

Internet Contamination as a Global Harm and a Social Problem

**V. Babiy², B. Bigelow³, R.S. Grewal³, R. Janicki², T. Kakiashvili³,
W.W. Koczkodaj^{1,3},
K. Passi³, R. Tadeusiewicz⁴**

² *McMaster University*
Department of Computing and Software
1280 Main St. West
Hamilton, Ontario
Canada L8S 4K1
janicki@cas.mcmaster.ca
babiyv@univmail.cis.mcmaster.ca

³ *Laurentian University,*
Department of Mathematics and Computer Science
Ramsey Lake Road
Sudbury, Ontario
Canada P3E 2C6
bbigelow@laurentian.ca
rsgrewal@cs.laurentian.ca
tx_kakiashvili@laurentian.ca
wkoczkodaj@cs.laurentian.ca
kpassi@cs.laurentian.ca

⁴ *AGH University of Science and Technology*
Department of Automatics
Al. Mickiewicza 30
30-059 Kraków, Poland
rtad@agh.edu.pl

Abstract. *This position paper demonstrates that the global and cumulative cost of dealing with spam is at the level of some natural disasters. Internet email has been a very powerful new technology with enormous social and scientific benefits. However, Internet contamination has currently become a serious social problem. In particular, email spam is a significant irritant and personal stressor which impairs quality of life. Technology solutions, such as filtering tools, are useful but imperfect as they are either too tight or too loose and require their own daily management. Spam volume has impaired daily operations of individual computers and causes servers to crash. It also threatens data integrity as important messages are often filtered along with the unwanted ones. Excessive Internet usage already can threaten mental health and the huge growth of spam only threatens to make the problem intolerable in the very near future. Spam is driven by profit. Social solutions, such as collective action, are needed as spam is a global threat and needs to be prosecuted as a serious threat to security.*

1 - The corresponding author, wkoczkodaj at cs laurentian ca; alphabetical order implies equal contribution of all authors.

Keywords: *Internet, spam, global harm, cumulative harm, collective action, threat*

1. Introduction

A new technology, such as the Internet, has great benefits but often is capable of inflicting great harm. Due to the Internet, the instantaneous sharing of valuable information has helped to thrust science forward at a considerable pace. As well, extended families from the four corners of the globe can communicate instantly over the internet. One of the incalculable benefits of the Internet is usability of life-saving medical data when it is of acceptable quality. However, there are real problems that cannot be denied. The availability of Internet-based information has a social cost. Information quality has a price. Both *spam*-filtering and *malware*-filtering are slowing down computer operation.

Spam has been allowed to spread because it has been seen as a mere irritant at this point. A slow death inflicted by many small wounds, none lethal in itself, but fatal in their cumulative effect was a death once reserved for heinous types of crimes such as treason. Likewise, as a society, we show that Internet torture (i.e., spam) is not a thousand but billions of cuts of our personal slices of time (hence life) inflicted upon Internet users and their families. It deprives innocent people of a good portion of their lives and cumulatively and collectively

surpasses the level of lives lost by *Hurricane Katrina* as it is demonstrated in this position paper.

Quality of life is a constant question in our competitive internet-based world of work and play. Modern families have many competing forces impinging on their daily lives. Social and emotional needs of our tribal daily existence are constantly being eroded in the service of extended work hours, sleep deprivation, and more recently by the Internet. While people can usually cope with occasional short-term hassles such as flat tires, tax returns, illness or minor accidents, it is our position that daily intrusions on our lives on a regular basis take their toll over the long term. In fact, we have the numbers to support our position. Minor daily irritants do in fact matter and *spam* is such an irritant.

2. Collective harm

According to [9], spam (electronic), is defined as unsolicited or undesired bulk email messages. In general, there are many types of electronic *spam*, including:

- email *spam*, unsolicited email,
- mobile phone *spam*, unsolicited text messages,
- forum *spam*, posting advertisements or useless posts on a forum,
- *spamdexing*, manipulating a search engine to create the illusion of popularity for webpages,
- *spam* in blogs, posting random comments or promoting commercial services to blogs, wikis, or guest books,
- newsgroup *spam*, advertisement and forgery on newsgroups,
- messaging *spam* ("*SPIM*"), use of instant messenger services for advertisement or even extortion,
- link *spam*.

