TERRORISM AND BATHTUBS:
A LOOK AT CYBER TERRORISM

Nils Tenelsen
University of Applied Sciences Wedel

Written for the IT security seminar overseen by Prof. Gerd Beuster, WS2019
Wedel, January 21, 2019

Abstract

In the past few years a lot of scientists, journalists and public figures have drawn comparisons between the risk of dying in a terrorist attack and the yearly death toll of bathtub drownings and falls. With the rise of this argument also came its critics. These critics generally dismiss the comparison between terrorism deaths and bathtub drownings due to several reasons and have gone so far as to dub it the “Bathtub Fallacy”.

These reasons include but are not limited to the fear and anxiety caused by terrorist attacks, which indirectly raise the cost after an attack has long passed. They also include other factors, such as the generally excessive counter measures to stop terrorism or the driving force of living, breathing terrorists behind the attacks, that will only lead to further, more damaging attacks.

The discussion in this paper is largely based on a paper that was published in the *Terrorism and Political Violence* Journal in October 2018 (“Terrorism and Bathtubs: Comparing and Assessing the Risks” by John Mueller and Mark G. Stewart). [20] The likelihood that anyone outside a war zone will be killed by an Islamist extremist terrorist is extremely small. In the United States, for example, some six people have perished each year since 9/11 at the hands of such terrorists—vastly smaller than the number of people who die in bathtub drownings. Some argue, however, that the incidence of terrorist destruction is low because counterterrorism measures are so effective. They also contend that terrorism may well become more frequent and destructive in the future as terrorists plot and plan and learn from experience, and that terrorism, unlike bathtubs, provides no benefit and exacts costs far beyond those in the event itself by damagingly sowing fear and anxiety and by requiring policy makers to adopt countermeasures that are costly and excessive. This paper finds these arguments to be wanting. In the process, it concludes that terrorism is rare outside war zones because, to a substantial degree, terrorists don’t exist there. In general, as with rare diseases that kill few, it makes more policy sense to expend limited funds on hazards that inflict far more damage. It also discusses the issue or risk communication for this hazard. [20] In the aforementioned paper, Mueller and Stewart raise the points mentioned above, assess the actual difference in risk between terrorist attacks and bathtub drownings and find criticism of the “Bathtub Fallacy” to be lacking.

This paper summarizes their findings in the original paper and draws comparisons to issues in IT security and especially cyber terrorism where applicable. Due to Mueller and Stewart specifically examining Islamist terror in the United States of America, this paper will also largely remain focused on these two parties.

TERRORISM AND BATHTUBS:
A LOOK AT CYBER TERRORISM

It might be surprising that bathtubs are, on average, more lethal over the course of a given year, than terrorism. Precisely because of this, a comparison between the two is frequently drawn. The first side of the comparison is made up of a rather harmless appliance, the other of attacks carried out by organized terror networks. One could argue that this comparison is quite apt in its nature, especially since bathtubs are actually a lot more lethal than terrorist attacks; they kill roughly 400 Americans per annum, while Islamist terrorists only vanquish a relatively little 6 US citizens per year.[20] However this comparison has often been criticized in recent times and even become known under the name of "Bathtub Fallacy". Some critics of the comparison, such as CNN's Jennie M. Easterly and Joshua A. Geltzer, simply dislike the metrics, which are used to carry it out: "Much of the recent debate over the bathtub fallacy has been a statistical one, assessing whether the numbers really bear out the comparison. To us, that's beside the point." [13]

Journalist Jeffrey Goldberg voices a more motif-based criticism and points out that terrorists "seek unconventional weapons that would allow them to kill a far-larger number of Americans than died on Sept. 11." Whereas bathtubs are generally not "engaged in a conspiracy with other bathtubs to murder ever-larger numbers of Americans." (Goldberg, qtd. in "Terrorism and Bathtubs: Comparing and Assessing the Risks") [20] The criticism that most often befalls the bathtub fallacy is made up of a few main points, namely bathtubs are not actively seeking the demise of the American people. Terrorists on the other hand actively pursue this goal while also steadily searching for new ways to achieve it. Here we find the first parallel that can be drawn to cyber terrorism: ingenuity and a steady evolution of the threat one faces.

Next on the list is the amount of counter measures in place to protect against terrorism, without which the risk supposedly would be much greater than they currently are. The parallel to cyber terrorism is not as clear in this instance, but there are some similarities in the way terrorism interacts with countermeasures and a range of common cyber-attacks that either already do or could see use in cyber terrorism.

The third point being is that terrorism, by design, leaves anxiety and fear behind. Or rather sows terror in its wake, thus undermining the general feeling of safety, well-being and trust within a society, while simultaneously causing a growing feeling of helplessness. Therefore,

terrorism should take a large toll on a society that cannot be fully assessed by just looking at the damages caused directly by, and the ground of, a terrorist attack. Again, there is interesting questions that arise in regard to IT security and cyber terrorism: What are the psychological consequences of cyber terrorism and how do they compare to classic terrorism?

Another point is that bathtubs only present a risk due to their intrinsic benefit when fulfilling their main purpose: they can be used to bathe. Terrorism, however, provides no similar benefits. While the same can be said for cyber terrorism, this is only a minor aspect that will not be described in detail.

Finally, there are frequent political responses to terrorism, these artificially increase the costs of terrorism as officials are put under pressure by the public and opt to adopt excessive counter measures. Here the paper will simply shine a light on proper political responses that could be taken in a reaction to terrorism. However an apt comparison can hardly be made as cyber terrorism has neither been uniformly addressed in the public nor have there been a lot, if any, cyber terrorist attack of public interest yet. [17]

Cyber terrorism

In order to understand cyber terrorism and draw parallels between it and traditional terrorism, one needs to know what cyber terrorism is, by which means it may be conducted, and how it differs from conventional attacks. The difficulty in doing so lies in the various existing definitions of the term. There is no single widely agreed upon definition of cyber terrorism and, even when they apply the same definition, different people often reach separate conclusions when reviewing the same incident. [10] Cyber terrorism is extremely similar to terrorism in this regard. Some definitions simply include any and all cyber-attacks with the classical motivations of terrorism, others may even include attacks that simply aid in conventional terrorism. However, some definitions are more strict and only include attacks that either cause physical destruction or aim to at least harm, if not outright kill, humans. This fuzziness of definitions can make it hard to distinguish between common cyber-crime, cyber terrorism, even cyber warfare, and the more widely known hacktivism conducted by groups such as Anonymous. The issue does not stop there though, as certain incidents may be considered to fall into any of the above categories depending on the perpetrators; however, those are not always known. although this will not be as prevalent when using definitions that use physical harm as a requirement for cyber terrorism, as there have barely been any attacks that fulfill this prerequisite. [17]

Definitions of cyber crime

According to a 2000 report for McConnell International cybercrime can be defined as "harmful acts committed from or against a computer or network". [21] These cyber-crimes are different from conventional crime mostly because they can often be committed from anywhere outside the jurisdiction of the target, require a relatively small investment of resources, and regularly find themselves in legal grey areas. Ayofe and Oluwaseyifunmitan, who cite the above report in their 2009 article in the International Journal of Computer Science and Information Security, also note that other definitions exist, which may restrict cyber-crime to strictly illegal activities that aim to undermine the security of a computer system itself or the data stored therein. [2] In general, cyber-crime is a lot more clearly defined and easier to discern than cyber terrorism, although it too has varying definitions. A general consensus exists that it involves harmful attacks, albeit these attacks might not necessarily need to be strictly illegal depending on the definition.

Definitions of hacktivism

Hacktivism can be said to act as a bridge between conventional cyber-crime and outright cyberterrorism. It fuses hacking with political activism. The methods of hacktivism are no different than in conventional hacking. Only the motivation and goals of the hackers differ. They typically only disrupt service without leaving long-term damages. The deployed attacks can cause a plethora of different disruptions, the variety of attack types does not differ much from classical hacking. [8] An example is swarming also referred to as "virtual sit-ins", these attacks work similarly to DDoS attacks and generate a lot of traffic on the target server; however, they only make it harder to reach without the intent to crash the server or even corrupt data by doing so. These attacks also may not be conducted anonymously and often will involve political messages left as part of the attacks akin to physical political activists. [9]

Definitions of cyberterrorism

A 2013 paper published in the *International Journal of Network Security* defines cyberterrorism as follows: "The use of Internet based attacks for terrorist activity including acts of deliberate large scale disruption of computer networks by use of tools such as computer viruses." [24] While this definition does not include the previously mentioned loss of life or destruction of property, it opens up other uncertainties. The definition is not only dependent on an accurate and constant definition of terrorism, it also does not clearly define what "use for

terrorist activity" is. Depending on interpretation this might only include the direct use in an attack attempting to sow terror. It could on the other hand also include the mere gathering of intelligence or stealing of funds through hacking.

It is often acknowledged that too narrow a definition would lead to the exclusion of many large-scale attacks on the fringe of cyberterrorism, while too broad a definition would result in countless instances of mere cyber-crime (e.g. the aforementioned securing of funds) into cyberterrorism. Although generally it can be assumed that cyberterrorism is politically motivated and seeks to intimidate or even coerce a government or its people. Another part of a number of definitions is the targeting of civilians. [19] Oftentimes sources even explicitly dismiss the loss of life or destruction of infrastructure as a prerequisite for cyberterrorism and go as far as to label certain attacks as "seemingly banal". [14]

OPIsrael

The hacktivist group *Anonymous* targeted Israel in a rather well known set of 2015 cyber-attacks. The targets of the attacks were a selection of Israeli websites, although no government sites were directly targeted. This attack was also dubbed an electronic Holocaust against Israel. [7] The goal of these attacks was to take a stand in support of the Palestinian side in their conflict with Israel. Although the attack is generally be considered mere hacktivism, they are a great example of the blurry lines between cyber-crime, hacktivism and cyber terrorism. The main reason for this is that they are sometimes also seen as cyber terrorism. This is mostly due to them taking sides in an ongoing armed conflict, thus elevating the actions of *Anonymous* above comparatively harmless criminal actions. [14]

Definitions of cyber warfare

Similarly to the difference between hacktivism and cyber terrorism, it is also hard to make a clear cut between cyber terrorism and cyber warfare. It could be seen as being merely another battlefield in conventional warfare. Although this is a rarely adopted viewpoint, it does exist. A more generally accepted stance would be the definition as large scale assaults coordinated by one government onto the other with the goal to penetrate computers and networks in order to cause destruction or disruption. This already reads eerily similar to the definitions of cyber terrorism. However, cyber warfare may even include actions taken by "large groups of citizens", thus introducing assaults similar to civil cyber war making the lines between cyber warfare and cyber terrorism even blurrier.

