IMMUNE FROM CYBER-FIRE?

The Psychological & Physiological Effects of Cyberwar

Daphna Canetti, Michael L. Gross* & Israel Waismel-Manor
The University of Haifa, Israel

In: ***Binary Bullets: The Ethics of Cyberwarfare*** .
Edited by Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser.
Oxford: Oxford University Press, forthcoming

* mgross@poli.haifa.ac.il

Introduction

When noncombatants suffer bodily injury or loss of life during war, they experience harm in the most obvious way. While protected from direct or intentional harm, noncombatants may, nonetheless, suffer proportionate collateral harm in the course of effective and necessary military operations. This is the principle of noncombatant immunity. To inflict *direct* harm upon noncombatants is to egregiously violate this principle and commit a crime of war against the innocent.

What then of cyberwar? What kind of harm does cyberwar inflict upon noncombatants? Do victims of cyber-attacks suffer significant physiological harm or only some measure of mental suffering, distress and anxiety? And, if the latter, does such suffering violate noncombatant immunity? Compared to death and injury, psychological harm appears far less grave. While one can certainly paint scenarios of cyber-attacks that cause acute mental trauma, much of the suffering that cyberwarfare seems to bring lacks the pain and persistence of many physical injuries.

Following an overview that describes the challenge that cyber-operations pose for the principle of noncombatant immunity, the following sections map out and analyze the harms of cyberwarfare. Consider, first, physiological harm. Although no person has lost his life or suffered any kind of physical injury from a cyber-attack to date, the literature is replete with scenarios of death and devastation. These come in the course of cyber-attacks on vital infrastructures that disrupt air and rail transportation or poison water supplies. In many ways, these are similar to the consequences of conventional war. For the most part, however, modern cyber-warfare causes no physical injury. As a result, one may reasonably ask whether noncombatants enjoy protection from cyber-attacks that disrupt telecommunications, disable social media, or destroy, disclose or steal financial data and personal information. The answer hinges upon the psychological harm that victims suffer, particularly if belligerents target civilians and civilian infrastructures directly. Extrapolating from studies of cyber-bullying, identity theft and ordinary burglary, and building upon the effects of simulated cyber-terrorism in the laboratory, we explore the psychological harms of cyberwarfare. Cyberwarfare is not benign but causes stress, anxiety and fear. Such mental suffering threatens to disrupt routine life, impair educational and workplace performance, impact significantly on the poor and elderly, and increase public pressure on the government to act. Although most forms of psychological suffering are not as intense, prolonged or irreversible as bodily injury or loss of life, our analysis suggests that the psychological harm of cyberwar can affect well-being nonetheless.

Noncombatant Immunity, Cyberwar, and Cyber-terrorism

In conventional war noncombatants, that is, those who take no direct part in the hostilities, are protected from both direct and collateral injury. Posing no threat, noncombatants may not be intentionally killed or injured. Everyone has long recognized, however, that noncombatants will die in war as belligerents disable military targets. When such deaths are necessary, unavoidable and unintended, just war theory and international law make room for collateral or incidental civilian casualties as long as they are neither excessive nor disproportionate relative to the military gains a belligerent seeks. When too many civilians die in the course of

military operations, states face condemnation for causing disproportionate harm. When parties to a conflict intentionally harm civilians, they face charges of murder and terrorism. To assess proportionality or terrorism, one must understand the harm noncombatants suffer. Observers usually measure harm in terms of civilian deaths. Injuries and property destruction may also weigh in but psychological malaise enjoys little attention and rarely figures in calculations of proportionality. This leaves cyberwarfare -which targets facilities rather than individuals and have, to date, caused no immediate injuries - beyond considerations of proportionality and wide open to unconstrained use.

Cyber-operations, whether directed at military targets (cyberwarfare) or civilian targets (cyber-terrorism) attack a wide range of infrastructures whose destruction may kill or injure noncombatants and whose penetration may lead to the theft, eradication or disclosure of privileged data. Other operations may go after civilians directly by attacking personal cell phones or computers to steal identities, pilfer bank accounts or threaten civilians with personal harm. Only a few of these attacks present a threat to life or limb (Table 1).

Table 1 Types and Outcomes of Cyber-attacks

Target of Cyber-attack	**Outcomes**	**Possibility of Physical Harm to Life and limb**
CRITICAL INFRASTRUCTURES		
Public Security; Fire, Police	● Disclosure of confidential information ● Disruption/cessation of service	No Yes
Water/Dams	● Disruption of water supply ● Pollution ● Flooding	No Yes Yes
Transportation Networks	● Disrupted schedules ● Equipment failure (train/airplane crashes)	No Yes
OTHER INFRASTRUCTURES		
Medical Infrastructures	● Disclosure of personal information ● Alteration of medical records and prescriptions ● Disruption of vital medical services: operating rooms, ventilators	No Yes Yes
Financial Networks	● No access to bank accounts ● Stolen Funds ● Collapse of Stock Exchange	No No No
Public Records	● Disclosure of criminal records, classified court hearings – sexual abuse, national security cases, adoption) ● Alteration of public records ● Disclosure of biometric information	No No No

PERSONAL ATTACKS		
Personal Computers/ Cell Phones	● Destruction/theft of Data ● Disclosure of personal information ● Identity theft ● Invasion of privacy	No No No No
Individual users	● Cyberbullying: Threaten individuals with harm	Yes

Table 1 suggests that most cyber-operations can not cause physical harm. Those that do have yet to materialize. Absent the prospect of injuries or loss of life in the course of cyberwar, the principle of noncombatant immunity faces two challenges. First, do cyber-attacks harm noncombatants? If not, then noncombatants are appropriate targets of cyber-operations and cyber-terrorism is permissible. If, on the other hand, cyber-attacks bring harm to noncombatants, then cyber-terrorism is impermissible but proportionate collateral harm is not. This raises the second challenge: Do cyber-attacks against military targets cause disproportionate harm to noncombatants?

Injury and loss of life provide one metric to answer these two questions. Kinetic attacks that kill or injure cause sufficient harm to prohibit both direct and disproportionate attacks on noncombatants. But if cyber-attacks do not kill or injure anyone, how might one evaluate direct or collateral harm? How do we know when cyber-attacks violate the principle of proportionality? Psychological harm and mental suffering provide one criterion to address these questions. Kinetic terrorism offers the clearest example. When a suicide bomber, for example, kills 20 people and injures 100, terrorism violates noncombatant immunity in the most extreme way, first by intentionally killing small numbers of individuals (the primary victims of terror) and then by traumatizing large number of individuals (the secondary victims of terror). Terrorism causes intense anxiety and dread among those who fear that they or their loved ones will be next to die.

Cyber-terrorism, however, works differently. While in some cases cyber-attacks may cause death and injury, none to date have done so. Instead, cyber-terrorism disrupts civilian infrastructures and often targets noncombatant assets *directly*. There is no doubt that these attacks are intentional and direct. The question is: "Do they cause any harm?" *The Tallinn Manual on the International Law Applicable to Cyberwarfare*, for example, defines a cyber-attack as "a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.[2]" Understanding that not all cyber-attacks can cause injury or death, the framers of Tallinn consider that cyber-operations cause sufficiently severe mental suffering to warrant condemnation:

While the notion of attack extends to injuries and death caused to individual, it is, in light of the law of armed conflict's underlying humanitarian purposes,

[2] Michael N. Schmitt. Ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013, 106.

reasonable to extend the definition to serious injury and *severe mental suffering* that are tantamount to injury. In particular, note that Article 51(2) of the Additional Protocol I prohibits "acts or threats of violence the primary purpose of which is to spread terror among the population." Since terror is a psychological condition resulting in mental suffering, inclusion of such suffering in this Rule is supportable through analogy.[3]

The Tallinn Manual's conclusion is short an empirical anchor. We will review the psychological sequelae of terrorism below but it is not at all clear that cyber-terrorism of the most extreme, hypothetical kind will cause severe mental suffering. Instead and in the worst case, the effects of cyberwarfare closely resemble acts conventional warfare and economic sanctions that bring long term damage to industrial, agricultural, utility and water infrastructures but do not necessarily cause widespread death or injury. The same might be expected of many cyber-attacks. Some cyber-operations may leave the economy decimated while others may leave people distressed and even terrified of losing data or money. They are not, however, necessarily "terrorized" if by that we mean fearful of losing life or limb.