Probably the most alarming is email *spam*, also known as "bulk email" or "junk email". It is not only the easiest to use but is fueled by large profit. Email *spam*, currently at the level of 90% of all email messages sent by the Internet, is a major problem. The rate of growth of *spam* damage for the user of the Internet is comparable in scope, from a psychological point of view, to the problem of global warming on the physical environment. It is hardly noticeable on an individual and daily basis, yet destroying Internet users' time and the effective use of the Internet on a global scale.

Hurricane Katrina constitutes a major natural disaster and may serve as an emotional yard stick for measuring other acts of disastrous consequences. So, we propose that *Hurricane Katrina's* confirmed death toll (total of direct) of 1,836 be used in a similar way as the Hiroshima-type A-bomb is used as a bench

mark for expressing the destructive power of other nuclear weapons. According to the statistical data of life expectancy of the [1], for the USA, life expectancy as of 2005 at birth (years) for males is 75.0 and life expectancy at birth (years) females is 80.0. We assume an average of 77.5 in our calculations. Without any additional data, we assume that the average life was cut in half. The expression $1,836 \cdot (75+80)/2$, gives a value of 71,145 of lost life time in years by *Hurricane Katrina*.

One astronomical year is approximated to 365.25 days or 31,557,600 seconds so the computation yields 2,245,165,452,000 seconds of total lost lives. This is a big number and no wonder that *Hurricane Katrina* can be considered a reference point for other heinous acts committed against humanity.

According to www.internetworldstats.com, the number of Internet users was 1,319,872,109 as of December 31, 2007 which is 20.0% of the world's population. So the natural question exists: how much time does an average Internet user waste for the total (i.e., collective) time to be equal to *Hurricane Katrina* total lives lost? It is surprisingly 1,701 seconds which can be rounded to 28 min 21.05 seconds. In other words, if we assume that an Internet user wastes 28 min 21.05 seconds a day, the total collective time wasted by the Internet is equal to *Hurricane Katrina* every day. It is quite realistic to assume that the average time wasted by the Internet is already close to half hour, if not, it is coming soon. Collectively, our lives are wasted every day by *spam* to the value equivalent of shortening lives of all "official" victims of *Hurricane Katrina* and no one even notices only because the death is not sudden but by stealth. Table 1 shows us simple statistical data and some calculations.

3. A ton of feathers and interpretation of the obtained figures

Skeptics may argue that the above figures may be exaggerated and irrelevant. It may be the same as, for example, waiting for coffee in a coffee shop. It is, however, not exactly so. While waiting for coffee in a coffee shop is voluntary, using the Internet is not. Purposeful Internet contamination is a case of a random act of violence. From the user's point of view, it is a case of an innocent bystander caught in the middle of a bank holdup. It is a crime – the innocent bystander could be fatally struck during the bank hold up. Purposeful endangerment constitutes a crime even if the bank robber uses a fake gun.

In a similar way, as a society, we can ignore individual traffic deaths but not major catastrophes, even when the annual death toll of driving exceeds that of Sept. 11th. *Spam* is increasing yearly. How long will it take before *spam* is recognized as a disaster? At the crest of the spam distribution, one of the authors received over 100,000 *spam* messages on his University computer. Because of it,

he was unable to send a message to his students on time. Such a *spam* attack can be fatal if one finds oneself on an island (there are 30,000 on the Georgian Bay) where no cell phone service is provided and many cottages use a satellite dish as the only Internet connection. If a family member suddenly suffered a heart attack or stroke, the only way of calling for an ambulance would be using *VOIP* (*Voice over Internet Protocol*). But the computer may also be close to death while trying to clear the 100,000 *spam* messages. If this example is also not convincing, many Inuit people in the high Arctic routinely rely on e-Health.

Surprisingly, computer contaminants on the Internet have many of the cardinal characteristics of cancer in medicine and as such it was reported in [3] by: “There is very little doubt that we are very fast approaching or even most likely passed a point in time when our personal computers are busier attacking web cancer (malware, malignant software, is related only to software) than conducting useful computations.” Internet contamination is *aggressive* (grows and divide without respect to normal limits), *invasive* (invade and destroy adjacent Internet nodes), and *metastatic* (spread to other locations) which is apparently the main characteristic of medical cancer (appropriately adjusted to the situation).