One key difference distinguishing cyber warfare and conventional warfare is the anonymity of cyber warfare, where the attacker cannot always be clearly determined. In some instances cyber-attacks have been used as part of a larger armed conflict, for example when Russia disrupted Georgian communications in 2008. [23]

Attacks on Estonia

In 2007 there was an ongoing political conflict between Estonia and Russia, where the Estonians removed a Soviet era statue in Tallinn sparking widespread protests by ethnic Russians within the country. After the statue was down a wave of DDoS attacks against Estonian websites started. The Estonian government immediately jumped to the conclusion that Russia had to be behind the attacks, even bringing these accusations to the attention of NATO and bringing the topic up in talks with US President Bush. [6]

While the attacks seem to have originated in Russia, no evidence of direct involvement of the Russian government was found. This attack was of a comparatively minor scale compared to the possibilities e.g. the USA possess, but this still resulted in Estonia being assured NATO backup in case Russia was indeed responsible for the attacks. [23]

Likewise to OPIsrael, this attack illustrates a blurriness in definitions, in this case due to the perpetrators being unknown. Were these attacks indeed perpetrated by Russian officials, one would most likely consider them a minor cyber war. Another possibility would be Russian hacktivists as the perpetrators, which would make the attacks Hacktivism, but given the involvement of NATO and other international parties like the US they would be more likely classified as cyber terrorism.

Stuxnet

A highly sophisticated computer worm discovered in 2010. The involvement of a government in its development is strongly suspected by experts around the world. The worm was initially introduced via an USB stick, while worms normally are spread via the internet. A USB stick was limited to only three infections. When three systems have been infected no further manual spread using the same USB stick is possible. The worm also limits its own spread and will only attempt to further infect other systems for 21 days. Other atypical aspects include two stolen certificates used to mask the worm as well as four included zero-day windows exploits. This number exceeds anything included in a singular piece of malware before. Since the worm was targeted at the Iranian nuclear program, it only targeted systems running relevant controllers

for physical processes (specifically Siemens programmable logic controllers) in which it later injected code to achieve its goals. The governments most likely to be responsible for Stuxnet are the US or Israel. [6]

One of the main distinguishing factors between the damage caused by Stuxnet and that caused by cyber terrorism is their purpose. In case of Stuxnet this was not to cause terror, but most likely to disrupt the Iranian nuclear program and to warn the Iranian government not to pursue the venture further. Which it is believed to have achieved successfully.

Whether other hackers copy Stuxnet or merely let themselves be inspired by its achievements, the worm and other similar effects have likely accelerated the development of cyber terrorism. As they are now in the hands of countless hackers around the world and furthermore demonstrate that targeting physical systems such as industrial machines or elevators is very much possible and thus should not be ignored as a possible attack vector of cyber terrorism. [17]

Evolution of terrorism

The first main point of critique that frequently hits the "Bathtub Fallacy" comes in the form of bathtubs simply being unwilled objects. One of the main critics, Janan Ganesh, said "Bathroom deaths could multiply by 50 without a threat to civil order. The incidence of terror could not." (Ganesh, qtd. in "Terrorism and Bathtubs: Comparing and Assessing the Risks") [20] This implies it is not only more likely for the direct threat presented by terrorism to change than that presented by bathtubs, it would also have unproportionally higher consequences. As Jeffrey Goldberg puts it: "seek unconventional weapons that would allow them to kill a far-larger number of Americans than died on Sept. 11." and "the fear of terrorism isn't motivated solely by what terrorist have done, but what terrorists hope to do." (Ganesh, qtd. in "Terrorism and Bathtubs: Comparing and Assessing the Risks") [20] Often times critics note that terrorism deaths could not only multiply, but terrorist constantly seek for more effective ways and weapons to kill Americans. But is this truly valid criticism of the comparison between terrorism and bathtubs? Mueller and Stewart use the 9/11 attack as a reference. Surely given the supposed drive of terrorists, after there had already been such a destructive attack in 2001 there would have been others following its path coming close to the previous destruction, or even surpassing the 9/11 attacks? In order to properly compare committed attacks, they reduce their outlook to terror attacks committed within in the Western world that were under the "command and control"

of Al-Qaeda Central, the original core of Al-Qaeda, who were responsible for 9/11. They only find two such attacks, which, according to them, “failed miserably”. It is also noted that given the supposed constant drive to seek more destruction and the ingenuity attributed to terrorism, it is hard to see, why they did not simply employ simpler methods that have generally proven more effective in other parts of the world. As attack vectors like simply shooting people in large groups require less logistical challenges and significantly lower amounts of planning or man power, yet they have not been executed. [20] However, which attacks truly were controlled by the Al-Qaeda core, is not easy to define. Other sources have other opinions, some even attribute multiple, very successful attacks in the West to the group, such as the Madrid and London Metro bombings in 2004 and 2005 respectively, which killed a combined number of 243 people. [5] While this may seem very different from two attacks that failed on to inflict significant loss of life, in reality, it supports the same point. The very same group, who orchestrated the 9/11 attacks did indeed not become more vicious or dangerous. In fact, they did not even inflict 10% of the casualties suffered on 9/11 during the next decade of the Western world.

Another specific way, in which terrorism would was often predicted to evolve over the past years, was the gradual incorporation of weapons of mass destruction, most alarmingly nuclear weapons, into terror attacks. Theodore Taylor for example even went so far as to say that it was already too late to prevent terrorists from acquiring nuclear weapons and even said “in another ten or fifteen years, it will be too late.” (Ganesh, qtd. in “Terrorism and Bathtubs: Comparing and Assessing the Risks”) [20] However, even now, almost 20 years later there have not been any condemning signs of terrorists groups being in the possession of nuclear arms, or even made any notable progress towards this goal. Given the difficulties and logistical requirements in developing such a weapon this should come as no surprise. However, there is also at least some evidence to back this speculation up. In 2001, an Al-Qaeda computer was seized in Afghanistan, its data indicating the group merely attributed a couple of thousand of dollars towards researching weapons of mass destruction and even less towards nuclear ones. This evidence was further cemented in the surroundings of the killing of Osama bin Laden, were another secured computer suggested the group had all but abandoned any efforts in this direction and also did not possess the means to change this course.

The now prevalent use of vehicles in attacks appears to be the only a noticeable change in the execution of terrorist attacks; one example being the 9/11 attacks themselves, which with

the direct use of planes presented an even bigger change in attack vector and destructiveness compared to other attacks. Thus Mueller and Stewart dismiss the innovation potential and capability of terrorist groups as “confused, inadequate, incompetent, blundering and gullible” and their schemes “frenetic and often self-deluded”. [20]

Zero-day exploits

Akin to the development of the IT-industry as a whole zero-day exploits are a good example to distance cyber terrorism and even conventional cyber-crime from the stagnation of conventional terrorism presented above. There has been one use case of zero-day exploits that stands out as being extremely relevant to terrorism and the topic of this paper: The usage of at least 4 zero-day exploits of Microsoft Windows in the now infamous worm Stuxnet. [17] Zero-day exploits include any variety of exploit or vulnerability that is known to an attacker without the developer of the target system or, more importantly, the public being aware of said vulnerability. The intrinsic danger of zero-day exploits lays in the mere fact that they are unknown, thus they are virtually impossible to detect prior to disclosure. Indeed, hackers are sometimes so far ahead of developers that a bounty market of both developers and other hackers competing to buy zero-day exploits from their discoverers has sprung up. [12] The existence of such a market might suggest that these exploits are often quickly known to the developers. However, this is often not the case. Since these vulnerabilities are easily exploited by an attacker and in their unknown nature are very hard to detect, they offer an immense value to attackers and developers alike. Due to their nature, it is hard to collect comprehensive data on zero-day attacks, as they generally only become known after an attack has concluded. However, some studies have been conducted. One such study remarks that only 65% of publicly disclosed zero-day exploits have fixes available for them when they are being disclosed, thus an exploit originally only used by the original hackers can be used by a plethora of hackers around the globe with extreme effectiveness, albeit only briefly until anti-virus vendors and the developers of the system have reacted and patched the vulnerability. Some of the examined exploits have only been used in attacks for a couple of weeks, while others have been in use for up to 2.5 years, this long-term exploit being Stuxnet. Unlike Stuxnet, most of the examined exploits have been extremely targeted attacks. Most single day exploits appear to be targeting only a single host. Naturally, with the viability of an exploit being largely dependent on being undetected, these specifically

targeted exploits would most likely not be sold on the black market, but be discovered during unrelated testing or released after the attacks have already concluded. [4]

While the market of selling zero-day exploits may be seen as a positive influence, both granting awareness of security risks and potentially forming lasting bonds between developers and white hat hackers, they are also often seen critically. As this practice may even encourage illicit behaviors such as actively planting bugs to sell, creating a bigger incentive for people to find exploits in the first place, making developers aware of more risks, but also creating new exploits on the flip side. Others argue resources allocated to buy out zero-day exploits might simply be better allocated in other means of IT security. [12]

Effectiveness of countermeasures

The next point of criticism concerning the "bathtub fallacy" is the existence of a large amount of counterterrorism measures and while shower mats, instructions for parents, handlebars etc. exist their use is not mandated or widespread enough to be examined further. [20] Terrorism attacks on the other hand supposedly get thwarted so effectively by government measures that terrorism appears much less dangerous than it truly is. Once again Mueller and Stewart analyze Islamist terror, as opposed to terrorism as a whole. They note that there have been 124 known Islamist attacks between 9/11 and 2017. Of these attacks an impressive 97 have been stopped by authorities, before they could be carried out. The remaining 27 were indeed successful, albeit only ten attacks resulted in deaths. This leaves the overall tally of deaths from these 124 plots at around 6 per year. Considering the thousands of deaths caused by 9/11 this number does not seem alarming at all. There would of course have been a risk presented by the 97 thwarted attacks, had they not been detected by authorities. However, Mueller and Stewart dem this risk as relatively minor, as the failed plots mostly included the more amateurish plots. According to them the schemes were "inept" and "incoherent", "their organizational skills close to non-existent". The failed schemes that did not have said weaknesses usually were aided by FBI infiltrators. Due to these weaknesses of the thwarted attacks, they suggest they could have potentially increased the death toll to anywhere between 12 and 18 yearly deaths. While this would be an increase of 50% to 100% it is still a very small number, considering it would be attributed to all known Islamist terror targeting the US, especially when compared to the 400+ bathtub drownings in 2011.

At this point, one has to consider plots that have not been disclosed to the public, their existence is also an often-cited argument. As Journalists, Terrorism experts and former governments operatives put it though, there is no knowledge of any significant plots ever having been hidden after they were stopped. In fact, the notion of not disclosing these successes would counter act the political goals often found to motivate counterterrorism measures.

No-entry measures are a commonly known type of counterterrorism measure. Similarly to stopping plots already in motion, these do not seem to have an enormous effect though, as there are no known terrorist operatives that are known to have infiltrated the US to commit an attack in the years after 9/11. While this could be interpreted as no-entry measures being virtually impenetrable, it seems more likely that there simply have not been many infiltration attempts. At this point, a comparison to a European country is in order. The UK spends roughly half as much on counter terrorism as the US, yet have an average of 5 terrorism related deaths per year from 9/11 up to and including 2016. While this number is relatively close to the US statistics even though the UK has a significantly smaller population, one has to note such as this number including all kinds of terrorism, not only Islamist attacks, the lesser counter terrorism expenses of the UK and the already existing large Muslim population in the UK, making no -entry measures somewhat less effective by nature. All this suggests that counter measures and specifically no-entry measures are not extremely effective at all.