In short, we need to know about psychological harm for two reasons. The first is to determine whether direct cyber-attacks upon noncombatants constitute terrorism. The second is to assess the proportionality of collateral harm in the course of legitimate military strikes. Direct harm defines terrorism. Excessive harm constrains proportionality. If cyber-attacks cause nothing but moderate inconvenience, they cannot be acts of terrorism or ever cause disproportionate harm. "Inconvenience," of course, is a very broad term and may include all kinds of hardship short of severe mental or physical suffering. If severe mental suffering turns on fear of death, then cyber-operations will usually fall short. The question remains whether cyber-attacks substantially affect well-being in other ways?

Terrorism and Cyber-terrorism: Confronting Bodily Injury and Loss of Life

The primary victims of kinetic terrorism die or suffer horrible injuries while secondary victims avoid physical harm but suffer psychologically. Terrorism gains purchase by posing a deadly, persistent and unpredictable threat. The psychological effects of kinetic terrorism are well documented. Among the most severe is post-traumatic stress disorder (PTSD) a severe anxiety disorder that occurs following exposure to a traumatic event involving death or serious injury and to which individuals respond with "fear, helplessness, or horror.[4]" Following terror attacks, PTSD victims re-experience their trauma through intrusive recollections, dreams, and hallucinations and suffer from insomnia, uncontrollable anger, and difficulty concentrating. PTSD can impair daily functioning and puts patients at increased risk for depression, drug and alcohol abuse, eating disorders, suicidal thoughts and actions, cardiovascular disease, chronic pain, and autoimmune diseases. Prior to 9/11, PTSD affected 5-6% of men and 10-14% of women in the US.[5] Following the

[3] Schmitt, *Tallinn Manual*, 93 (emphasis added).

[4] Rachel Yehuda, "Post-Traumatic Stress Disorder." *New England Journal of Medicine* 346, no. 2 (2002): 108.

[5] Yehuda, "Post-Traumatic Stress Disorder.

9/11 attacks and other terror attacks around the world, studies demonstrate a significant increase PTSD and other anxiety disorders.[6] In Southern Israel, too, PTSD and related anxiety disorder symptoms were common in the aftermath of rocket attacks that continued unabated from 2001 to 2008.[7]

Digging deeper, closer studies reveal two distinct groups of individuals suffering fear related effects from terrorism. One group exhibits the common PTSD symptoms including psychological distress, insomnia and exaggerated startle responses. The other group does not re-experience a *past* trauma but suffers instead from "anticipatory anxiety," that is, fear and dread associated with *future* attacks. These fears grow as the threat persists. While relatively few people suffer from PTSD following a terrorist attack, many more suffer from various degrees of debilitating fear.[8] These, too, are secondary victims of terrorism who experience no physical harm nor are they necessarily present at the site of a terror attack.

The differences between the incidence of PTSD and anticipatory anxiety are striking. While the incidence of PTSD dropped across a US sample from 17% two months after 9/11 to 5.8% six months after the attacks, 60-65% continued to fear future terrorist attacks and worry about harm befalling their family.[9] Widespread fear, then, rather than specific incidence of PTSD is the more pervasive effect of terrorism and more accurately reflects the psychological malaise that accompanies war and terrorism. Terrorism fears correlate with anxiety, depression and insomnia and feelings of incapacitating helplessness.[10] Random bombings and missile attacks lead to fear induced changes in behavior. Victims of terrorism avoid public transportation, public forums and confined venues such as restaurants, cafes and theaters while others often disparage those ethnic groups they identify with terrorists.[11] Others simply flee.[12] As a result of increased isolation, migration and ethnocentrism, social intercourse diminishes. Terrorism brings a constant sense of anxiety, fears about harm to family members, heightened vigilance with regard to suspicious packages and people. Ruminations about recent attacks and fruitless efforts to predict future strikes in an atmosphere of acute fatalism become a constant

---

[6] Justin S. Sinclair, "Fears Of Terrorism and Future Threat: Theoretical and Empirical Considerations," in *Interdisciplinary Analyses of Terrorism and Political Aggression* edited by Samuel J. Sinclair and Daneil Antonius, 101-115. Newcastle upon Tyne: Cambridge Scholars Publishing, 2010; Rachel Yehuda, et al. "Pathological Responses to Terrorism." *Neuropsychopharmacology* 30, no. 10 (2005): 1793-1805.

[7] Marc Gelkopf, Rony Berger, Avraham Bleich, and Roxane Cohen Silver, "Protective Factors and Predictors of Vulnerability to Chronic Stress: A Comparative Study of 4 Communities after 7 Years Of Continuous Rocket Fire." *Social Science & Medicine* 74, no. 5 (2012): 757-766.

[8] Samuel J. Sinclair, and Alice LoCicero. "Fearing Future Terrorism: Development, Validation, and Psychometric Testing of the Terrorism Catastrophizing Scale (TCS)." *Traumatology* 13, no. 4 (2007): 75-90.

[9] Roxanne E. Silver-Cohen, et al. "Nationwide Longitudinal Study of Psychological Responses to September 11." *JAMA* 288, no. 10 (2002): 1235-1244.

[10] Justin S. Sinclair and Daniel Antonius, *The Psychology of Terrorism Fears*. Oxford: Oxford University Press, 2012.

[11] Daphna Canetti-Nisim, et al. "A New Stress-Based Model of Political Extremism Personal Exposure to Terrorism, Psychological Distress, and Exclusionist Political Attitudes." *Journal of Conflict Resolution* 53, no. 3 (2009): 363-389.

[12] Gary M. Diamond, et al. "Ongoing Traumatic Stress Response (OTSR) in Sderot, Israel." *Professional Psychology: Research and Practice* 41, no. 1 (2010): 19.

preoccupation. Workplace efficiency deteriorates, turnover and absenteeism increase while performance, morale and motivation suffer.[13] Civil society perseveres but community and economic life suffer in the wake of terrorism. Among many secondary victims of kinetic terrorism, personal well-being deteriorates in a most fundamental way.

Will cyber-terrorism, even in its most extreme form, bring such consequences? This depends on the nature of the cyber-attack. Consider the hypothetical scenarios that pervade the literature. Here, individuals may certainly die if trains derail or airplanes crash. In these cases cyber-terrorism resembles suicide bombings. The primary victims will suffer death and injury while the secondary victims will endure psychological pain and suffering. Yet cyber-attacks of even the most extreme type are far more focused than kinetic attacks. A terrorist can blow himself up anywhere but cyber-terrorism requires a computer network to attack. Public gathering places, a favorite venue for suicide bombers would not make likely targets for cyber-terrorists. As such, the random nature of terror and with it the resulting anxiety, might be mitigated by avoiding vulnerable targets.

The psychological consequences of cyber-terrorism diminish further when one considers less catastrophic assaults on other infrastructures. Flooding, pollution and the destruction of utility networks are common scenarios. What physical and psychological harm do these attacks bring? While deaths may occur, far more prevalent is the economic devastation and deleterious long term public health effects that come when farmlands flood, electrical grids collapse or water treatment plants break down. While unknown in the world of cyber, such effects are common during and after armed conflict.

In the course of war, the destruction of property is not benign. Apart from immediate harm to persons are the longer term effects that come when vital services collapse following armed attacks. This is particularly true when health, water, sanitation, manufacturing and agricultural facilities are destroyed or damaged. During the 2006 Second Lebanon War, for example, observers documented extensive damage to airports, ports, water and sewage treatment, electrical plants, roads, fuel stations, bridges, overpasses, commercial properties homes, cropland and livestock in Southern Lebanon. Unexploded ordnance further rendered large tracts of land untillable, while the destruction of fuel storage tanks caused a disastrous oil spill along the coast.[14] The indirect costs of armed conflict include capital flight, discouragement of investments, decreased tourism, emigration (of medical and other professionals in particular), inflation and food insecurity.[15] Many of these outcomes mirror those predicted for cyberwarfare and cyber-terrorism. Under these conditions, the civilian population suffers enormously. In the wake of the Second

[13] Luke Howie, "The Terrorism Threat and Managing Workplaces." *Disaster Prevention and Management* 16, no. 1 (2007): 70-78

[14] Bassam Fattouh and Joachim Kolb. "The Outlook for Economic Reconstruction in Lebanon After the 2006 War." *http://web. mit. edu/cis/www/mitejmes* (2006). *The MIT Electronic Journal of Middle East Studies*, 6, 97-111; Ragy Darwish, Nadim Farajalla, and Rania Masri. "The 2006 War and Its Inter-Temporal Economic Impact on Agriculture in Lebanon." *Disasters* 33, no. 4 (2009): 629-644.