It is more and more evident that Internet contaminations are here to stay. There is less and less hope that current technology can fix it. *Spam* filters fail drastically being either too tight (causing “false positives”) or too loose. Antivirus software impairs computer operation. According to *The Federal Trade Commission* of 2004, the law has failed to protect us. It is time to realize how that it is serious social problem which we hope to bring to public attention by this position paper. Internet contaminations have many characteristics common with medical problems. In particular, new Internet induced mental illnesses and disorders have begun to surface.

The brain is quite vulnerable to excessive or traumatic stress as the hypothalamic-pituitary-thalamic system becomes overly aroused for too long and becomes exhausted. Hans Selye [5] discovered this fact when overstressed animals became ill and died from exhaustion after repeated exposure to stress. In humans, this sort of reaction is called “battle fatigue”, “shell shock” or *PTSD*, in modern parlance. Sudden events with traumatic consequences on people are induced by the Internet such as the suicide of an Internet game addicted teenager who left behind a letter with the reason for his suicide indicating that joining the heroes of the game he worshipped. A businessman loses a key contract because of a crashed hard drive or a filtered email message. However, in the long run, dealing with daily spam is also a real encroachment on our lives. Cumulative stress often leads to chronic pain, chronic relationship problems, and mental disorders. Amongst many others, depression, anxiety, loss of control, and lowered self-esteem are attributed to chronic stresses. Excessive Internet use has been associated with clinical depression, anxiety and loneliness [10]. Social

withdrawal often accompanies psychosis and, in all likelihood, it is fostered or ameliorated by excessive usage.

The linkage between the mind and the body is very intimate. As Selye's research so aptly found, excessive stress overrides the natural immune response to viruses and bacteria, and inflames arterial walls. Modern patho-physiology identifies cytokines and is responsible for immuno-suppression. Heart disease, obesity, diabetes, rheumatoid arthritis, and memory impairment secondary to depression are either aggravated or directly caused by such excessive stress. Examples abound. Wekerle, Wall, Leung and Trocme [7] have found adverse physiological effects in spouses of abusive partners and in caregivers of disabled family members. Children, especially, bear the burden of chronic urban stresses in their lack of adjustment to elementary school [4]. Another name for cumulative stress is *allostatic load* [11]. Indeed, over a four-year period, peer and academic hassles have been linked by their mothers with internalizing and externalizing syndromes, with adolescent-reported symptoms higher for internalizing syndromes [2].

The impact of cumulative stress on individual functioning is difficult to ascertain as some people are more adaptive than others. However, using the diathesis-stress model of illness vulnerability, approximately 10% of the population is susceptible to serious psychological disorders as a complication of or as a direct result from exposure to such stresses. Indeed, about 10% of the general population has a life-time prevalence of such a disorder. Anxiety and depressive disorders are at epidemic levels in the west. We can estimate that lifetime cumulative effect of Internet-induced stress on the population to be the equivalent of a sudden disaster, such as an earthquake, tsunami, or terrorist attack. Unlike some natural disasters, Internet stress is an attack by stealth. No one even notices that our competitive and hurried lives are being seriously stressed by billions of frights and traumas facilitated by computers in the service of making life more efficient and productive.

4. The Internet Encroachment on our Personal and Social Space

Changes brought about by new communication technologies in general and the Internet in particular greatly influences our lives in unanticipated ways. The advent of the steam engine is but one historical example. The point is each and every one of us has already invented their own way of coping with this situation. For example, the first thing we do on the way to the washroom in the morning is turning computer to boot it up since even booting takes time. On the way back, we press on the "email" button so when we dress, the computer may read and filter *spam*. This is a bit harder to do it at the place of work. We can

only imagine that in a situation like stock exchange, where a fraction of a second may decide a big loss or gain, one may need to come a bit earlier to work, have someone else to turn on the personal computer, use a mainframe solution with a sophisticated firewall, or run the computer the entire night, contributing to global warming. However, this scenario will not continue indefinitely. One day we will run out of options and begin experiencing more and more problems. It is true that in such situations, society usually is able to marshal up resources to find some practical solution.