But could it not be that the mere existence of all these counter measures already dissuades many terrorists from carrying out their attacks? The article concludes that this is also unlikely, as the vast amount of security measures is concentrated around protecting certain high value targets, such as military targets or aircraft and airports. However, spending so much on protecting specific targets does little to reduce overall terrorism on country level. An abundance of other, unprotected targets is always in reach: trains, malls or any crowd come to mind. Examples of this are attacks like the Boston Marathon bombings in 2013 or the Charlie Hebdo attacks, which focused on unpredicted, relatively easy to hit targets. [20]

Relevance for IT security

A key difference between counterterrorism measures and those against cyber terrorism is that counters to cyber terrorism have more benefits related to general security. As elaborated earlier, cyber terrorism uses the same tool kit as conventional cyber-crime. Thus, any measure against cyber terrorism also works towards IT security in general. In some way cyber-crime is

distinct from cyber terrorism though. The deterrence aspect of security does not work on a lot of cyber-crime, as a lot of worms, viruses or phishing scams are designed to attack as many targets as possible. They do not have a specific target and have a very generic goal. Even the extremely selective worm Stuxnet, which did indeed have a specific target, infected multiple thousands of devices. [4] Due to the same reasons as conventional terrorism the overall amount of cyber terrorism, regardless of attack method, is not much affected by deterrence issues. An attack would likely only be aimed at and tailored towards a single, specific target, with the goals of the attack being to inflict damage, to cause terror or to take lives. However, these goals are extremely generic in nature and could also be achieved attacking virtually any of the vast amounts of other targets in the world. Although a failed attack would still be a setback for the attacker, as the time and resources invested into reconnaissance would be, this does not present a large setback compared to e.g. being arrested. A similarly oriented attack in normal cyber-crime could for example be a personalized phishing attack that is after money, instead of a more personal target, possibly sensitive data sets or similar assets. An example of such an attack can be found in Attachment 1, where an attacker researched the work environment of an employee (anonymized as Margo R. Spiegelman) and proceeded to impersonate an existing coworker needing urgent help. The target was researched, a fake email account impersonating the coworker created and a somewhat plausible scenario was manifested. The attack had a very specific target, very much like terrorist attacks, however the goal of this phishing attempt was to acquire steam wallet funds purchased in a corner shop, this again, like with terrorism, is a very generic goal. In this case Mrs. Spiegelman reacted intelligently and only replied in short sentences, not revealing any further information, nor did she purchase the funds. However, such cleverness or specific training on a small scale will not reduce the prevalence of such phishing attempts overall, as there will always be a million other phish left in the target pool who do not have such protection.

While no-entry measures, border controls or similar measures will not do much against cyber terrorism, it does share one major quality with conventional terrorism: It is a multinational crime. It is even possible to commit an attack from multiple different countries without any one of the attackers ever entering the targeted jurisdiction. Moreover, the difference in jurisdiction might even result in an attack not being illegal in its origin jurisdiction. Both this internationality and the resulting fuzziness result in international cooperatives. Both prosecution as well as

defining proper international laws on cyber-crime and cyber terrorism would be sensible courses of action. [19]

The grand deterrent

Lastly, there is one enormous form of deterrence, which does not really exist in IT security. It is what Mueller and Stewart simply call the "grand deterrent", a collection of characteristics sometimes attributed to the general lack of terrorism attacks. They suggest terrorism simply is not the best course of action in most scenarios, as terrorism is impractical, "counterproductive" and has a certain "fundamental absurdity" to it. [20] Terrorist attacks simply are not common because terrorism itself is a very unappealing enterprise and thus largely does not exist. [20]

Fear and anxiety caused by terror

One of the main goals of terrorism is, of course, to stoke fear and anxiety, or in other words to sow terror. Naturally, this is used in the next counter point against the "bathtub fallacy", while bathtubs may cause more deaths than terrorism, these deaths are have less of a lasting impact on people not directly related to the victim and thus have a lesser lasting impact on society than the fewer deaths caused by terror.

On a first glance at poll data presented by Mueller and Stewart, this notion seems to hold true. About a quarter of Americans felt like their lives had changed permanently following 9/11, with half of them thinking their fellow citizens had changed their ways permanently following the attacks. Curiously, these numbers even rose slightly after 2007 (Figure 1). A similar trend can be spotted in poll results, when they were asked whether their lives would ever return to a normal state (Figure 2). A significant number of Americans have attested to changing their lives and being less inclined to travel overseas (about 50%), attend large-scale events (40%), travel by plane (30%) or enter a skyscraper (20%). While these numbers have initially declined overall, they rose after 2011 to reach their current levels, which are roughly like those directly following the 9/11 attacks (Figure 3). These numbers coincide with the share of Americans feeling their country is less safe in the wake of 9/11, which also show a rise starting 2011, now standing at about 50% as well (Figure 4 and 5).

When asked about their actual life circumstances outside of the context of terrorism, however, these numbers do not seem to reflect reality. Terrorism has remained low on the list of biggest problems Americans see the country facing. With less than 10% of people ranking it as

the countries top issue in their eyes for 10 years following 2007, with only one poll conducted shortly after the attacks in Paris in winter 2015 rising just slightly higher (Figure 6). More than 85% of Americans even were at least somewhat satisfied with their personal safety in 2014, a number almost up to par with polls in 2001 and noticeably above those conducted in 1998 (Figure 7). More importantly, the number of Americans satisfied with their general quality of live has not dropped significantly following the 9/11 attacks, with the only noticeable dip in satisfaction occurring when the 2008 financial crisis hit the world (Figure 8).

The behavior displayed by the American people also disagrees with their statements about permanently changed lives. As people are not avoiding the targets of the attacks, with real estate prices rising in both, Washington D.C. and New York, attendance figures of football games rising continuously from 2000 to 2003 without any noticeable impact of 9/11 and cinema revenue also increased post 2001. While some attacks did have local effects, like the May 2017 Manchester bombings, which did hamper tourism quite noticeably, this dip has not lasted until even the end of the year and might even partially be explained by events scheduled in the targeted arena having to be cancelled, as opposed to any fear of terrorism. Such effects do not have to be economic net negatives for a country, the 2005 underground bombings in London are a great example for this. While tourism in London did sink for a while, it simultaneously rose in other parts of the country. Generally, most countries can withstand the effects of terrorism, which usually are not very severe nor possess any notable longevity or more than regional impact. [20]

Fear and anxiety induced by cyber terrorism

Cyber-attacks can have lasting psychological impact on a person, types of attacks where this is especially prevalent are e.g. identity theft or extortion via stolen sensitive data. These often leave victims feeling powerless, in a state of blaming themselves, or even a fear of new technologies. However, these are rather extreme examples. More often reactions include a feeling of being cheated, anger or mere annoyance. Only roughly 9% of people feel very safe online, yet, likely due to the rather mild emotional reactions described above, only half of adult internet users would change their online behavior after becoming a victim.

The reactions to large scale attacks are dependent on many factors, such as the overall scale, which might not be known when an attack is disclosed to the public, the perpetrators or even the target selection, where a large group of randomly selected individuals would cause less distress than a single attack on one localized, but important target. [3]

Researchers from the University of Haifa conducted a set of studies on the psychological impact of cyber terrorism on the populace, also including conventional terrorism in their studies to create a reference. The majority of the questions were answered on the base of a Likert scale [1] adapted to the particular question, while the data regarding anxiety was acquired employing the State-Trait-Anxiety Inventory, a widely spread set of questions used to measure anxiety. [18]

The studies were conducted questioning Israeli population. While similar results have also been found in US studies on conventional terrorism, the results cannot be perfectly matched to the US populace. Their findings, however, were still very much interesting. [14] For example, subjects presented with news coverage of a fictional cyber terror attack did indeed feel substantially more anxious than individuals that were not presented with any terrorism at all. However, the difference between lethal and non-lethal cyber terror was relatively small, at only 0.2 on a 4 point scale, while conventional terrorism on the other hand saw anxiety levels rise to 0.4 points higher than even lethal cyber terrorism did reaching the highest end of the scale at 4 (Figure 9). Their data on fear (Figure 10) paints a very similar picture: cyber terrorism, does increase fear in the population, lethal cyber terrorism even does so only to a slightly lesser extent than non-lethal cyber terrorism. The studies further inquired what measures people would see as appropriate in the aftermath of an attack (Figures 11 & 12). Here they only looked at cyber-attacks one group being presented with the Hamas as perpetrators, the other with Anonymous. These are two factions with significance for Israel, the Hamas of course being in a yearlong armed conflict with Israel. While Anonymous have conducted OPIsrael, a “digital holocaust” on Israel. While both groups were eager to at least implement some counter measures, the Hamas generally sparked a greater response. With more people supporting the monitoring of Facebook or Twitter and the amount of people who supported the government spying on emails even doubling when faced with the Hamas. A similar trend was seen in the groups questioned on possible retaliation strategies. People generally supported harsher measures when the Hamas were the perpetrators. Especially when asked about physical force in response to an attack, the Hamas group was more favorable. With 50% more supporting strikes against “military” targets (infrastructure used or usable to conduct the attacks), more than twice the amount of support for physical strikes against both military and civilian targets. This might, however, not only come down to the threat seen in Anonymous, but the Hacktivists being more spread out and isolated around the globe, it would simply be harder to carry out physical strikes against them. This is

supported by the figures regarding retaliation via cyber-attacks, where attacks only against "military" targets have wider support among the Anonymous group. Strikes on civilian targets are once again enjoying higher support among the Hamas group, however.

It appears like cyber terrorism has a very similar effect on the populace as conventional terrorism, with even non-lethal attacks having a noticeable negative effect on the population. However, conventional terrorism still reigns supreme in its ability to sow terror, as both conventional terror attacks and cyber-attacks conducted by terrorist prompt a harsher reaction, with the political reaction to attacks carried out by the Hamas being more extreme than that reacting to a Anonymous posing a threat. However, both groups supported actions could still have negative attacks on a democratic society, possibly even with global impact. [15]

Cost-benefit analysis of terrorism

Another way to assess the psychological costs of terrorism is to look at the monetary costs associated with the loss of lives. Conventionally, the cost of a single human life is estimated at $7.5 million (Lisa A. Robinson et al, qtd. in "Terrorism and Bathtubs: Comparing and Assessing the Risks"). [22] Mueller and Stewart use this estimate along with other estimates for property damages and other societal damages not included in the estimate of $7.5 million to compare the costs of various terror incidents to those associated with bathtub drownings over a single year (Table 1). They do not provide a full analysis, but they do manage to put the numbers into perspective to counter measures employed in the US. It is of note that the costs estimated for most terrorist incidents even exceed those that would be reached when following the recommendation to double the costs per life issued by the Department of Homeland Security. [22] Using these estimates, the 9/11 attacks reach a cost of $250 billion. Other incidents reach significantly lower amounts. The London underground bombings of 2005 merely reach a $5 billion tally, while the Boston Marathon bombing only reaches a grand total of $500 million. For reference the yearly costs for domestic counter terrorism, so excluding any international efforts and the anti-terror wars waged over seas, amount to $115 billion. In order to be cost effective, these measures would thus have to prevent a 9/11 scale event biannually or 230 attacks per annum that are on the scale of the Boston Marathon bombings. Given the previously mentioned total of 124 known Islamist plots, these numbers are unlikely to ever be reached.