[15] Goran Lindgren, *Studies in Conflict Economics and Economic Growth. Report No. 72*. Uppsala: Department of Peace and Conflict Research, Uppsala University, 2006.

Lebanon War, financial hardship and "trauma exposure" significantly influenced psychiatric morbidity among the Southern Lebanese civilian population."[16]

If cyber-operations destroy infrastructures in ways similar to conventional war, one might expect similar psychological consequences. When some civilians lose their lives, others will fear massively for their own. When the economy is wrecked, many will suffer significant stress and anxiety. But civilians will also rebound. Following missile attacks in Southern Israel, a large percentage (40-78%) of victims was symptom free and "the emotional impact... fairly moderate," an outcome that did not change much after 44 months of intermittent attack.[17] Researchers attribute resilience to "a habituation process and coping mechanisms," "self-efficacy," strong community networks and social cohesion.[18] Following the 2006 Lebanon War, these same tight social networks prevented outbreaks of major disease or social unrest and mitigated the incidence of PTSD and depression. Communities without the requisite resources and social networks, on the other hand, experienced greater incidence of mental illness and dysfunction.[19]

One might expect similar effects from cyber-operations that target critical infrastructures whose destruction will lead to death, disease and severe economic hardship. Most cyber-operations, however, lack this reach and aim instead to disable or disrupt facilities that support social networks, banking institutions and public institutions. Other operations target civilians directly by stealing data and money or threatening personal harm. What psychological suffering do these acts bring? Are routine life and personal well-being affected as adversely when the threat to life and limb is absent?

Cyber-terrorism: Confronting Psychological Harm and Severe Mental Suffering

In the worst cases, cyber-operations that disable or destroy critical infrastructures and cause physical injury and loss of life are nearly analogous to kinetic terror attacks. Although relatively few people may die, one might easily speculate that the secondary victims of cyber-terrorism experience some measure of severe mental suffering. However, cyber-attacks, unlike kinetic terrorist attacks, do not target individuals but infrastructures. The effects on individuals may be immediate (as when trains derail) or indirect and less lethal (as when water sources are poisoned or electrical grids rendered inoperative). As a result, the secondary target (i.e. the civilian population) may not suffer psychological harm akin to

---

[16] Laila Farhood, Hani Dimassi, and Nicole L. Strauss. "Understanding Post-Conflict Mental Health: Assessment of PTSD, Depression, General Health and Life Events in Civilian Population One Year after the 2006 War in South Lebanon." *Journal of Trauma and Stress Disorders Treatment* 2:2. (2013) https://scholarworks.aub.edu.lb/bitstream/handle/10938/9704/understanding_post_conflict_mental_health.pdf?sequence=1.

[17] Zvi Zemishlany, "Resilience and Vulnerability in Coping with Stress and Terrorism." *Israeli Medial Association* 14, no. 5 (2012): 307-309

[18] Avraham Bleich, Marc Gelkopf, and Zahava Solomon. "Exposure to Terrorism, Stress-Related Mental Health Symptoms, and Coping Behaviors among a Nationally Representative Sample in Israel." *JAMA* 290, no. 5 (2003): 612-620; Avi Bleich, et al. "Mental Health and Resiliency Following 44 Months of Terrorism: A Survey of an Israeli National Representative Sample." *BMC Medicine* 4, no. 1 (2006): 21. http://www.biomedcentral.com/1741-7015/4/21.

[19] Imam Nuwayhid, et al. "Summer 2006 War on Lebanon: A Lesson in Community Resilience." *Global Public Health* 6, no. 5 (2011): 505-519; Farhood, Dimassi, and Strauss, "Understanding Post-Conflict Mental Health."

terrorization but something less acute as occurs with the collapse of many infrastructures during war more generally.

When cyber-operations target individuals, computerized networks or facilities, there is no obvious reason to expect that such attacks will cause severe suffering at all. For this reason, perhaps, the Tallinn Manual dismisses many potentially harmful cyber-attacks. Cyber-operations that include, "blocking email throughout the country," (§30.12); DDOS attacks, "mere economic coercion" (§11.2); "cyber psychological operations intended solely to undermine confidence in a government or economy (§11.3) or, in one elaborate example "a tweet to cause panic "falsely indicating that a highly contagious and deadly disease is spreading through the population" (§36.3) do not rise to the requisite level of force to constitute an armed attack in the opinion of the Manual's experts. Any such attack, therefore, will not constitute cyber-terrorism if directed against noncombatants.

Addressing these serious lacunae in the evolving law of cyberwarfare requires a different conception of terrorism than that assumed by Tallinn as well as a better understanding of the psychological harm that cyber-terrorism can cause. The framers of Tallinn believe, for example, that "the internet is not indispensable to the survival of the civilian population (§81.5)." Such a remark exhibits a complete lack of understanding of the growing role of cyber-networks in everyday life. Although not indispensable in the way food and water are, the internet is the foundation of modern communications, banking and other services and, for many, social connectivity. And while individuals will survive without internet (just as they can survive without many basics) they may suffer significant distress if the network is disrupted or destroyed. While cyber-attacks may not cause serious harm, they nevertheless impair the faith citizens have in their governments. Until twenty or so years ago, citizens' sense of security was a derivative of safe streets and borders. In today's world, where much of individuals' lives take place online, a person may live in a safe nation and still feel high anxiety for his online safety.

This is precisely the supposition we intend to test. There is some evidence to expect that cyber-attacks and related assaults cause significant anxiety. Notwithstanding the statistic that 25% of Americans are victims of identity theft, there is little research on related psychological harm of cyber-attacks. Studies by and Sharp and his colleagues, for example, found that two weeks after learning of the crime, victims experienced irritability, anger, fear, anxiety and frustration, sleep deprivation, anxiety, nervousness, loss of appetite, weight changes and headaches.[20] Twenty six weeks later, emotional responses turned to severe distress and desperation, mistrust and paranoia, nervousness, gastrointestinal problems and headaches. These are little different from the psychological trauma of ordinary burglary and non-violent home invasion.[21] Qualitative research has suggested that fear of cyber-identity theft stokes fear of financial losses, damage to reputation and

[20] Tracy Sharp, et al. "Exploring the psychological and somatic impact of identity theft." *Journal of Forensic Sciences* 49, no. 1 (2004): 131-136.

[21] Alan Beaton, et al. "The Psychological Impact of Burglary." *Psychology, Crime and Law* 6, no. 1 (2000): 33-43; Barbara B. Brown, and Paul B. Harris. "Residential Burglary Victimization: Reactions to the Invasion of a Primary Territory." *Journal of Environmental Psychology* 9, no. 2 (1989): 119-132; Mike Maguire, "Impact of Burglary upon Victims," *The British. Journal of Criminology* 20 (1980): 261- 275.

loss of online privacy.[22] Cyber-bullying is an aggressive act that subjects targets to a barrage of degrading, threatening, and/or sexually explicit messages and images using web sites, instant messaging, blogs, chat rooms, cell phones, e-mail, and personal online profiles that is very difficult to supervise or detect.[23] Targets of cyber-bullying experience intense anger, powerlessness, sadness, fear, loss of confidence, disassociation, a general sense of uneasiness, possible trauma and aggressiveness.[24] These findings suggest that significant psychological suffering may be present even when the threat of physical harm is relatively minor, thereby reinforcing our perception of cyber-terrorism as acts that do not necessarily entail death or injury but elicit fear by damaging personal property, creating civil disorder or causing significant economic harm.[25] At the same time, the fear, anxiety and mental suffering that cyber-terrorism can bring belies any attempt to understand cyber-terrorism as victimless. Quite the contrary, Hamas hactivists, for example, recently used text messaging to deliver hostile, personal threats to intimidate Israeli civilians. When credible, such threats can raise fears of injury or death.