One of the more significant cases to remember was the outbreak of severe acute respiratory syndrome (*SARS*), a respiratory disease in humans. There has been one near pandemic to date, between November 2002 and July 2003, with 8,096 known infected cases and 774 deaths (a mortality rate of 9.6% which has probably been lowered down by the lack of reliable numbers) worldwide as provided by a concluding report from the [1]. Unfortunately, the same cannot be said about *AIDS* which has not yet been eradicated and still presents a real and substantial threat. One can even risk a statement that because of *AIDS*, our civilization was better prepared for *SARS*. *AIDS* probably spread so fast and became a global issue because of the lack of immediate alertness: it was stealthy. This is why we hope to alert society to the threat of spam.

The Internet has also fueled the growth of websites such as *FaceBook* which signals a social dependency on the Internet for families and friends. This need will only grow. Along with business and entertainment, such growth is now threatening band width. Spam is now a serious additional burden to band width and threatens to stall and interfere with the Internet as a social space.

5. The Doomsday Scenario and Big Business and Social Preventive Measures to Spam

Spam is a profitable business. It is easy to see that email spam would not exist if there was no market for it. It is not hard to imagine if one day ordinary Internet users will begin sending spam email around for profit. Although this is a very unlikely scenario to take place, we only need a small fraction of Internet users to follow the current big fish in helping to spread *spam*. Currently, we do not devote enough attention to spam. In fact, we often glorify it. National TV programs show the biggest Internet perpetrators openly admitting to huge profits. Industry has begun to fight back already. The *Messaging Anti-Abuse Working Group (MAAWG)* is a powerful global organization. In its “*About*” section [<http://www.maawg.org/about/>; information retrieved on 2008 Feb 10], they state:

The purpose of MAAWG is to bring the messaging industry together to work collaboratively and successfully address forms of messaging abuse such as messaging spam, virus attacks, denial-of-service attacks, and other forms of abuse. To accomplish this, MAAWG is developing initiatives in the three areas needed to resolve the messaging abuse problem: Collaboration, Technology, and Public Policy.

The focuses of MAAWG are to:

1. protect electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence,
2. To ensure the deliverability of legitimate messages. MAAWG claims to be the only organization viewing the messaging abuse problem “holistically”.

However, there is no clear position against *spam* although it is implied. MAAWG is more concerned with the messaging abuse but it is important to note that it is done so by focusing on technology, industry collaboration and public policy initiatives.

The Internet is an extremely cheap mass medium. Professional Internet perpetrators have automated their processes to an extent which is not comprehensible for most Internet users. Most email *spam* is dispatched via "zombie networks". They are created by virus- or worm-infected personal computers around the globe. Computer contaminants install a “backdoor” which allows the Internet perpetrator access to the computer. In fact, there is an Internet underground where malware developers, Internet perpetrators learn new tricks and techniques from each other, and very likely form dangerous partnerships. It is only one step ahead from real, not only Internet, terrorism. Internet organizations can obviously be very destructive from a society point of view. Such cases surface from time to time especially related to child pornography.

The high profit, despite of what would otherwise be considered extremely low response rates, of email *spamming* attracts regular criminals. As of now, the high level of Internet expertise is restricting popularity of such criminal activity. However, methods and tools can be and will be soon available on the market. One may hope that in this case, over flooding the market may be a solution to email spam but the availability of the destructive methods and tools creates a real terrorism threat. It seems to be an unstoppable process, hence the *spam* doomsday is coming and as with everything else, the social and legal solution is the only realistic hope.

6. Web Cancer and the Up Hill Battle

The sheer volume of benign *spam* saps significant user time and commercially available filters, while helpful, lack sufficient precision to be used as ‘cures’. The distress of having one’s business or personal life disrupted or spied upon can be quite considerable. However, on a collective level, the scope of the problem is astounding. Considering the millions of businesses and homes that are dependent on the Internet, the collective harm of infectious email messages and *spam* volume is quite substantial. In fact, a case can be made that deliberate dissemination of pernicious computer codes and benign but bothersome *spam* is a form of terrorism. Indeed, *spam* is a form of malware when the intent of the disseminator is harmful. Ordinary *spam* is a form of commercial harassment, much like unwanted and persistent telephone calls. California, West Virginia and several other states have anti-*spam* laws and the U.S. Federal government now has the *CAN-SPAM Act* (2003) (see, [9]), targeting unsolicited commercial email that at the time of the act, accounted for over 50% of email traffic. At the very least, *spam* is a major form of harassment and it is costing people world-wide a lot of time and money. Given the rapid rate of growth (the *CAN-SPAM Act*, 2003) in the electronic environment, email traffic can be anticipated to be overwhelming in just a few more years. In the hands of terrorist groups, it has the potential to be used as a form of financial and social warfare.