Bathtubs drownings on the other hand reach a total yearly cost of roughly $3.7 billion, putting them in the close vicinity of the London underground attacks. [20]

Bathtub drownings in comparison to other hazards

Bathtubs provide a benefit to their users. Terrorist attacks usually do not provide comparable benefits, at least not for their victims. This distinction is an important one to make, as there are certain hazards, e.g. traffic or industrial accidents, which only happen in the context of providing benefits. In such cases human are much more willing to accept a risk. In 2014, more than twice as many people died on US roads than were killed in homicides. Yet, cars are still widely accepted due to the comfortable transportation they provide, even though safer alternatives exist. When a hazard does not provide a benefit to the populace, it is much less accepted by society. The cut off for a risk that is deemed too high, when no benefit is provided, can be estimated to lie at roughly one death per million people per annum. This would amount to somewhere in between 300 and 400 deaths when extrapolated onto the entire population of the US. Bathtub drowning exceeds this threshold, but, as established above, they provide a benefit; thus, their risk is deemed acceptable. Terrorism only kills roughly 6 people per year in the US, a number noticeably under the threshold, yet there are enormous undertakings taking place to counter it, most likely due to political pressure due to the perceived threat of terrorism, not due to the actual threat presented by it. Even terrorism between 1970 and 2016 in the UK, so including most of “The Troubles”, does not exceed the number of 1 yearly death per million inhabitants. [20] For context from 2006 to 2015, 31 people died of lightning strikes every year, [16] 5 times as many as from terrorist attacks, yet, no special counter measures have been taken up to defend against lightning attacks.

Political overreaction

Any political reaction to terrorism is, in part, a success for the terrorists. Terrorism usually does demand the attention of politicians, even though the actual consequences of it might be comparatively minor. Citizens will still want to feel protected from targeted, violent death much more than from e.g. bathtubs. Terrorism is far more in the focus of the public eye than bathtub drownings, thus politicians feel forced to turn their attention towards terrorism. But are their actions justified? Are they expected? Or are politicians overreacting to terrorism? Judging it to be a far bigger threat to their country and their careers than it is in reality?

The authors of the original paper, Mueller and Stewart, think that politicians often do not need to react much at all in response to terrorism. [20] A hard to miss example for this are the wars in Iraq and Afghanistan. Both were not directly demanded by the public at the time. George

W. Bush had to react in some manner, but invading foreign countries was by no means a political necessity. In the case of Afghanistan, the country had a government, the Taliban, which while not at all perfect allies most likely would have cooperated with the US to reprimand those responsible in some way. Had they not they would have been largely alone on the world stage, with even their allies at the time, Pakistan and Saudi Arabia, expressing their support of the US. In fact, Saudi-Arabia even tried to extract Osama bin Laden for years prior to the 9/11 attacks. While the Taliban did eventually agree to hand over bin Laden to any country in the world, they did not agree to hand him over to the US, which then turned down negotiations. Even dismissing such comparatively easy deals, there were still more targeted measures, like selective bombing or targeted raids, that could have been taken instead of a ground invasion.

The war on Iraq happened in a different situation, as Americans were still extremely hostile towards Saddam Hussein due to the aftermath of the Gulf War. Support for militarily deposing of Hussein was as high as 50% even before 9/11, rising up to 75% after the attacks, but quickly falling back down. Even targeted campaigns to raise war support prior to going to war in 2002 did not achieve significant changes. While Bush did declare a war on both countries, he did not need backing of the public to do so.

Both wars combined cost $750 billion, only up to 2009, [11] adding up to a yearly cost of roughly $93 billion, not far off the $115 billion spend on domestic counter terrorism per year. Thus, these wars were not only a huge commitment of lives, they also doubled anti-terrorism expenses by themselves. Therefore, it should be further investigated whether such a drastic course of action was truly necessary.

Previous presidents and their actions, however, suggest that such a reaction was overblown and not necessary to keep public peace. While prior attacks of course were not as deadly as the 9/11 attacks, the responses to the previously biggest terror attacks on the US were all but extreme. Ronald Reagan for example held speeches to condone the victims of the 1983 bombings in Lebanon and eventually recalled the US military from the country. Following the 1988 Lockerbie plane bombing, the government simply conducted a thorough inquiry to find the culprits and eventually did identify them in cooperation with British police. This approach of simply thoroughly investigating the incidents, was the norm across the Western world, with no discernible negative impact on e.g. Reagan’s reelection.

As established earlier, Americans still feel relatively unsafe due to 9/11 with no apparent changes due to counter policies. There were certain periods of short alleviation, e.g. when bin Laden was killed, but these have mostly been temporary (Figure 5). Counter measures have failed to create a feeling of safety in the US. Even though the public never demanded specific measures, only that any measures should be taken. The proper course of action would thus be to employ risk analysis and cost-benefit procedures to determine the most effective policies. However, even government agencies attest that this largely has not been done. Instead, officials followed a policy of using as many security elements as possible, regardless of their effectiveness and associated costs, creating a wholly inefficient counter terrorism machinery.

Not only did more tame reactions in previous years not negatively impact elections. Politicians even openly made remarks regarding how much of a non-issue terrorism is for the average citizen and the country. Both, President Obama and Michael Bloomberg, former Mayor of New York City, made public remarks dismissing the dangers of terrorism without noticeably repercussions in the following elections. This however does not change the way the public thinks. Acting at all, even if not effectively to stop terrorism, is generally considered the safer route. [20] A politician implementing counter measures can hardly be proven wrong: When no attacks occur the measures are successful and if an attack does occur the political direction was still correct. A politician not implementing counter measures, though, always faces the risk of becoming a scape goat for attacks happening in their terms, thus most politicians opt for exaggerating the dangers of terrorism and acting accordingly. [20]

Conclusion

The dangers and risks of terrorism appear to be largely overblown, at least when one does not include terrorism outside the Western world. Terrorists fail to become more threatening and generally do not plan many attacks on the West. The biggest success of terrorism seems to be counter terrorism itself, effectively wasting billions of Dollars. Ironically, successful terrorism thus directly makes further acts of terrorism harder. It is advised to seek de-escalation of the issue, both, from the public side and politicians, as at the moment both exaggerate the issue to one another, with politicians seeing a non-existent political necessity to act, therefore overexaggerating the dangers themselves and stoking a public response of fear that otherwise would possibly not have occurred.

Cyber terrorism is a separate issue, though, and should be focused on more. It encompasses the very same risks as conventional terrorism, if not more, but is easier to commit with limited man power or funds and can even be started at the hands of splintered groups across the world, that are even harder to crack down on than conventional terrorists. While no deadly cyber terror attack has yet occurred and conventional terrorism is not very widespread, effective measures against cyber terrorism would also defend against cyber warfare, another ever growing concern in modern society.

References

[1] Elaine Allen and Christopher Seaman. Statistics Roundtable: Likert Scales and Data Analyses. *Quality Progress*. Retrieved January 16, 2020 from http://rube.asq.org/quality-progress/2007/07/statistics/likert-scales-and-data-analyses.html

[2] Azeez Nureni Ayofe and Osunade Oluwaseyifunmitan. 2009. Towards Ameliorating Cybercrime and Cybersecurity. *International Journal of Computer Science and Information Security* 3, 1 (2009). Retrieved from https://pdfs.semanticscholar.org/cfd8/b70276ea5ac7d534ba2768723a0a9ce02325.pdf

[3] Maria Bada and Jason R.C. Nurse. 2020. The social and psychological impact of cyberattacks. In *Emerging Cyber Threats and Cognitive Vulnerabilities*. Elsevier. DOI:https://doi.org/10.1016/B978-0-12-816203-3.00004-6

[4] Leyla Bilge and Tudor Dumitras. 2012. Before we knew it: an empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12*, ACM Press. DOI:https://doi.org/10.1145/2382196.2382284

[5] Daniel Byman. 2019. Does Al Qaeda Have a Future? *The Washington Quarterly* 42, 3 (July 2019). DOI:https://doi.org/10.1080/0163660X.2019.1663117

[6] Thomas M. Chen. 2010. Stuxnet, the real start of cyber warfare? [Editor's Note]. *IEEE Network* 24, 6 (November 2010). DOI:https://doi.org/10.1109/MNET.2010.5634434

[7] Matthew S. Cohen, Charles D. Freilich, and Gabi Siboni. 2015. Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives* (December 2015). DOI:https://doi.org/10.1093/isp/ekv023

[8] Maura Conway. 2007. Cyberterrorism: Hype and Reality. In *Computer Fraud & Security*. Retrieved from https://pdfs.semanticscholar.org/e30f/ca854868b1ef0066a17ce54af94e86626ce6.pdf

[9] Dorothy E Denning. 2000. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In *Networks and netwars. The future of terror, crime and militancy*. Retrieved from https://pdfs.semanticscholar.org/cf05/5fd12c0fecf64b777a26aff07c5260d553f5.pdf

[10] Murat Dogrul, Adil Aslan, and Eyyup Celik. 2011. Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. In *3rd International Conference on Cyber Conflict*.

[11] Ryan Edwards. 2010. *A Review of War Costs in Iraq and Afghanistan*. National Bureau of Economic Research, Cambridge, MA. DOI:https://doi.org/10.3386/w16163

[12] Serge Egelman, Cormac Herley, and Paul C. van Oorschot. 2013. Markets for zero-day exploits: ethics and implications. In *Proceedings of the 2013 workshop on New security paradigms workshop - NSPW '13*, ACM Press, Banff, Alberta, Canada. DOI:https://doi.org/10.1145/2535813.2535818

[13] Jennie M. Easterly and Joshua A. Geltzer. More die in bathtubs than in terrorism. It's still worth spending billions to fight it. *CNN*. Retrieved January 11, 2020 from https://www.cnn.com/2017/05/21/opinions/deadly-bathtub-compared-to-terrorism-opinion-geltzer-easterly/index.html

[14] Michael L. Gross, Daphna Canetti, and Dana R. Vashdi. 2016. The psychological effects of cyber terrorism. *The Bulletin of the atomic scientists* 72, 5 (2016). DOI:https://doi.org/10.1080/00963402.2016.1216502

[15] Michael L. Gross, Daphna Canetti, and Dana R. Vashdi. 2017. Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity* 3, 1 (March 2017). DOI:https://doi.org/10.1093/cybsec/tyw018

[16] Ronald L Holle. 2016. The Number of Documented Global Lightning Fatalities. In *24th International Lightning Detection Conference & 6th International Lightning Meteorology Conference*, 4. Retrieved from https://my.vaisala.net/Vaisala%20Documents/Scientific%20papers/2016%20ILDC%20ILMC/Ron%20Holle.%20Number%20of%20Documented%20Global%20Lightning%20Fatalities.pdf

[17] Michael Kenney. 2015. Cyber-Terrorism in a Post-Stuxnet World. *Orbis* 59, 1 (2015). DOI:https://doi.org/10.1016/j.orbis.2014.11.009

[18] Theresa M. Marteau and Hilary Bekker. 1992. The development of a six-item short-form of the state scale of the Spielberger State—Trait Anxiety Inventory (STAI). *British Journal of Clinical Psychology* 31, 3 (September 1992). DOI:https://doi.org/10.1111/j.2044-8260.1992.tb00997.x