Extrapolating from these psychological data we expect two sorts of psychological suffering in the wake of cyberwarfare. First, individuals will experience the distress and anxiety that come with the disruption of everyday services when people cannot ensure their privacy, access their bank accounts, fill prescriptions timely, travel as necessary, maintain communications and run their computers. Realistic scenarios depicting the impact of cyberwarfare variously describe denial of service, the inability to enter web sites, lost or stolen data, the unauthorized disclosure of confidential information, the destruction of computer infrastructures and the collapse of social networks. While these disruptions are free of the fears of injury or death that accompany kinetic terrorism, they would seriously impair people's ability to function effectively in a modern, industrial society. These effects may be particularly severe among vulnerable groups such as the poor and elderly. But ordinary citizens may be no less affected. On January 21 2014, South Koreans awoke to find that thieves had stolen the credit card numbers, names and addresses of 40% of the population. The immediate result was widespread panic,

[22] Roberts, Lynne D. "Cyber Identity Theft." *Handbook of Research on Technoethics*, 542-557. In Handbook of Research on Technoethics edited by R. Luppicini, & R. Adell, 542–557. Hershey, PA: Information Science Reference, 2008.

[23] Peter K. Smith, et al. "Cyberbullying: Its Nature and Impact in Secondary School Pupils." *Journal of Child Psychology and Psychiatry* 49, no. 4 (2008): 376-385; S. Shariff, and R. Gouin. "Cyber-hierarchies: a New Arsenal of Weapons for Gendered Violence in Schools." In *Combating Gender Violence In and Around Schools* edited by C. Mitchell and F. Leech, (2006): 33-41. London: Trentham Books, 2006; Qing Li, "Cyberbullying in Schools a Research of Gender Differences." *School Psychology International* 27, no. 2 (2006): 157-170; Andrew J. Milson, and Beong-Wan Chu. "Character Education for Cyberspace: Developing Good Netizens." *The Social Studies* 93, no. 3 (2002): 117-119.

[24] Andre Sourander, et al. "Psychosocial Risk Factors Associated with Cyberbullying among Adolescents: A Population-Based Study." *Archives of General Psychiatry* 67, no. 7 (2010): 720-728; Gianluca Gini and Tiziana Pozzoli. "Association between Bullying and Psychosomatic Problems: A Meta-Analysis." *Pediatrics* 123 (3) (2009): 1059-65; Diane L. Hoff and Sidney. N. Mitchell. "Cyberbullying: Causes, Effects, and Remedies." *Journal of Educational Administration* 47 (5) (2009): 652-65.

[25] Gil Ariely "Knowledge Management, Terrorism, and Cyber Terrorism. In *Cyber Warfare and Cyber Terrorism* edited by L. Janczewski and A. Colarik, 7-16. Hershey, PA: IGI Global. 2008.

system crashes, a run on banks to cancel credit cards and massive lawsuits.[26] The culprit in Korea was an insider, but the effect upon the citizenry was no different than a cyber-strike. Attacks such as these feed a second but amorphous fear that comes with the constant assault by unknown, malevolent agents whose agenda is neither clear nor predictable. Cyber-terrorism stokes anxieties about loss of control and unpredictability that might be as inescapable as those accompanying war and kinetic terrorism.

Assessing the Psychological Effects of Cyber-terrorism in the Lab

To evaluate the psychological effects of cyber-terrorism we conducted a series of laboratory experiments to simulate cyber-attacks on individuals. Our experimental attacks simulate those that hacktivist and non-state actors perpetrate and whose goal is to disrupt the lives of individuals and, often, establish a platform for their grievances. In this way, cyber-attacks share the aims of conventional, kinetic terror attacks. Both use short lived but spectacular attacks to strengthen morale among compatriots, discomfit their enemies by underscoring their weaknesses and place their political cause squarely on the international agenda.

The manipulations chosen for this study simulate the way ordinary citizens may experience a cyber-attack. These are individual, not mass casualty attacks. While mass casualty terrorism hopes to violently disrupt civil society and kill civilians, individual attacks will at best bring chaos, personal discomfort or anxiety. The manipulation, therefore, had but one purpose – to generate among respondents the recognition that their private online identity was private no more. We did not cause or threaten specific harms such as loss of medical or financial information. Yet by using the video chat window together with the threatening "Anonymous" logo and a text message to their private phone, we sent the participant a clear message that she was not alone any more. "Anonymous" is a well-known, diffused global network of hackers responsible for hundreds of cyber-attacks, from Tunisia and PayPal to the Scientology Church and Swiss financial institutions.[27] By making Anonymous the attacker, we steered away from the particularity of a specific conflict, thereby making our findings generalizable. To simulate intrusiveness and breach of privacy we conducted the experiment on a lab computer and the participants' private cell phone. The text message to the participants' cell phones cemented the feeling among participants that *they* were the target of the cyber-attack, not the lab computer. Before and during the manipulation subjects provided a saliva sample to measure cortisol, a hormone associated with stress.

Experimental Results

To test the impact of simulated cyber attacks, we designed fully controlled randomized experiments - i.e., pre-post-treatment-control. The study began with a battery of questions asking participants to describe their computer savviness and

---

[26] J. Lee, "South Koreans Seethe, Sue as Credit Card Details swiped," *Reuters*, 21 January 2014. http://www.reuters.com/article/2014/01/21/us-korea-cards-idUSBREA0K05120140121.

[27] Parmy Olson. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York: Hachette Digital, Inc, 2012.

usage, probe political attitudes, and describe their overall psychological well-being. After providing us with a saliva sample, respondents continued the survey. At this stage respondents in the treatment group saw a pop-up screen with a message from Anonymous (Figure 1), which only the research assistant (RA) could unlock. If questioned about whether it was part of the experiment, the RA was instructed to reassure the student that she knows nothing and that subjects must ignore it and continue the study.

Figure 1: Cyber-Attack Stage I – Anonymous Screen

After a few additional questions, a skype-like split video screen popped up where subjects could see themselves live and see and hear a suspicious looking person typing (Figure 2).

Figure 2: Cyber-Attack Stage II – Video Chat Activation

As before, only the RA could close the screen, and again it was her role to reassure the respondent it must be a fluke. Finally, five questions later they received an anonymous phone text message which stated that their personal data were hacked (Figure 3). If a respondent became uncomfortable, the RA again asked the participant to continue. At no point was the RA to admit it had anything to do with the study, and stressed that "over 30 students completed the study and nothing like

this ever happened." Control group respondents completed the very same questions, but without the cyber-threat component.

Figure 3: Cyber-Attack Stage III – Personal Text Message

At the completion of the survey, all respondents provided a second saliva sample, again reported their overall psychological well-being and completed a battery of questions on cyber-threats and cyber-policies. Upon completion, we debriefed all respondents.

As expected, our preliminary results demonstrated that exposure to cyber-attacks has psychological and physiological impact. Our preliminary study (n=37) shows an average decrease of about 7 percent in the cortisol level of the control group consistent with diurnal effects that cause a decrease of cortisol as the day progresses. The treatment group however, experienced an average rise of 5 percent in cortisol, a clear indication that the cyber-attack caused stress and anxiety.[28]

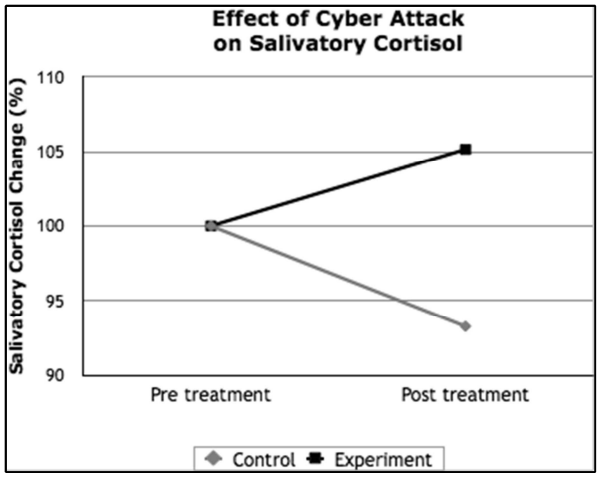

Figure 4: Physiological Effects of Cyber-attack

[28] As evident from Figure 4, and from other auxiliary analyses we have been advancing, the two subject groups -- treatment vs. control, clearly differ in the way they respond to the treatment. However, caution is required in interpreting our results. We relied on a small sample which precludes additional relevant analyses of other mechanisms. It is too small to expect significant differences in this early stage of this ongoing study.

