.988, p = 0.001; Cohen's d: 0.79, 95% CI for the difference = [–755.19, –253.31]). Analysis of variance revealed a significant interaction between treatment assignment and pre–post measurement [$F(1, 199) = 4.97$, $p < 0.03$, $\eta^2 = 0.02$], indicating that cortisol levels increased significantly among those exposed to the cyberattack, while decreasing among those who were not.

Second, perceptions of threat were significantly stronger among the experimental group posttreatment (M = 2.6, SD = 1.38) than among the control group (M = 3.24, SD = 1.63) ($t(98) = 2.11$, p = 0.04, Cohen's d: 0.42, 95% CI for the difference = [–1.24, –0.38]). Finally, we did not find any significant differences between the control and treatment groups concerning STAI, our self-reported psychological measure. Specifically, STAI did not differ greatly between the control (M = –0.006, SD = 0.879) and treatment group (M = –0.006, SD = 0.994) pretreatment (t = –0.071, p = 0.52; Cohen's d: 0.01; 95% CI for the difference = [–0.013, 0.187]), and did not also differ between the control (M = –0.04, SD = 0.849) and treatment group (M = 0.04, SD = 1.029) posttreatment (t = 0.432, p = 0.33; Cohen's d: 0.08, 95% CI for the difference = [–0.293, –0.456]). Analysis of variance did not reveal a significant interaction between treatment assignment and pre–post measurement [$F(1, 199) = 0.13$, $p = 0.72$, $\eta^2 = 0.001$].

We employed a seemingly unrelated regression (SUR) model using the structural equation modeling framework available through STATA[31] to examine our main hypothesis that exposure to cyberattack simultaneously affects cortisol, cyberthreat perception, and STAI. The model estimates a series of linear equations (three in our case), while allowing for contemporaneous cross-equation correlation of the errors (i.e., allowing a correlation among the residuals of the three equations). Table 2 presents the path coefficients of all covariates. Turning to predictors of cortisol, Table 2 shows that the difference in the changes of cortisol level between the control and treatment groups holds in a multivariate analysis controlling for demographics and computer knowledge and usage. With respect to the predictors of the perception of cyberthreat, we did not find a significant effect of the experimental manipulation. As seen in Table 2, gender was positively associated with threat perception (95% CI for gender = 0.18, 0.15). Finally, none of the predictors were significantly associated with STAI. We also found that the error terms of the three equations were not significantly correlated (see Supplementary Data).

Discussion

Through a full experiment incorporating treatment and control groups, we demonstrate how even nonviolent forms of cyberattacks have considerable impact on terror threat perception. Exposure to terror can foster a threatening worldview and support for hard-line politics.[13,32,33] Admittedly, because we compared the control group only to one experimental group that experienced exposure to cyberthreat, we cannot disentangle the specific aspects characterizing cyberthreat from the impact of other forms of terror. Hence, our findings serve as exploratory evidence demonstrating that findings on

Table 2. Unstandardized Coefficients from a Seemingly Unrelated Regression Model Predicting Cortisol

	Pre–post cortisol gap			*Cyberthreat*			*STAI gap*		
Predictor	*Coeff.*	*SE*	p	*Coeff.*	*SE*	p	*Coeff.*	*SE*	p
TC	388.30***	–136.53	0.004	0.47	–0.29	0.102	0.05	–0.16	0.766
Computer usage	–37.88	–81.44	0.6	–0.08	–0.17	0.651	0.10	–0.1	0.305
Computer knowledge	–66.75	–82.15	0.4	0.21	–0.17	0.231	0.03	–0.1	0.743
Gender	–32.31	–135.59	0.812	0.96***	–0.29	0.001	0.21	–0.16	0.194
Income	18.42	–57.74	0.75	0.03	–0.12	0.801	–0.00	–0.07	0.999
Postsecondary nonacademic education	–67.98	–176.5	0.7	–0.25	–0.38	0.505	–0.07	–0.21	0.752
Postsecondary academic education	13.42	–223.23	0.952	–0.43	–0.48	0.369	–0.43	–0.26	0.1
Religiosity	119.02	–152.49	0.435	–0.49	–0.32	0.132	–0.15	–0.18	0.389
Political orientation	49.49	–83.87	0.555	0.17	–0.18	0.344	–0.01	–0.1	0.931
Constant	–413.53	–438.42	0.346	1.91*	–0.93	0.041	0.05	–0.52	0.916
R^2		0.08			0.18			0.06	

Note: $rs(\zeta_1, \zeta_2) = -0.097$, 95% CI $[-0.29, 0.09]$; $rs(\zeta_1, \zeta_3) = -0.143$, 95% CI $[-0.33, 0.05]$; $rs(\zeta_2, \zeta_3) = 0.03$, 95% CI $[-0.16, 0.22]$.
*$p < .05$ ***$p < .001$.
TC, treatment-control.

kinetic terror extend also to cyberterror. While victims of cyberattacks may never suffer bodily harm, our findings demonstrate that cortisol levels rose significantly when participants experienced simulated cyberattacks. Moreover, following a simulated cyberattack, even in a laboratory setting where the attacker was Anonymous and not a terrorist group feared for its kinetic and cyberattacks, like ISIS, we find that Israeli civilians were significantly more likely to perceive an imminent cyberthreat and experience feelings of personal insecurity.