[19] Pardis Moslemzadeh Tehrani, Nazura Abdul Manap, and Hossein Taji. 2013. Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. *Computer Law & Security Review* 29, 3 (June 2013). DOI:https://doi.org/10.1016/j.clsr.2013.03.011

[20] John Mueller and Mark G. Stewart. 2018. Terrorism and Bathtubs: Comparing and Assessing the Risks. *Terrorism and Political Violence* (October 2018). DOI:https://doi.org/10.1080/09546553.2018.1530662

[21] Helena Plater-Zyberk. 2000. Cyber Crime... and Punishment. *McConnell International* (December 2000). Retrieved from http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf

[22] Lisa Robinson, James Hammitt, Joseph Aldy, Alan Krupnick, and Jennifer Baxter. 2010. Valuing the Risk of Death from Terrorist Attacks. *Journal of Homeland Security and Emergency Management* 7, (January 2010). DOI:https://doi.org/10.2202/1547-7355.1626

[23] Kamile Nur Sevis and Ensar Seker. 2016. Cyber warfare: terms, issues, laws and controversies. In *2016 International Conference On Cyber Security And Protection Of Digital Services*, London, United Kingdom. DOI:https://doi.org/10.1109/CyberSecPODS.2016.7502348

[24] M Uma and G Padmavathi. 2013. A Survey on Various Cyber Attacks and Their Classification. *International Journal of Network Security* 15, 5 (2013). Retrieved from https://pdfs.semanticscholar.org/ba7b/234738e80b027240e9bfd837bfba61c13e17.pdf

Recommended Reading

[1] Elaine Allen and Christopher Seaman. Statistics Roundtable: Likert Scales and Data Analyses. *Quality Progress*. Retrieved January 16, 2020 from http://rube.asq.org/quality-progress/2007/07/statistics/likert-scales-and-data-analyses.html

[2] Azeez Nureni Ayofe and Osunade Oluwaseyifunmitan. 2009. Towards Ameliorating Cybercrime and Cybersecurity. *International Journal of Computer Science and Information Security* 3, 1 (2009). Retrieved from https://pdfs.semanticscholar.org/cfd8/b70276ea5ac7d534ba2768723a0a9ce02325.pdf

[3] Maria Bada and Jason R.C. Nurse. 2020. The social and psychological impact of cyberattacks. In *Emerging Cyber Threats and Cognitive Vulnerabilities*. Elsevier. DOI:https://doi.org/10.1016/B978-0-12-816203-3.00004-6

[4] Leyla Bilge and Tudor Dumitras. 2012. Before we knew it: an empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12*, ACM Press. DOI:https://doi.org/10.1145/2382196.2382284

[5] Daniel Byman. 2019. Does Al Qaeda Have a Future? *The Washington Quarterly* 42, 3 (July 2019). DOI:https://doi.org/10.1080/0163660X.2019.1663117

[6] Thomas M. Chen. 2010. Stuxnet, the real start of cyber warfare? [Editor's Note]. *IEEE Network* 24, 6 (November 2010). DOI:https://doi.org/10.1109/MNET.2010.5634434

[7] Matthew S. Cohen, Charles D. Freilich, and Gabi Siboni. 2015. Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives* (December 2015). DOI:https://doi.org/10.1093/isp/ekv023

[8] Maura Conway. 2007. Cyberterrorism: Hype and Reality. In *Computer Fraud & Security*. Retrieved from https://pdfs.semanticscholar.org/e30f/ca854868b1ef0066a17ce54af94e86626ce6.pdf

[9] Dorothy E Denning. 2000. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In *Networks and netwars. The future of terror, crime and militancy*. Retrieved from https://pdfs.semanticscholar.org/cf05/5fd12c0fecf64b777a26aff07c5260d553f5.pdf

[10] Murat Dogrul, Adil Aslan, and Eyyup Celik. 2011. Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. In *3rd International Conference on Cyber Conflict*.

[11] Ryan Edwards. 2010. *A Review of War Costs in Iraq and Afghanistan*. National Bureau of Economic Research, Cambridge, MA. DOI:https://doi.org/10.3386/w16163

[12] Serge Egelman, Cormac Herley, and Paul C. van Oorschot. 2013. Markets for zero-day exploits: ethics and implications. In *Proceedings of the 2013 workshop on New security paradigms workshop - NSPW '13*, ACM Press, Banff, Alberta, Canada. DOI:https://doi.org/10.1145/2535813.2535818

[13] Jennie M. Easterly and Joshua A. Geltzer. More die in bathtubs than in terrorism. It's still worth spending billions to fight it. *CNN*. Retrieved January 11, 2020 from https://www.cnn.com/2017/05/21/opinions/deadly-bathtub-compared-to-terrorism-opinion-geltzer-easterly/index.html

[14] Michael L. Gross, Daphna Canetti, and Dana R. Vashdi. 2016. The psychological effects of cyber terrorism. *The Bulletin of the atomic scientists* 72, 5 (2016). DOI:https://doi.org/10.1080/00963402.2016.1216502

[15] Michael L. Gross, Daphna Canetti, and Dana R. Vashdi. 2017. Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity* 3, 1 (March 2017). DOI:https://doi.org/10.1093/cybsec/tyw018

[16] Ronald L Holle. 2016. The Number of Documented Global Lightning Fatalities. In *24th International Lightning Detection Conference & 6th International Lightning Meteorology Conference*, 4. Retrieved from https://my.vaisala.net/Vaisala%20Documents/Scientific%20papers/2016%20ILDC%20ILMC/Ron%20Holle.%20Number%20of%20Documented%20Global%20Lightning%20Fatalities.pdf

[17] Michael Kenney. 2015. Cyber-Terrorism in a Post-Stuxnet World. *Orbis* 59, 1 (2015). DOI:https://doi.org/10.1016/j.orbis.2014.11.009

[18] Theresa M. Marteau and Hilary Bekker. 1992. The development of a six-item short-form of the state scale of the Spielberger State—Trait Anxiety Inventory (STAI). *British Journal of Clinical Psychology* 31, 3 (September 1992). DOI:https://doi.org/10.1111/j.2044-8260.1992.tb00997.x

[19] Pardis Moslemzadeh Tehrani, Nazura Abdul Manap, and Hossein Taji. 2013. Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. *Computer Law & Security Review* 29, 3 (June 2013). DOI:https://doi.org/10.1016/j.clsr.2013.03.011

[20] John Mueller and Mark G. Stewart. 2018. Terrorism and Bathtubs: Comparing and Assessing the Risks. *Terrorism and Political Violence* (October 2018). DOI:https://doi.org/10.1080/09546553.2018.1530662

[21] Helena Plater-Zyberk. 2000. Cyber Crime... and Punishment. *McConnell International* (December 2000). Retrieved from http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf

[22] Lisa Robinson, James Hammitt, Joseph Aldy, Alan Krupnick, and Jennifer Baxter. 2010. Valuing the Risk of Death from Terrorist Attacks. *Journal of Homeland Security and Emergency Management* 7, (January 2010). DOI:https://doi.org/10.2202/1547-7355.1626

[23] Kamile Nur Sevis and Ensar Seker. 2016. Cyber warfare: terms, issues, laws and controversies. In *2016 International Conference On Cyber Security And Protection Of Digital Services*, London, United Kingdom. DOI:https://doi.org/10.1109/CyberSecPODS.2016.7502348

[24] M Uma and G Padmavathi. 2013. A Survey on Various Cyber Attacks and Their Classification. *International Journal of Network Security* 15, 5 (2013). Retrieved from https://pdfs.semanticscholar.org/ba7b/234738e80b027240e9bfd837bfba61c13e17.pdf

Tables

Terrorist event	Number killed	Direct costs		Indirect and social costs	Total cost (approx)	Indirect costs include high estimates for:
		Cost of lives lost	Cost of property damage			
September 11, 2001	2,975	$25,000	$30,000	$55,000 to $200,000	$250,000	Economic disruption, reduced airline traffic, reduced tourism
London, 2005	52	$400	$100	$4,500	$5,000	Lost ticket revenues, reductions in tourism and retail.
Fort Hood, 2009	13	$98	$2	$15	$115	
Boston Marathon, 2013	3	$25	$10	$100 to $500	$500	Policing, city shutdown
Orlando, 2016	49	$370	$5	$50	$425	
Manchester, 2017	23	$175	$25	$2,300	$2,500	Arena closed for 4 months. Assume losses half of London 2005.
Comparison:						
Bathtub drowning	1	$7.5	0	$1	$8.5	Long term pain and suffering especially by parents
431 bathtub drownings (2011)	431	$3,250	0	$431	$3,681	Long term pain and suffering especially by parents

All costs are in millions of 2017 US dollars, and many are rounded up for convenience.

Table 1. Estimated Costs of Terrorist Evens ($ millions)[20]

Figures

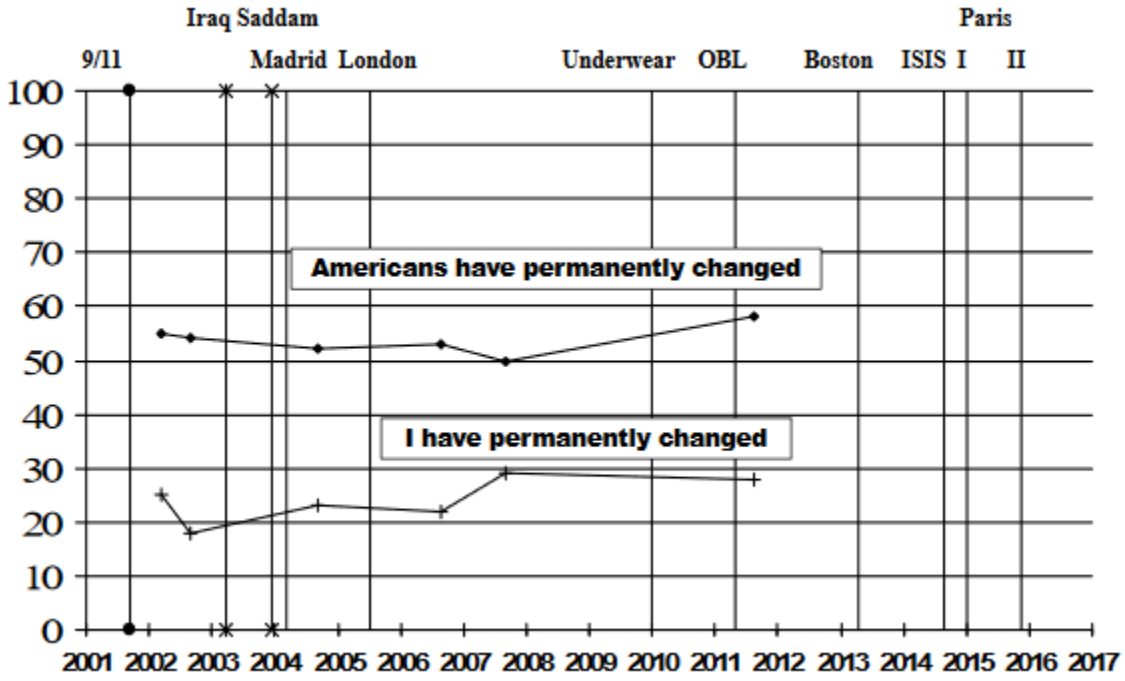

Figure 1. As a result of the September 11th terrorist attacks, do you think Americans have permanently changed the way they live, or not? have you permanently changed the way you live, or not? *Gallup/CNN/USA Today*[20]