Unfortunately, as they are currently written, anti *spam* laws are unenforceable because of the sheer amount of crime involved. Ironically, it would not help much even if we placed a computer trained police person in front of each computer. A single user would be hard-pressed to trace (i.e., ping) even one unwanted *SPAM* email message to the original source. Such messages tend to be batched from re-routed commercial servers where jurisdictions render them untouchable. Most spam comes from distant locations. One of the authors received a message with criminal content from an address which was in another country. The police were contacted in this country but no reply (or even a confirmation) has ever been received. It is hard to blame the police since they cannot reply to millions of complaints. With the possible exception of personal computer abuse within the same jurisdiction, such as attempts to hack into government systems, there is no doubt that it is too late for the police to handle individual end-user complaints. Even setting up an automatic system to analyze such complaints for chasing the most popular *spam* IPs and handing them to a higher level of authority is a missed opportunity. One of the crown examples was a failed attempt to create “A National Do Not Email” registry in the past (upon the US Congress ruling). *The Federal Trade Commission* (2004) concluded that it would fail to reduce the amount of *spam* consumers receive. In

fact, the report stipulated that the creation of such a registry could even backfire and contribute to *spam* generation since nothing could stop Internet perpetrators from using such a list! The full and frankly useless report, 60 pages long, has been posted at <http://www.ftc.gov/reports>. Probably the only useful recommendation was to replace *SMTP* with a protocol that verifies the full email address of the sender at least at the domain name level but this is not easy considering the massive changes needed.

Spam not only wastes our computer time but our own as well. Each of us needs to spend probably close to one hour per day to verifying whether or not our defense programs actually work. We update and scan frequently. Indeed, we should. This time all adds up and our anti-virus and anti-spam software are not fool-proof. Our wasted time is ever increasing since illegal attacks become more and more sophisticated and anti-*spam* and anti-viral software are tested to their limits.

Email *spam* is difficult to fight for many reasons. One of them is that email *spam* is unique in that the receivers pay more for it than the sender does. A notable example is of *AOL* receiving 1.8 million spam messages from *Cyber Promotions* per day until they got a court injunction to stop it. Even if it took only 10 seconds to identify and discard a message for an average user, the accumulated time lost for all users was 5,000 hours per day spent for discarding their *spam*, just on *AOL* alone. By contrast, a T1 line costing about \$100/day is all an Internet perpetrator needs to send such *spam*. There is no other kind of advertising allowing the advertiser to disseminate so much for so little cost. The recipients' accumulated cost was staggering (between approximately \$50,000 for all "minimum wage users" to \$500,000 for all users paid at a professional rate.

It is not easy to convince people of the necessity of giving up, or even decreasing the use of their vehicles or using less technology. In fact, the technology is to be blamed for all of it and doubtfully, the technology can be a solution. It is a social-legal issue. Justice, or more preciously, social justice is one of them. Founded in 1998, *Spamhaus* is based in Geneva, Switzerland and London, UK and is run by a dedicated team of 25 investigators and forensics specialists located in 10 countries. According to *Spamhaus* (<http://www.spamhaus.org/statistics/spammers.lasso>, information retrieved on 2008 Feb 10), up to 80% of *spam* targeted at Internet users in North America and Europe is generated by a hard-core group of around 200 known professional *spam* gangs whose names, aliases and operations are documented in *Spamhaus' Register Of Known Spam Operations (ROKSO)* database. The *Spamhaus Project* is an international non-profit organization whose mission is to track the Internet *spam* gangs, to provide dependable real time anti-*spam* protection for Internet networks, to work with law enforcement agencies to identify and pursue Internet perpetrators worldwide, and to lobby governments for effective anti-*spam* legislation.