These physiological findings are further supported by the psychological well-being measures. Using the widely accepted State-Trait Anxiety Inventory (STAI), we asked respondents to report from low (1) to high (4) their overall mood using six items, three positive (calm, serene, content) and three negative (upset, worried, tense), providing us with both poles of their positive and negative affect.[29] Figure 5 shows how cyber-attacks negatively affect personal psychological well-being.

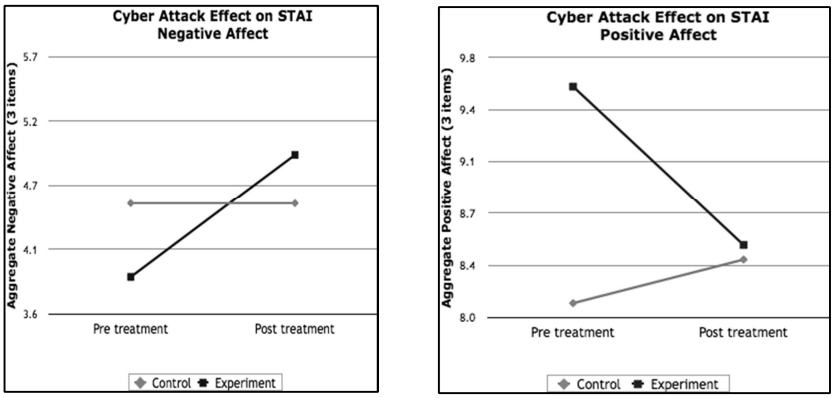

Figure 5: Cyber-attack Effect on STAI[30]

These results clearly, but preliminarily, indicate that psychological well-being deteriorated in the treatment (cyber-attacked) group while the control group experienced no significant mood change. Together with the cortisol results, these findings demonstrate that cyber-research, which is predominantly governed by security experts (national and computer), must not only take into account the number of casualties, computers or mainframes affected, but also the way in which individuals might be psychologically impaired following such an attack.[31] As noted, the simulated attacks did not cause or threaten to cause permanent damage or harm to participants. Cyber-attacks that steal identities, data, or money, disclose confidential information or threaten individuals with random, personal harm are likely to cause significant fear, stress and anxiety that can effectively impinge upon the rational decision making that governments require from their citizens for good governance.

[29] Charles Spielberger, et al. *Manual for the State-Trait Anxiety Inventory*. Palo Alto, CA: Consulting Psychologists Press, 1983.

[30] A paired-samples t-test was conducted to compare the aggregate *positive* psychological well-being before and after the cyber-attack. There was a significant difference in the scores for before (M=9.6, SD=2.33) and after (M=8.5, SD=2.94) conditions; t(24)=2.85, p = 0.009. The scores for the control group, which did not experience a cyber-attack, show little difference between the before (M=8.1, SD=2.77) and after (M=8.4, SD=2.35) tests; t(11)=-5.9, p = 0.570 (Figure 5). Another paired-samples t-test was conducted to compare the aggregate *negative* psychological well-being before and after the cyber-attack. There was a significant difference in the scores for before (M=3.9, SD=1.22) and after (M=4.9, SD=2.06) conditions; t(24)=-2.295, p = 0.031. The scores for the control group show no difference at all between the before (M=4.5, SD=1.68) and after (M=4.5, SD=1.45) conditions; t(11)=0.00, p = 1.000 (Figure 5).

[31] The effects of these attacks are expected to be significantly larger when they take place outside a lab setting and when the person is the actual owner of the attacked computer.

Acute stress has been found to disrupt decision-making[32] making people with higher levels of cortisol more sensitive to immediate rewards than those with lower levels.[33] The former are also more prone to making snap decisions, indicative of a loss of top-down control.[34] Beyond the stress-response, there is evidence that the psychological and physiological reactions following exposure to threatening events such as political violence affect the immune system negatively and cause inflammations in the body in a way that can significantly radicalize political attitudes and behavior.[35] Investigating cortisol and inflammatory markers is of special interest to those concerned with protecting against politically related violence that comes with the militant and aggressive attitudes may follow cyber-terrorism. While people may not necessarily be aware of the forces and conditions that underlie their reactions to cyber-attacks, understanding the role of physiological reactivity markers fills a pressing need for objective data and empirically based generalizations about their effects on civilians.

Figure 6 describes the general outcome of our investigation into the psychological effects of cyberwarfare and cyber-terrorism. The first row depicts a model that informs the framers of the Tallinn Manual, terrorists themselves and nearly everyone else. Kinetic terrorism kills or injures small numbers of individuals (the primary target) and terrorizes large numbers of individuals by inflicting severe mental suffering that disrupts daily life, skews rational decision making and hopes to bring the civilian population to pressure their government to take immediate steps to end the conflict and meet terrorists' demands.

---

[32] Giora Keinan, Nehemia Friedland, and Yossef Ben-Porath. "Decision Making Under Stress: Scanning of Alternatives under Physical Threat." *Acta Psychologica* 64 (3) (1987): 219-28; Stephanie Preston et al. "Effects of Anticipatory Stress on Decision Making in a Gambling Task." *Behavioral Neuroscience* 121, (2007): 257-263; Anthony J. Porcelli and Mauricio. R. Delgado. "Acute Stress Modulates Risk Taking in Financial Decision Making." *Psychological Science* 20 (3) (2009): 278-83.

[33] Pier V. Piazza et al. "Corticosterone in the Range of Stress-Induced Levels Possesses Reinforcing Properties: Implications for Sensation-Seeking Behaviors." *Proceedings of the National Academy of Sciences of the United States of America* 90 (24) (1993): 11738-42. Tanja, C. Adam and Elissa S. Epel, "Stress, Eating and the Reward System." *Physiology & Behavior* 91 (2007): 449-58; Emily Newman, Daryl. B. O'Connor and Mark Conner. "Daily Hassles and Eating Behaviour: The Role of Cortisol Reactivity Status. *Psychoneuroendocrinology* 32 (2) (2007): 125-32.

[34] See Keinan. "Decision Making". Porcelli. "Acute Stress"

[35] Jennifer E. Graham. "Hostility and Pain are Related to Inflammation in Older Adults." *Brain, Behavior and Immunity*, 20, (2006): 389-40; Thaddeus W. Pace et al. "Innate Immune, Neuroendocrine and Behavioral Responses to Psychosocial Stress Do Not Predict Subsequent Compassion Meditation Practice Time." *Psychoneuroendocrinology*, 35(2) (2010): 310-5; Daphna Canetti et al. "Inflamed by the Flames? The Impact of Terrorism and War on Immunity." *Journal of Traumatic Stress* 27 (2014): 1-8.