	8/2002	8/2005
Life did not change on 9/11	31%	24%
Life changed on 9/11, but now completely back to normal	11	13
Life changed on 9/11, but will completely return to normal	24	19
Life changed on 9/11, and will never completely return to normal	32	42

—Gallup

Figure 2. Outlook on life after 9/11[20]

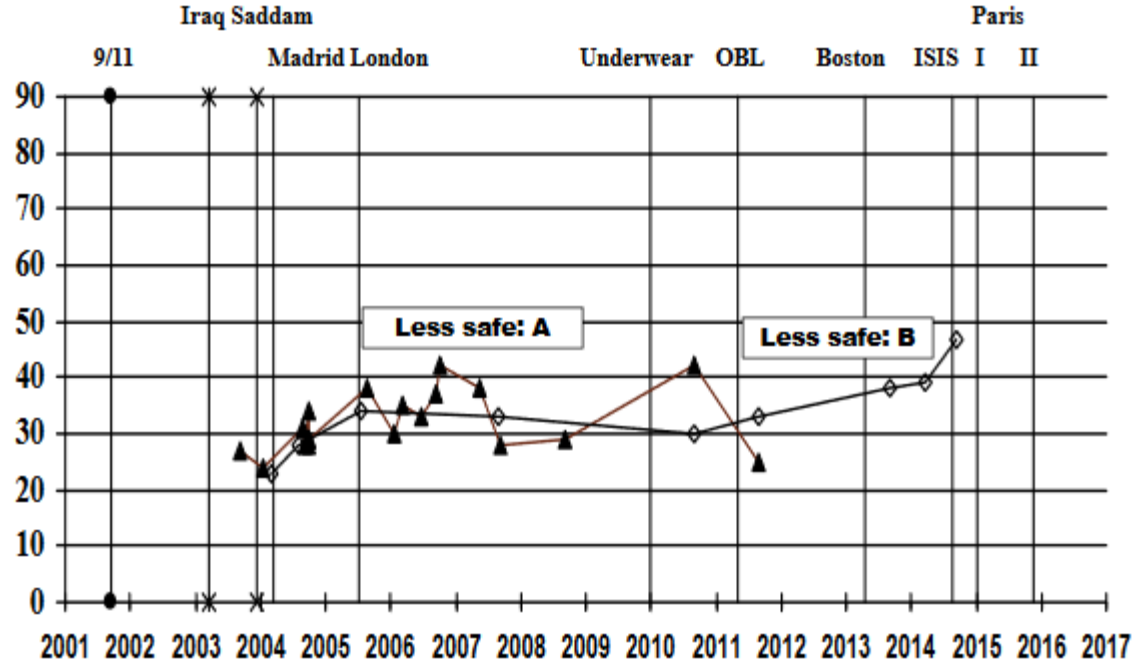

Figure 3. A: Compared to before September 11, 2001, do you think the country today is safer from terrorism or less safe from terrorism? *ABC/Washington Post*
B: Do you think the United States is safer or less safe today than before 9/11? *Fox/Opinion Dynamics* [20]

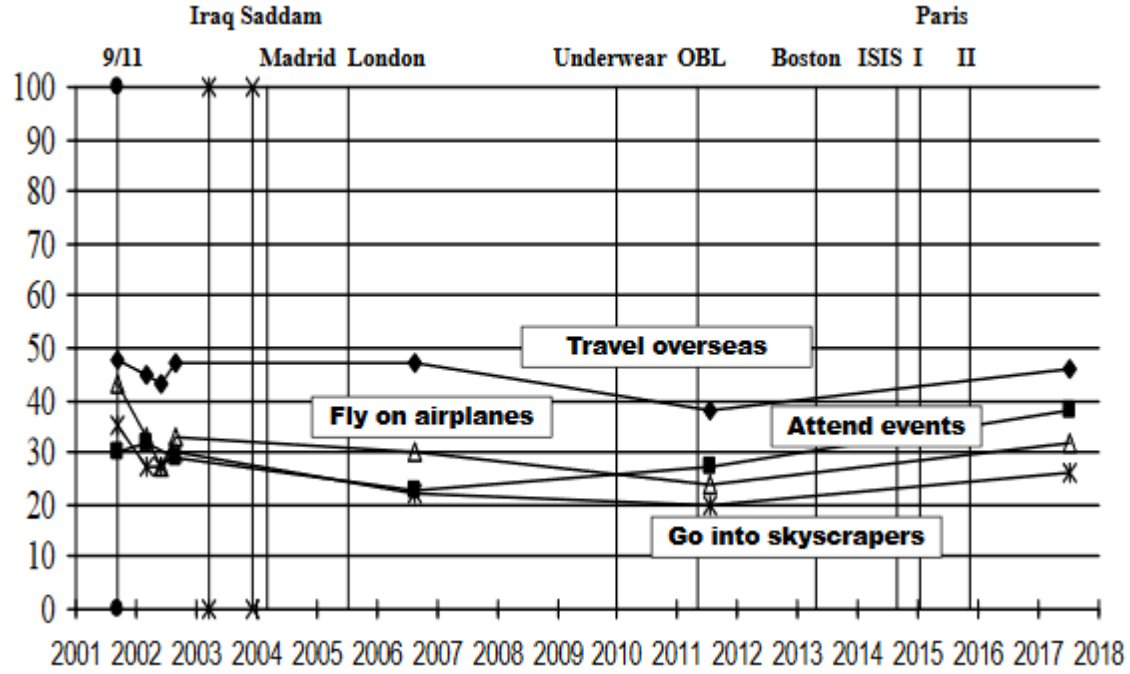

Figure 4. As a result of the events that occurred on September 11th [2017: As a result of the events relating to terrorism inrecent years], would you say that now you are less willing to fly on airplanes, go into skyscrapers, attend eventswhere there are thousands of people, travel overseas--or not? (order randomized) *Gallup*[20]

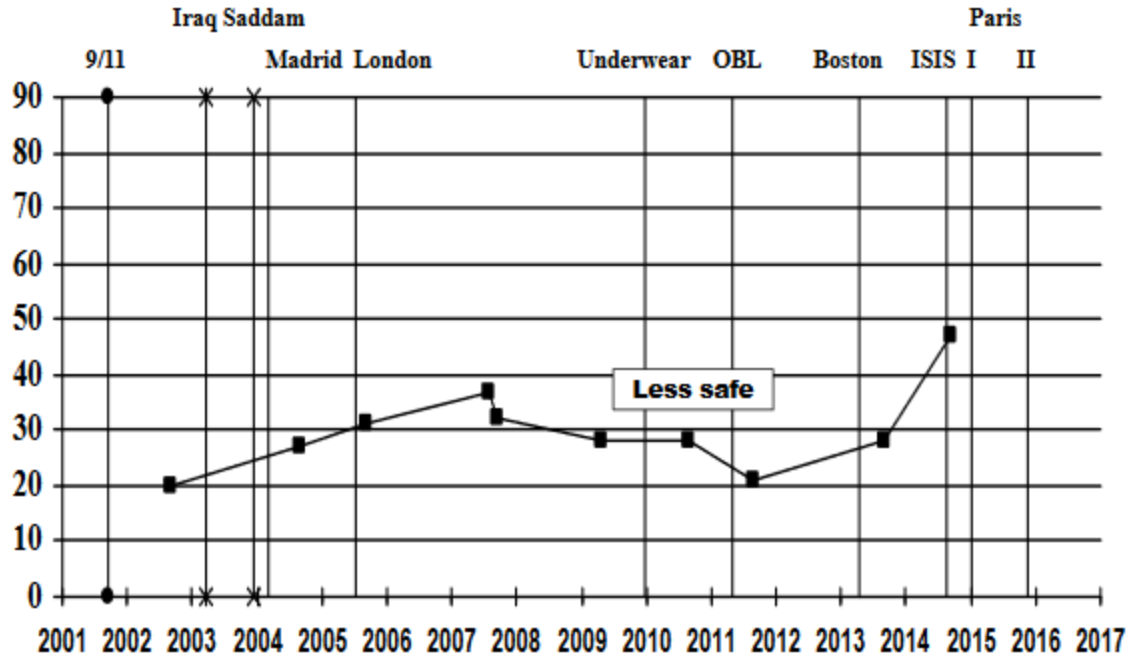

Figure 5. Do you think that as a country, we are more safe, about as safe, or less safe than we were before September 11? *NBC/Wall Street Journal*[20]

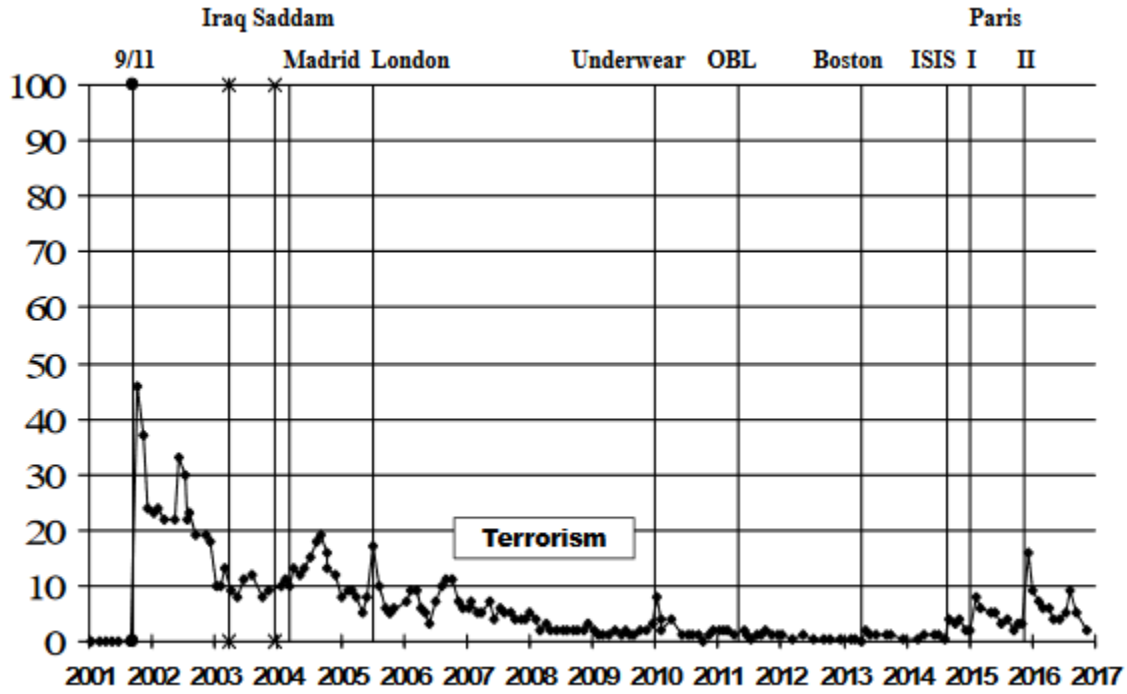

Figure 6. What do you think is the most important problem facing thiscountry today? *Gallup*[20]