Similar to previous studies, we found that cortisol levels rose in response to triggers of stress.[12] Stress responses are related to one's sense of insecurity and vulnerability,[11] which can exacerbate the perception of a real and imminent threat. Also similar to previous studies,[25,34] STAI did not reveal significant difference between the control and treatment group—this could be due to the reliability of self-report measures,[35] particularly on issues of stress and anxiety, which continue to carry a social stigma.

Researchers have been more interested in either cyberbullying[36] or the economic costs of cybercrime and the potential material costs of cyberterror,[37] while ignoring its impact on threat perception and political attitudes.[4,38] These lacunae in the literature are particularly troubling given the rising tide of cyberterror. The impact of cyberattacks explored in this study shows how the outsized effects of cyberattacks offer nonstates (e.g., guerrillas) an opportunity to add a relatively cheap and economical tactic to their repertoire that augments conventional attacks and reinforces the perception that civilians are under threat from all sides. ISIS (the Islamic State militant group), whose social media savvy demonstrates the power of cyber campaigns, is a pertinent example. Cyberattacks are not benign. Even when no one suffers physical harm, the opportunity to cause anxiety and stress, instill fear, and disrupt everyday life is immense. Future research should focus on educational and psychological intervention techniques to ameliorate the psychological harms of cyberattacks. This study offers the first data-based research enabling researchers to evaluate the psychological distress and growing perceptions of threat and insecurity that contribute to the cycle of global cyberterror.

Acknowledgments

This research was made possible, in part, by grants awarded to Daphna Canetti 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 Michael L. Gross from the Israel Science Foundation (156/13). The authors thank Keren Levy Ganany-Snider and Shani Fachter for their invaluable assistance in running the experiments and Shay Zandani for making the cyber attacks look real.

Author Disclosure Statement

No competing financial interests exist.

References

1. Lerner JS, Gonzalez RM, Small DA, et al. Effects of fear and anger on perceived risks of terrorism a national field experiment. Psychological Science 2003; 14:144–150.
2. Tucker P, Pfefferbaum B, North CS, et al. Biological correlates of direct exposure to terrorism several years post disaster. Annual Clinical Psychiatry 2010; 22:186–195.
3. Canetti D, Gross LM, Waismel-Manor I. (2016) Immune from cyber fire? The psychological & physiological effects of cyber war. In Allhoff F, Henschke A, Strawser BJ, eds. *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press, pp. 157–176.
4. Ariely G. (2008) Knowledge management, terrorism, and cyber-terrorism. In Janczewski L Colarik A, eds. *Cyberwarfare and cyber-terrorism*. IGI Global, Hershey, PA: pp. 7–16.
5. McDermott R. (2010) Decision making under uncertainty. *Proceedings of a Workshop Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. National Academies Press, Washington, DC: pp. 227–241.
6. 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. Journal of Conflict Resolution 2009; 53:363–389.
7. Harrell E, Langton L. (2013) *Victims of identity theft, 2012*. Washington, DC: Bureau of Justice Statistics, p. 26.
8. Monahan T. Identity theft vulnerability: neoliberal governance through crime construction. Theoretical Criminology 2009; 13:155–176.
9. Sharp T, Shreve-Neiger A, Fremouw W, et al. Exploring the psychological and somatic impact of identity theft. Journal of Forensic Sciences 2004; 49:131–136.
10. Sinclair J, Antonius D. (2012) *The psychology of terrorism fears*. Oxford: Oxford University Press.
11. Bonanno GA, Galea S, Bucciarelli A, et al. Psychological resilience after disaster: New York City in the aftermath of the September 11th Terrorist Attack. Psychological Science 2006; 17:181–186.
12. Bleich A, Gelkopf M, Solomon Z. Exposure to terrorism, stress-related mental health symptoms, and coping behaviours among a nationally representative sample in Israel. JAMA 2004; 290:612–620.
13. Berrebi C, Klor EF. Are voters sensitive to terrorism? Direct evidence from the Israeli electorate. American Political Science Review 2008; 102:279–301.
14. Pfeffer CR, Altemus M, Heo M, et al. Salivary cortisol and psychopathology in adults bereaved by the September 11, 2001 terror attacks. The International Journal of Psychiatry in Medicine 2009; 39:215–226.
15. Dekel S, Ein-Dor T, Gordon KM, et al. Cortisol and PTSD symptoms among male and female high-exposure 9/11 survivors. Journal of Traumatic Stress 2013; 26: 621–625.
16. Schlotz W, Hammerfald K, Ehlert U, et al. Individual differences in the cortisol response to stress in young healthy men: testing the roles of perceived stress reactivity and threat appraisal using multiphase latent growth curve modeling. Biological Psychology 2011; 87:257–264.
17. Kirschbaum C, Hellhammer DH. Salivary cortisol in psychoneuroendocrine research: recent developments and applications. Psychoneuroendocrinology 1994; 19:313–333.
18. Umeda T, Hiramatsu R, Iwaoka T, et al. Use of saliva for monitoring unbound free cortisol levels in serum. Clinica Chimica Acta 1981; 110:245–253.
19. Wedekind D, Bandelow B, Broocks A, et al. Salivary, total plasma and plasma free cortisol in panic disorder. Journal of neural transmission (Vienna) 2000; 107:831–837.