It is evident that some kind of collective action must take place to slow down destructiveness of the Internet contamination. Collective action involves examining those factors that cause the setting of standards of social integration, as well as those factors which lead to deviations and created conflicts. An explanation of a collective action in sociology will involve the explanation of those things which are similar or dissimilar to collective actions at different times and in different places. New social organizations need to emerge to cope with new social Internet problems on truly an international level. It may not be easy since we are on the Internet often alone and not in a crowd. Hopefully, the Internet contamination problem, will be brought to *The Economic and Social Council of United Nations (UN)* as a serious social problem since its mandate is to coordinate the economic and social work of the *UN* and the *UN* family of organizations. The Council plays also the main role in fostering international cooperation for development. It is important to note that the Council consults with non-governmental organizations.

7. Conclusions

We need to accept that fighting Internet contamination by technology alone is not possible. Mass collaboration, as a form of collective action needs to take place. New social measures, such as anti-terrorism anti-*spam* laws and social disapproval, must be developed. The involvement of international organizations, such as United Nations may be needed to cope with clearly this international crisis encroaching on all of us soon.

As of now, however, we fear that there is no better conclusion to this note than quoting Sir Winston Churchill, who had never used email, "*This is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.*"

References

- [1] *World Health Organization (WHO) Core Health Indicators*, http://www.who.int/whosis/database/core/core_select_process.cfm, data accessed on Feb. 8, 2008.
- [2] Cater, J. S., Garber, J., Ciesla, J., & Cole, D. A. (2006). Modeling Relations between Hassles and Internalizing and Externalizing Symptoms in Adolescents: A Four-year Prospective Study. *Journal of Abnormal Psychology*, 115(3), 428-442.
- [3] Grewal, R. S., Janicki, R., Kakiashvili, T., Kielan, K., Koczkodaj, W.W., Passi, K., & Tadeusiewicz, T. (2007) Attacking the Web Cancer with the Automatic Understanding Approach, in *Advances in Intelligent Web Mastering*, 43 (136-141), Springer-Verlag; Berlin Heidelberg.

- [4] Morales, J. R., & Chadd, E. (2007). Effects of Multiple Contexts and Cumulative Stress on Urban Children's Adjustment in Elementary School. *Child Development*, 77(4), 907-923.
- [5] Selye, H. (1950). *The Physiology and Pathology of Exposure to Systemic Stress*. Acta, Montreal.
- [6] Tam J., Tang W. S., & Fernando D. J. (2007). The Internet and Suicide: A Double-Edged Tool. *European Journal of Internal Medicine*, 18(6), 453-454.
- [7] Wekerle, C., Wall, A. M., Leung, E., & Trocme, N. (2007). Cumulative Stress and Substantiated Maltreatment: The Importance of Caregiver Vulnerability and Adult Partner Violence. *Child Abuse and Neglect*, 31(4), 427-423.
- [8] [FBI] www.fbi.gov/publications/terror/terror99.pdf
- [9] en.wikipedia.org/wiki/Can_Spam_Act_of_2003
- [10] Caplan, S. E. (2002). Problematic internet use and psychosocial well-being: Development of a theory-based cognitive-behavioral measurement instrument. *Computers in Human Behavior*, 18(5), 553-556.
- [11] John D., & MacArthur, C. T. (1999). Allostatic load and allostasis. Research Network on Socioeconomic Status and Health. Retrieved Oct. 17, 2008 from: <http://www.macses.ucsf.edu/Research/Allostatic/notebook/allosatic.html>.

Table 1. Vital Statistics of Hurricane Katrina and Internet Users

Statistics		
1	Death toll of Hurricane Katrina	1,836
2	USA life expectancy at birth (years) for males in 2005	75
3	USA life expectancy at birth (years) for females in 2005	80
4	USA average life expectancy at birth (years) in 2005	77.5
5	Estimated life time lost in years	71145
6	Astronomical year in seconds	31,557,600
7	Estimated life time lost by Katrina in seconds	2,245,165,452,000
8	Internet users (as of 2007 December 31)	1,319,872,109
Calculations		
9	Value in row 7 divided by value in row 8 (in sec)	1701.047728
10	Above value converted to min and sec	28min 21.05sec