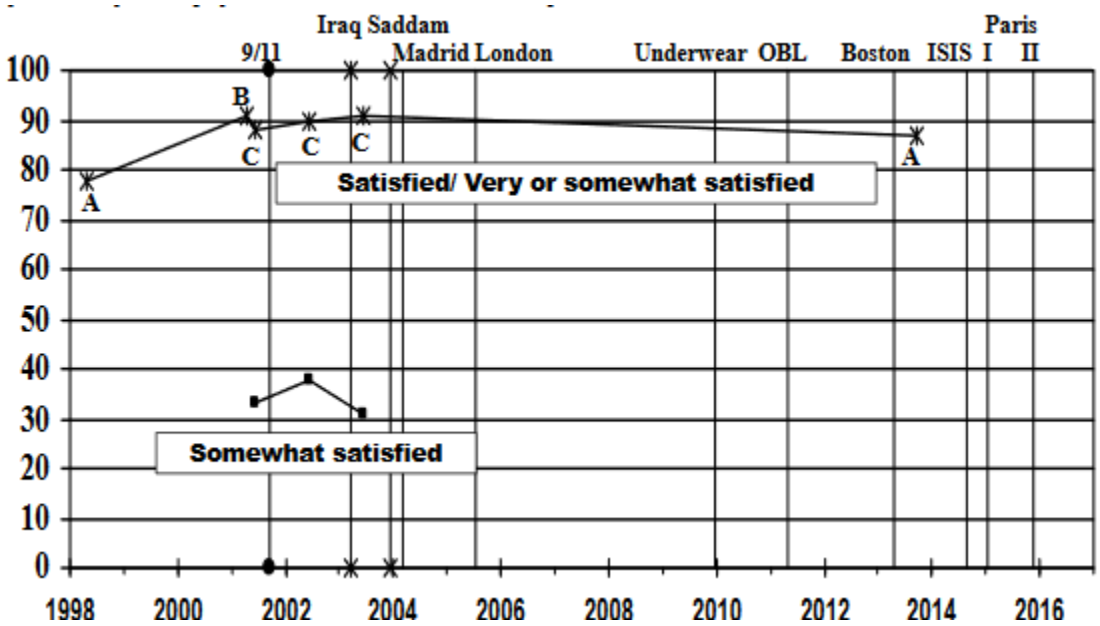

Figure 7. A. Please tell me whether you are generally satisfied or dissatisfied with each of the following. Howabout...your safety from physical harm or violence?B. I'd like to ask you about some aspects of your life. Are you satisfied or dissatisfied with the followingaspects of your life?) How about... your safety from physical harm or violence?C. We'd like to know how satisfied are you with each of the following aspects of your life--verysatisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied? How satisfied are you with...your safety from physical harm or violence? *Gallup*[20]

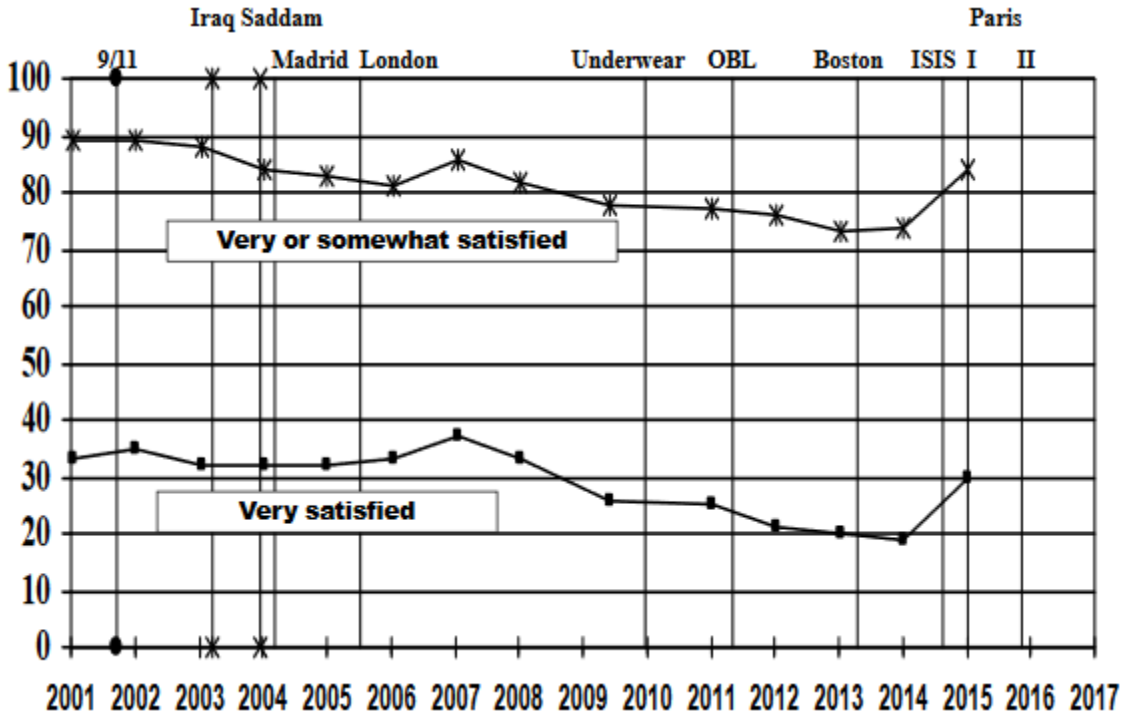

Figure 8. I'm going to read some aspects of life in America today. For each one, please saywhether you are—very satisfied, somewhat satisfied, somewhat dissatisfied, orvery dissatisfied. How about...the overall quality of life? *Gallup*[20]

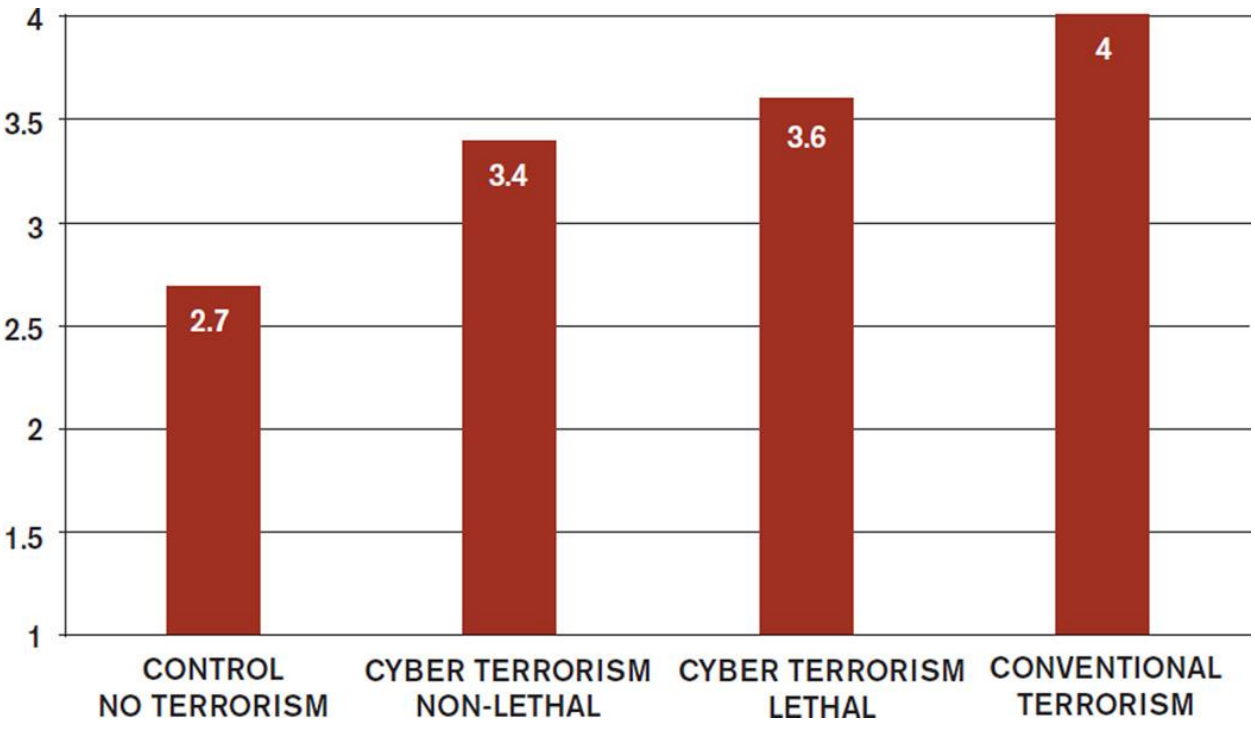

Figure 9.

Anxiety in the Wake of Terrorism [14]
Control: No terrorism
Cyberterrorism, non-lethal: Disclosure of account information (unknown perpetrator), loss of funds (Hamas)
Cyberterrorism, lethal: Deaths and injuries
Conventional terrorism, lethal: Deaths and injuries

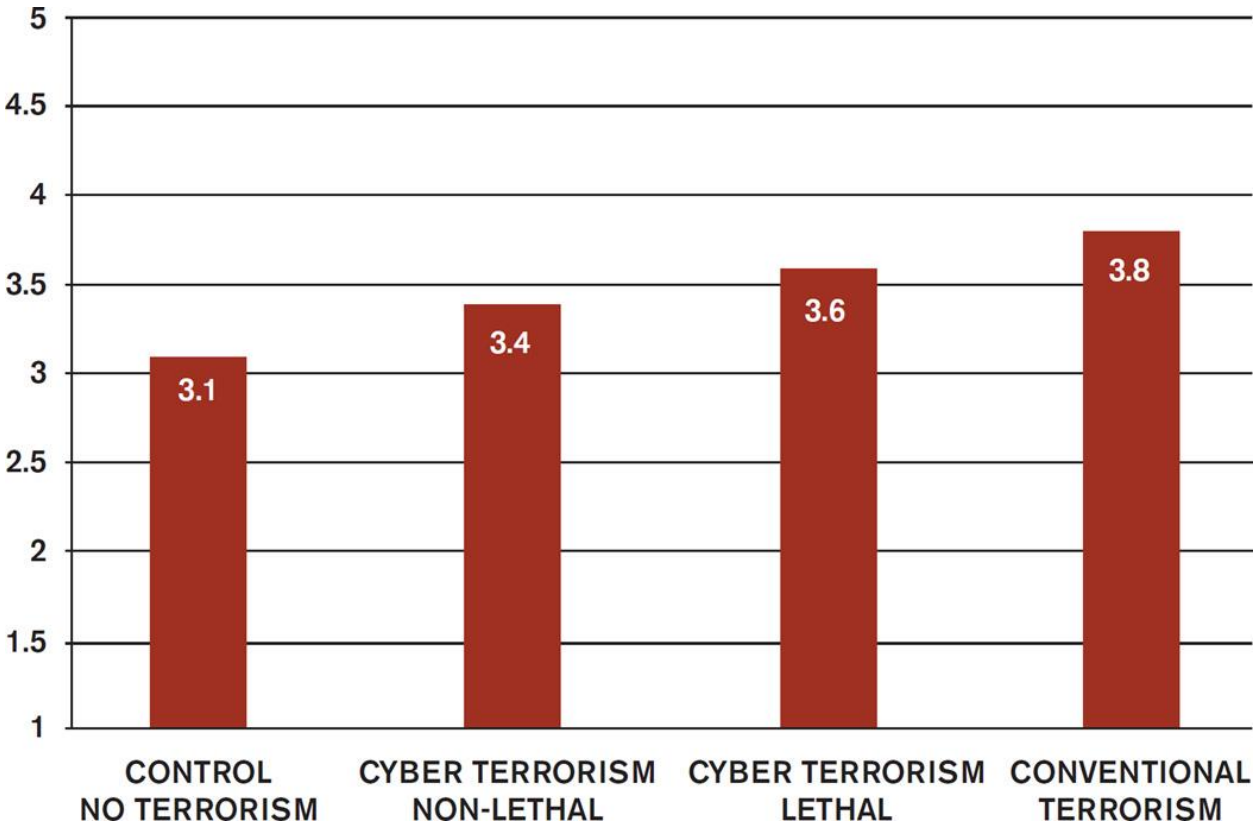

Figure 10.