20. Levine A, Zagoory-Sharon O, Feldman R, et al. Measuring cortisol in human psychobiological studies. Physiology & Behavior 2007; 90:43–53.
21. Angeli A. (1978) The binding of glucocorticoids to human plasma proteins. In: James, V. (ed.) *The endocrine function of the human adrenal cortex*. London: Academic Press, p. 155.
22. Kahn JP, Rubinow DR, Davis CL, et al. Salivary cortisol: a practical method for evaluation of adrenal function. Biological Psychiatry 1988; 23:335–349.
23. Vining RF, McGinley RA, Maksvytis JJ, et al. Salivary cortisol: a better measure of adrenal cortical function than serum cortisol. Annals of Clinical Biochemistry 1983; 20 (Pt 6):329–335.
24. Gozansky WS, Lynn JS, Laudenslager ML, et al. Salivary cortisol determined by enzyme immunoassay is preferable to serum total cortisol for assessment of dynamic hypothalamic–pituitary–adrenal axis activity. Clinical Endocrinology 2005; 63:336–341.
25. Waismel-Manor I, Ifergane G, Cohen H. When endocrinology and democracy collide: emotions, cortisol and voting at national elections. European Neuropsychopharmacology 2011; 21:789–795.
26. Moore J. Hacker group Anonymous threatens Israel with ‘Electronic Holocaust’. Newsweek, 30 March 2015. http://europe.newsweek.com/hacker-group-anonymous-threaten-israel-electronic-holocaust-317729?rm=eu Accessed January 7, 2017.
27. Liebelson D. Inside Anonymous’ cyberwar against the Israeli government. Mother Jones, 22 July 2014. www.motherjones.com/politics/2014/07 anonymous-cyberattack-israel-gaza Accessed December 22, 2016.
28. Spielberger CD, Gorsuch RL, Lushene R, et al. (1983) *Manual for the state-trait anxiety inventory*. Palo Alto, CA: Consulting Psychologists Press.
29. Marteau TM, Bekker H. The development of a six-item short-form of the state scale of the Spielberger State-Anxiety Inventory (STAI). British Journal of Clinical Psychology 2011; 31:301–306.
30. Greenfield DN. Psychological characteristics of compulsive internet use: a preliminary analysis. Cyber Psychology & Behavior 1999; 2:403–412.
31. Acock AC. (2013) *Discovering structural equation modeling using stata*. Rev. ed. College Station, TX: Stata Press.
32. Canetti D, Elad-Strenger J, Lavi I, Guy D, Bar-Tal D. Exposure to violence, ethos of conflict and support for compromise: survey in Israel, East Jerusalem, West Bank, and in Gaza. Journal of Conflict Resolution 2017; 61:84–113.
33. Canetti D. (2015) Explaining support for violence in wartime: individual-level exposure effect? In Halperin E, Sharvit K, eds. *The Israeli-Palestinian conflict: a social psychology perspective - celebrating the legacy of Daniel Bar-Tal, volume II.* New York: Springer, pp. 151–166.
34. Neiman J, Smith KB, French JA, et al. Voting at home is associated with lower cortisol than voting at the polls. PLoS One 2015; 10:e0135289.
35. Dickerson SS, Kemeny ME. Acute stressors and cortisol responses: a theoretical integration and synthesis of laboratory research. Psychological Bulletin 2004; 130:355–391.
36. Mesch GS. Parental mediation, online activities, and cyberbullying. CyberPsychology & Behavior 2009; 12:387–393.
37. Paulhus DL, Vazire S. The self-report method. Handbook of Research Methods in Personality Psychology 2007; 1:224–239.
38. Graves J, Acquisti A, Anderson R. Experimental measurement of attitudes regarding cybercrime. 13th Annual Workshop on the Economics of Information Security. Pennsylvania State University 2014.

Address correspondence to:
Dr. Israel Waismel-Manor
School of Political Science
University of Haifa
4018 Amadrega
Haifa 31905
Israel

E-mail: wisrael@poli.haifa.ac.il