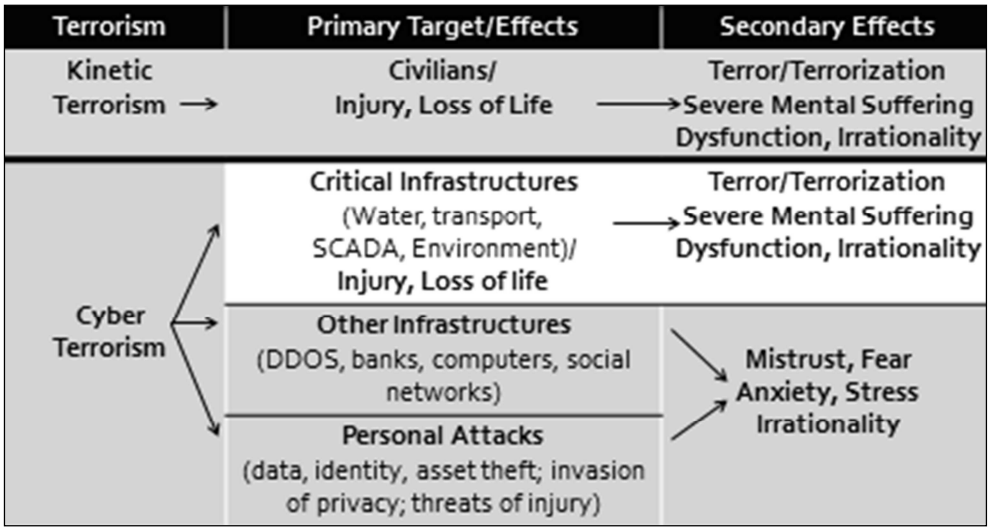

Figure 6: The Effects of Kinetic and Cyber-Terrorism

Cyber-terrorism and cyberwar are more complex. Cyber-terrorism attacks critical and other infrastructures and individuals indiscriminately while cyberwarfare harms the same civilians collaterally. The destruction of some critical infrastructures may bring loss of life that can have the same effects upon the civilian population as kinetic terrorism. This remains a matter of conjecture as no such attacks have yet occurred. Instead, cyber-operations will most likely disable other infrastructures (either directly or collaterally) or target individuals directly. In these cases, the civilian population will most likely suffer fear, anxiety, despair, loss of control and mistrust. Some will lose medical or legal records, confidential information, email communications, social networks. Others will find their identity or assets stolen or face physical threats from unknown assailants. Lives and businesses might be radically disrupted.

Psychological distress also shapes attitudes and political decision making. Exposure to kinetic terrorism leads to "psychological insecurity that induces militant attitudes, and violent and non-conciliatory political responses."[36] Helping to explain this outcome, the Shattered Assumptions Approach argues that traumatic events undermine a person's basic assumptions about the world triggering enhanced perceptions of "the world as threatening" and a correspondingly strong desire to reduce this threat through increased militancy.[37] Perceived threat, fear, and anxiety are the single best predictor of militarism.[38] Chronic exposure to war and terrorism

---

[36] Daphna Canetti, et al. "An Exposure Effect? Evidence from a Rigorous Study on the Psychopolitical Outcomes of Terrorism." In *The Political Psychology of Terrorism Fears*, edited by Samuel Justin Sinclair and Daniel Antonius, 193-212. Oxford: Oxford University Press, 2013; Stevan. E., Hobfoll, et. al. "Exposure to Terrorism, Stress-Related Mental Health Symptoms, and Defensive Coping among Jews and Arabs in Israel." *Journal of Consulting and Clinical Psychology* 74 (2) (2006): 207-218.

[37] Katherine B. Carnelley and Ronnie Janoff-Bulman. "Optimism About Love Relationships: General vs Specific Lessons from One's Personal Experiences." *Journal of Social and Personal Relationships* 9 (1) (1992): 5-20.

[38] George A. Bonanno and John T. Jost. "Conservative Shift among High- Exposure Survivors of the September 11th Terrorist Attacks." *Basic and Applied Social Psychology* 28(4) (2006): 311–23. Leone Huddy et al. "The Consequences of Terrorism: Disentangling the Effects of Personal and National Threat." *Political Psychology*

not only harms personal well-being but also contributes to an ongoing cycle of violence as affected citizens harden their political viewpoints in an attempt to cope with stress.[39] By impinging on the public's well-being, cyberwar and cyber-terrorism may affect political attitudes and public policy in a similar way, particularly as democratic leaders tend to follow public opinion when faced with a major public opinion shift.[40] In the wake of concerted cyber-attacks, leaders will face a barrage of demands. Some demands might be reasonable (protective software products), others may be expensive (a strategic cyber reserve of bandwidth and cyber capability), others intrusive, (state monitoring of networks and systems, regulation and/or wiretapping) and others belligerent (kinetic attacks against cyber-attackers). In the worst case policy makers may have no choice but to retaliate and escalate the conflict rather than capitulate.

Cyberwarfare: Implications for Ethics and Law

Despite the far reaching psychological effects of cyberwar and cyber-terrorism, one cannot escape the thought that they are preferable to armed conflict and analogous to economic warfare, sanctions and blockades. The psychological effects of economic warfare, like many of the worst forms of cyberwarfare, are long term, diffuse and of variable duration and intensity. Such indeterminate and mixed outcomes make it very difficult for commanders in the field or policy makers to weigh mental suffering as they wrestle with the principle of proportionality. In fact, it seems that the psychological sequelae of many forms of armed conflict merit no place at all when considering the ills that befall the civilian population.

It is no wonder then that international law is confused. While the Geneva Conventions, particularly Additional Protocol I, take a strong stand against terrorism induced mental suffering, they take virtually no stand when the same suffering follows economic warfare. Unlike the collateral harm that follows when infrastructures are destroyed in the normal course of war, sanctions and blockades target civilians directly. Yet economic warfare remains beyond the purview of the law of war as long as blockades or sanctions do not create a "humanitarian crisis" that takes the lives of large numbers of innocent civilians and while reducing the rest to penury. Despite its legal cover, the sanctions imposed on Iraq by the international community after the First Gulf War brought precisely this sort of crisis. There, notes Gottstein, "50,000 children under the age of five died each year, a quarter of all emergency patients in the hospitals could not be saved due to missing medicines and about 40% of the Iraqi people went hungry having received a food ration that provided only 25% of their vital needs."[41]

---

23 (3) (2002): 485-509; Leone Huddy, et al. "Threat, Anxiety, and Support of Antiterrorism Policies." *American Journal of Political Science* 49 (3) (2005): 593-608.

[39] Haim Bitterman at al. "Characterization of the Best Anatomical Sites in Screening for Methicillin-Resistant Staphylococcus Aureus Colonization." *European Journal of Clinical Microbiology & Infectious Diseases* 29 (4): (2010): 391-7. Bonanno. "Conservative Shift."

[40] Paul Burstein. "The Impact of Public Opinion on Public Policy: A Review and an Agenda." *Political Research Quarterly* 56 (1) (2003): 29-40; Benjamin. I. Page, and Robert Y. Shapiro. "Effects of Public Opinion on Policy." *The American Political Science Review*: 77:1 (1983): 175-90.

[41] R. Garfield The impact of economic sanctions on health and well-being. *Relief and Rehabilitation Network*, London. 1999. http://www.essex.ac.uk/armedcon/story_id/The%20Impact%20of%20Econmoic%20Sanctins%20on%20Health%20abd%20Well-Being.pdf; Ulrich Gottstein. "Peace Through Sanctions? Lessons from Cuba, Former Yugoslavia and Iraq". *Medicine, Conflict and Survival* 15 (3) (1999): 271-85.

Note the conspicuous absence of any reference to mental suffering in these descriptions of humanitarian crises. In contrast to death and debilitating injuries, mental suffering is the proper goal of sanctions and blockades and, therefore, carelessly ignored. By inflicting pain and hardship, one nation hopes to squeeze the civilian population of another so it pressures its government to desist from aggression. Economic warfare stops short of armed conflict and is so lauded as the penultimate resort that gives war legitimacy as the last resort. States, in other words, are often encouraged to wage economic warfare before resorting to armed force when they face aggression. It is tempting, therefore, to consider cyberwarfare and even cyber-terrorism as nothing but another form of economic warfare. As such, any resulting harm, whether direct or collateral, is of little consequence unless it brings a humanitarian crisis. Few cyber scenarios hold such potential.

From the perspective of economic warfare, then, it is easy to conclude that most cyber-operations neither violate the principle of noncombatant immunity nor constitute terrorism. On the contrary, cyber-operations may save a nation from the ravages of war. Before rushing to judgment, however, consider that there are several ways to view terrorism. One, that the Tallinn experts and many others adopt, turns on manifest terrorization accompanied by the ever present threat of death and, as Hannah Arendt describes it, "the bestial, desperate terror which, when confronted by real, present horror, inexorably paralyzes everything that is not mere reaction."[42] Noting that Arendt's view represents the most extreme outcome of terrorism, Jeremy Waldron suggests that terrorism also turns on less violent and coercive means. "The idea that I am pursuing," writes Waldron, "is that a government might be coerced by the loss of something it values very highly - indeed, something indispensable for its status as government - namely, the ability to command and mobilize a large civilian population. By rendering or threatening to render the population mindless with terror, the intimidator deprives the target regime of something it needs, a population capable of rational choice."[43] However, there is no need that a population be "mindless with terror" to undermine its rational decision making capability. And in fact, Waldron looks to something short of "bestial desperate panic" to include "a state or condition that governments cannot afford to let their populations fall into or languish in for long." Examples include the "collapse of economic morale," feelings of insecurity, apprehension and disruption of social intercourse and daily life.[44] These are precisely the effects we can expect of most cyber-operations.