Threat Perception and Insecurity [14]
Control: No terrorism
Cyberterrorism, non-lethal: Disclosure of account information (unknown perpetrator), loss of funds (Hamas)
Cyberterrorism, lethal: Deaths and injuries
Conventional terrorism, lethal: Deaths and injuries

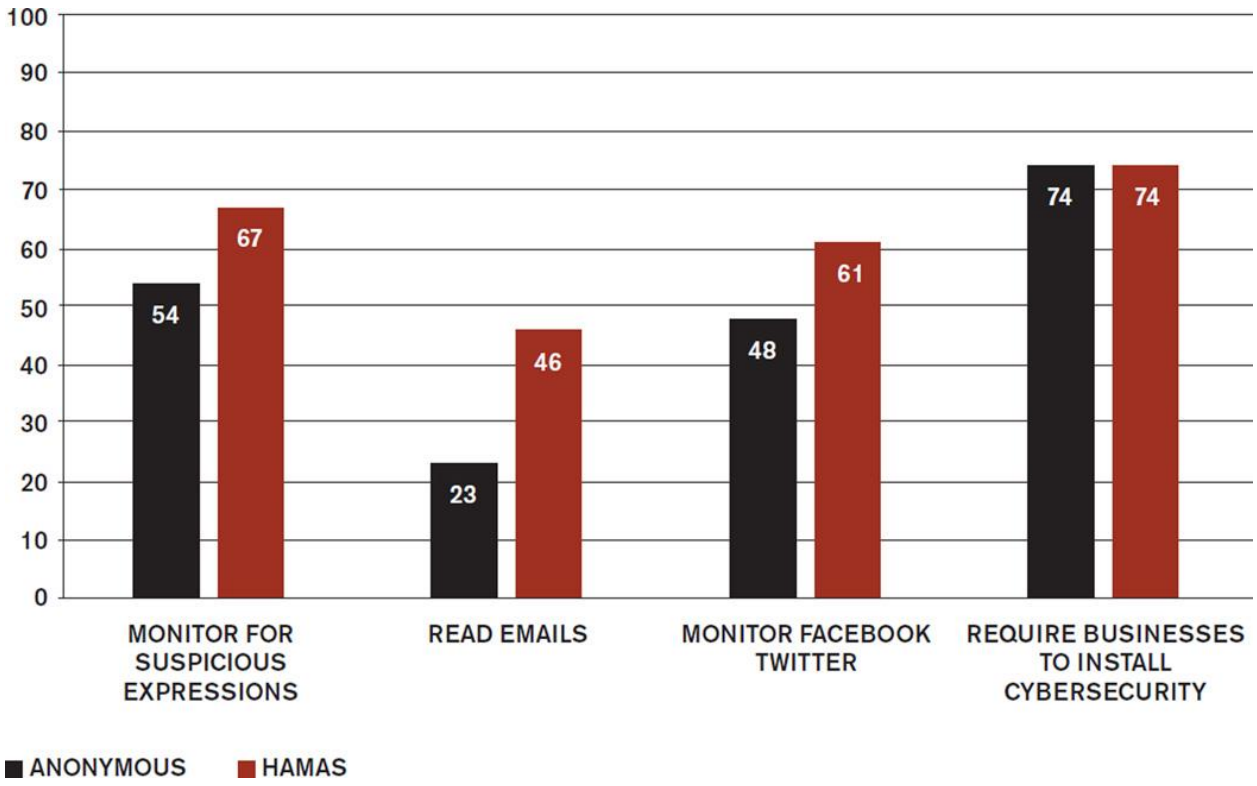

Figure 11.

Percent favoring surveillance and government regulation [14]

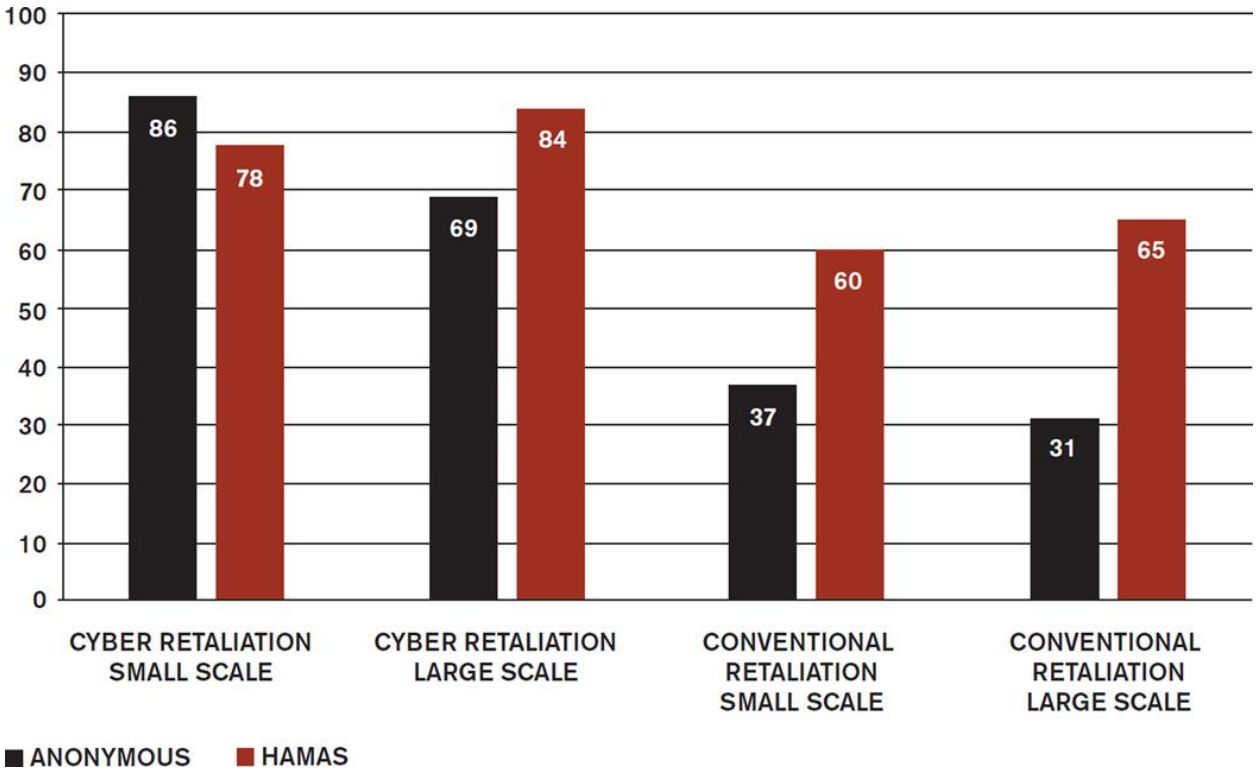

Figure 12.

Percent favoring small-scale and large-scale or conventional retaliation[14]
Cyber retaliation, small scale: Cyber-attacks against military targets
Cyber retaliation, large scale: Cyber-attacks against military and civilian targets
Conventional retaliation, small scale: Kinetic attacks against military targets
Conventional retaliation, large scale: Kinetic attacks against military targets

Attachments

Attachment 1: Anonymized phishing emails between an aware victim (Margo R. Spiegelman) and an attacker impersonating a colleague (Collin Coworker).

Am 01.11.2019 um 12:09 schrieb Collin Coworker:

> Hallo, bist du gerade verfügbar und frei?
> --
> freundliche Grüße,
> Vorsitzende
> Prof. Dr. Dr. rer. Nat. Collin Coworker
> coco.jacobsen-institute.de@my.com

Am 01.11.2019 um 13:22 schrieb Margo R. Spiegelman:

> ja, um was geht es?
>
> --
> Margo R. Spiegelman
> Leitung Department of Cartography
>
> Jacobsen Institute
> Greenrd. 248
> 12776 Agloe, New York
> E-Mail: mrs@jacobsen-institute.de
> Tel: +49 (0)8937 934 - 42
> Web: http://www.jacobsen-institute.de/

Am 01.11.2019 um 13:29 schrieb Collin Coworker:

> Ich bin gerade in einer Besprechung und deshalb kontaktiere ich Sie hier. Ich hätte Sie anrufen sollen, aber das Telefon darf während des Meetings nicht benutzt werden. Ich weiß nicht, wann das Treffen zu Ende geht, und Sie müssen mir sofort bei etwas sehr Wichtigem helfen.
>
> --
> freundliche Grüße,
> Vorsitzende
> Prof. Dr. Dr. rer. Nat. Collin Coworker
> coco.jacobsen-institute.de@my.com

Am 01.11.2019 um 13:38 schrieb Margo R. Spiegelman:

> ich höre...
>
> --
> Margo R. Spiegelman
> Leitung Department of Cartography
>
> Jacobsen Institute
> Greenrd. 248
> 12776 Agloe, New York
> E-Mail: mrs@jacobsen-institute.de
> Tel: +49 (0)8937 934 - 42
> Web: http://www.jacobsen-institute.de/

Am 01.11.2019 um 13:39 schrieb Collin Coworker:

> Sie müssen mir helfen, die Stream Wallet-Geschenkkarte aus dem Geschäft zu holen. Ich erstatte Ihnen die Geldsumme zurück, wenn ich im Büro bin. Ich muss es jemandem schicken und es ist sehr wichtig, weil ich noch in einer Besprechung bin und es so schnell wie möglich verschicken lassen muss. Der Betrag, den ich benötige, beträgt jeweils 100 € in 3 Stück, sodass insgesamt 300 € an Sie zurückerstattet werden. Ich brauche physische Karten, die du aus dem Laden holen wirst. Wenn Sie sie bekommen, kratzen Sie sie einfach und machen Sie ein Foto von ihnen und hängen Sie es an die E-Mail, dann senden Sie es mir hier ok.
>
> --
> freundliche Grüße,
> Vorsitzende
> Prof. Dr. Dr. rer. Nat. Collin Coworker
> coco.jacobsen-institute.de@my.com