If by terrorism we mean abject terrorization, then cyber-operations are not acts of terror or acts that violate the principle of noncombatant immunity. But if we think a little out of the box we can easily imagine how cyber-operations can cause terrorism of a more pervasive and no less dangerous kind by undermining well-being, morale, public trust and governability. To accomplish this end, one need not

---

[42] Hannah Arendt. *The Origins of Totalitarianism, New Edition*. New York: Harcourt, Brace, Jovanovich, 1973.

[43] Jeremy Waldron, "Terrorism and the Uses of Terror." *The Journal of Ethics*, Vol. 8, No. 1, (2004), 21.

[44] Jeremy Waldron, Terrorism, 21-23.

commit horrific acts of murder. In a modern society it is enough attack the foundations of everyday life. Among these, cyber-networks stand out. As critically, one cannot forget that many cyber-operations, however nonlethal they can be, place civilians in the cross hairs. By targeting civilians and civilian infrastructures, cyber-operations knowingly seek out noncombatants to demoralize the civilian population and bring pressure upon a government to meet their demands. Noncombatants, however, are not the proper objects of attacks that significantly impair their physiological or psychological well-being. Not only do noncombatants pose no threat but singling them out for any intentional or disproportionate harm whatsoever constitutes a grave affront to human dignity to which noncombatants are entitled. Noncombatants are not instruments of war and, for this reason, economic warfare although often lawfully permissible has earned the justifiable wrath of many moral philosophers. For this reason, too, noncombatants deserve every protection from cyberwarfare and the harms it brings.

Bibliography

Adam, Tanja, C., and Elissa S. Epel, "Stress, Eating and the Reward System." *Physiology & Behavior* 91 (2007): 449-58.

Arendt, Hannah. *The Origins of Totalitarianism*, New Edition, New York: Harcourt, Brace, Jovanovic, 1973.

Ariely, Gil. "Knowledge Management, Terrorism, and Cyber-terrorism. In *Cyberwarfare and Cyber-terrorism* edited by L. Janczewski and A. Colarik, 7-16. Hershey, PA: IGI Global. 2008

Beaton, Alan, Mark Cook, Mark Kavanagh, and Carla Herrington. "The Psychological Impact of Burglary." *Psychology, Crime and Law* 6, no. 1 (2000): 33-43.

Bitterman, Haim., Arie Laor, Sarah Itzhaki, and Gabriel Weber. "Characterization of the Best Anatomical Sites in Screening for Methicillin-Resistant Staphylococcus Aureus Colonization." *European Journal of Clinical Microbiology & Infectious Diseases* 29 (4): (2010): 391-7.

Bleich, Avi, Marc Gelkopf, Yuval Melamed, and Zahava Solomon. "Mental Health And Resiliency Following 44 Months Of Terrorism: A Survey of an Israeli National Representative Sample." *BMC medicine* 4, no. 1 (2006): 21. http://www.biomedcentral.com/1741-7015/4/21

Bleich, Avraham, Marc Gelkopf, and Zahava Solomon. "Exposure to Terrorism, Stress-Related Mental Health Symptoms, and Coping Behaviors among a Nationally Representative Sample in Israel."*JAMA* 290, no. 5 (2003): 612-620.

Bonanno, George A. and John T. Jost. "Conservative Shift among High- Exposure Survivors of the September 11th Terrorist Attacks." *Basic and Applied Social Psychology* 28(4) (2006): 311–23.

Brown, Barbara B., and Paul B. Harris. "Residential Burglary Victimization: Reactions to the Invasion of a Primary Territory." *Journal of Environmental Psychology* 9, no. 2 (1989): 119-132.

Burstein, Paul. "The Impact of Public Opinion on Public Policy: A Review and an Agenda." *Political Research Quarterly* 56 (1) (2003): 29-40.

Canetti, Daphna, Carmit Rapaport, Carly Wayne, Brian Hall, Stevan E. Hobfoll. "An Exposure Effect? Evidence from a Rigorous Study on the Psychopolitical Outcomes of Terrorism." In *The Political Psychology of Terrorism Fears*, edited by Samuel Justin Sinclair and Daniel Antonius, 193-212. Oxford: Oxford University Press, 2013.

Canetti, Daphna., Eric Russ, Judith Luborsky, and Stevan E. Hobfoll. "Inflamed by the Flames? The Impact of Terrorism and War on Immunity." *Journal of Traumatic Stress* 27 (2014): 1-8.

Canetti-Nisim, Daphna, Eran Halperin, Keren Sharvit, and Stevan E. Hobfoll. "A New Stress-Based Model of Political Extremism Personal Exposure to Terrorism, Psychological Distress, and Exclusionist Political Attitudes." *Journal of Conflict Resolution* 53, no. 3 (2009): 363-389.

Carnelley, Katherine B. and Ronnie Janoff-Bulman. "Optimism About Love Relationships: General vs Specific Lessons from One's Personal Experiences." *Journal of Social and Personal Relationships* 9 (1) (1992): 5-20.

Darwish, Ragy, Nadim Farajalla, and Rania Masri. "The 2006 War and Its Inter-Temporal Economic Impact on Agriculture in Lebanon." *Disasters* 33, no. 4 (2009): 629-644.

Diamond, Gary M., Joshua D. Lipsitz, Zvi Fajerman, and Omit Rozenblat. "Ongoing Traumatic Stress Response (OTSR) in Sderot, Israel." *Professional Psychology: Research and Practice* 41, no. 1 (2010): 19.

Farhood, Laila, Hani Dimassi, and Nicole L. Strauss. "Understanding Post-Conflict Mental Health: Assessment of PTSD, Depression, General Health and Life Events in Civilian Population One Year after the 2006 War in South Lebanon." (2013). *Journal pf Trauma and Stress Disorders Treatment* 2:2. https://scholarworks.aub.edu.lb/bitstream/handle/10938/9704/understanding_post_conflict_mental_health.pdf?sequence=1.

Fattouh, Bassam, and Joachim Kolb. "The Outlook for Economic Reconstruction in Lebanon after the 2006 War." *http://web. mit. edu/cis/www/mitejmes* (2006). *The MIT Electronic Journal of Middle East Studies*, 6, 97-111.

Galea, Sandro, David Vlahov, Heidi Resnick, Jennifer Ahern, Ezra Susser, Joel Gold, Michael Bucuvalas, and Dean Kilpatrick. "Trends of Probable Post-Traumatic Stress Disorder in New York City After the September 11 Terrorist Attacks." *American Journal of Epidemiology* 158 (6) (2003): 514-24.

Galea, Sandro, Jennifer Ahern, Heidi Resnick, Dean Kilpatrick, Michael Bucuvalas, Joel Gold, and David Vlahov. "Psychological Sequelae of the September 11 Terrorist Attacks in New York City." *New England Journal of Medicine* 346 (13) (2002): 982-7.

Garfield, R. "The impact of economic sanctions on health and well-being." *Relief and Rehabilitation Network*, London. http://www.essex.ac.uk/armedcon/story_id/The%20Impact%20of%20Econmoic%20Sanctins%20on%20Health%20abd%20Well-Being.pdf. 1999.

Gelkopf, Marc, Rony Berger, Avraham Bleich, and Roxane Cohen Silver. "Protective factors and Predictors of Vulnerability to Chronic Stress: A Comparative Study of 4 Communities after 7 Years of Continuous Rocket Fire." *Social Science & Medicine* 74, no. 5 (2012): 757-766.

Gini, Gianluca, and Tiziana Pozzoli. "Association between Bullying and Psychosomatic Problems: A meta-analysis." *Pediatrics* 123, no. 3 (2009): 1059-1065.

Gottstein, Ulrich. "Peace Through Sanctions? Lessons from Cuba, Former Yugoslavia and Iraq". *Medicine, Conflict and Survival* 15 (3) (1999): 271-85.

Graham, Jennifer.E., Theodore.F. Robles, Janice.K. Kiecolt-Glaser, William.B. Malarkey, Michael .J. Bissell, and Ronald Glaser. "Hostility and Pain are Related to Inflammation in Older Adults." *Brain, Behavior and Immunity*, 20, (2006): 389-400.

Hennessy, John W., and Seymour Levine. "Stress, Arousal, and the Pituitary-Adrenal System: A Psychoendocrine Hypothesis." *Progress in Psychobiology and Physiological Psychology* 8 (1979): 133-78.

Hobfoll, Stevan. E., Daphna Canetti-Nisim, and Robert J. Johnson. "Exposure to Terrorism, Stress-Related Mental Health Symptoms, and Defensive Coping Among Jews and Arabs in Israel." *Journal of Consulting and Clinical Psychology* 74 (2) (2006): 207.

Hoff, Dianne L., and Sidney N. Mitchell. "Cyberbullying: Causes, Effects, and Remedies." *Journal of Educational Administration* 47, no. 5 (2009): 652-665.

Howie, Luke. "The Terrorism Threat and Managing Workplaces." *Disaster Prevention and Management* 16, no. 1 (2007): 70-78.

Huddy, Leone., Stanley Feldman, Charles Taber., and Gallya, Lahav. "Threat, Anxiety, and Support of Antiterrorism Policies." *American Journal of Political Science* 49 (3) (2005): 593-608.

Huddy, Leone., Stanley Feldman, Theresa Capelos, and Colin Provost. "The Consequences of Terrorism: Disentangling the Effects of Personal and National Threat." *Political Psychology* 23 (3) (2002): 485-509.

Keinan, Giora, Nehemia Friedland, and Yossef Ben-Porath. "Decision Making Under Stress: Scanning of Alternatives under Physical Threat." *Acta Psychologica* 64 (3) (1987): 219-28.

Lee, J. "South Koreans Seethe, Sue as Credit Card Details Swiped." *Reuters*, 21 January, 2014. http://www.reuters.com/article/2014/01/21/us-korea-cards-idUSBREA0K05120140121

Li, Qing. "Cyberbullying in schools a research of gender differences." *School Psychology International* 27, no. 2 (2006): 157-170.

Lindgren, G. 2006. *Studies in Conflict Economics and Economic Growth. Report No. 72*, Department of Peace and Conflict Research, Uppsala: Uppsala University

Maguire, Mike. "Impact of Burglary upon Victims," The *British Journal of Criminology* 20 (1980): 261- 275.

Milson, Andrew J., and Beong-Wan Chu. "Character Education for Cyberspace: Developing Good Netizens." *The Social Studies* 93, no. 3 (2002): 117-119.

Newman, Emily., Daryl. B. O'Connor and Mark Conner. "Daily Hassles and Eating Behaviour: The Role of Cortisol Reactivity Status. *Psychoneuroendocrinology* 32 (2) (2007): 125-32.

Nuwayhid, Iman, Huda Zurayk, Rouham Yamout, and Chadi S. Cortas. "Summer 2006 War on Lebanon: A Lesson in Community Resilience." *Global Public Health* 6, no. 5 (2011): 505-519.

Olson, Parmy. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York: Hachette Digital, Inc, 2012.

Pace, Thaddeus W., Lobsang Tenzin Negi, Teresa I. Sivilli, Michael J. Issac, Steven P. Coled, Daniel D. Adamee and Charles L. Raison. "Innate Immune, Neuroendocrine and Behavioral Responses to Psychosocial Stress Do Not Predict Subsequent Compassion Meditation Practice Time." *Psychoneuroendocrinology*, 35(2) (2010): 310-5.

Page, Benjamin. I., &and Robert Y. Shapiro., Robert.Y. "Effects of Public Opinion on Policy." *The American Political Science Review*: 77:1 (1983): 175-90.

Piazza, Pier. V., Veronique Deroche, Jean Marie Deminiere, Stefania Maccari, Michael Le Moal, and Herve Simon. "Corticosterone in the Range of Stress-Induced Levels Possesses Reinforcing Properties: Implications for Sensation-Seeking Behaviors." *Proceedings of the National Academy of Sciences of the United States of America* 90 (24) (1993): 11738-42.

Porcelli, Anthony. J., and Mauricio. R. Delgado. "Acute Stress Modulates Risk Taking in Financial Decision Making." *Psychological Science* 20 (3) (2009): 278-83.

Preston, Stephanie .D., Tony W. Buchanan, Robert B. Stansfield and Antoine Bechara. "Effects of Anticipatory Stress on Decision Making in a Gambling Task." *Behavioral Neuroscience* 121, (2007): 257-263.

Roberts, Lynne D. "Cyber identity theft." *Handbook of Research on Technoethics*. In Handbook of Research on Technoethics edited by R. Luppicini, & R. Adell, 542–557. Hershey, PA*: Information Science Reference*, 2008.

Schlenger, William E, Juesta M Caddell, Lori Ebert, B Kathleen Jordan, Kathryn M Rourke, David Wilson, Lisa Thalji, J Michael Dennis, John A Fairbank, Richard A Kulka, "Psychological Reactions to Terrorist Attacks: Findings from the National Study of Americans' Reactions to September 11." *JAMA* 288 (5) (2002): 581-8.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyberwarfare*. New York: Cambridge University Press, 2013.

Shariff, S., and R. Gouin. "Cyber-hierarchies: a New Arsenal of Weapons for Gendered Violence In Schools." In *Combating Gender Violence In and Around Schools* edited by C. Mitchell and F. Leech, 33-41. London: Trentham Books, 2006.

Sharp, Tracy, Andrea Shreve-Neiger, William Fremouw, John Kane, and Shawn Hutton. "Exploring the Psychological and Somatic Impact of Identity Theft." *Journal of forensic sciences* 49, no. 1 (2004): 131-136.

Silver, Roxane Cohen, E. Alison Holman, Daniel N. McIntosh, Michael Poulin, and Virginia Gil-Rivas. "Nationwide Longitudinal Study of Psychological Responses to September 11." *JAMA* 288, no. 10 (2002): 1235-1244.

Sinclair, Justin and Daniel Antonius, *The Psychology of Terrorism Fears*. Oxford: Oxford University Press, 2012.

Sinclair, Justin and Daniel Antonius, eds. *The Political Psychology of Terrorism Fears*. Oxford: Oxford University Press, 2013.

Sinclair, Justin. (2010). Fears of terrorism and future threat: theoretical and empirical considerations. In D. Antonius (Eds). I*nterdisciplinary analyses of terrorism and political aggression* (pp. 101-115). Newcastle upon Tyne: Cambridge Scholars Publishing

Sinclair, Samuel J., and Alice LoCicero. "Fearing future terrorism: Development, validation, and psychometric testing of the Terrorism Catastrophizing Scale (TCS)." *Traumatology* 13, no. 4 (2007): 75-90

Smith, Peter K., Jess Mahdavi, Manuel Carvalho, Sonja Fisher, Shanette Russell, and Neil Tippett. "Cyberbullying: Its nature and impact in secondary school pupils." *Journal of Child Psychology and Psychiatry* 49, no. 4 (2008): 376-385.

Sourander, Andre, Anat Brunstein Klomek, Maria Ikonen, Jarna Lindroos, Terhi Luntamo, Merja Koskelainen, Terja Ristkari, and Hans Helenius. "Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study." *Archives of general psychiatry* 67, no. 7 (2010): 720-728;

Spielberger, Charles. D., Richard. L. Gorsuch, Robert Lushene, Peter. R. Vagg and Gerald A. Jacobs. Manual for the State-Trait Anxiety Inventory. Palo Alto, CA: Consulting Psychologists Press, 1983

Yehuda, Rachel. "Post-traumatic stress disorder." *New England Journal of Medicine* 346, no. 2 (2002): 108-114.

Zemishlany, Zvi. "Resilience and vulnerability in coping with stress and terrorism." *Israeli Medial Association* 14, no. 5 (2012): 307-309.