A Torture-Free Cyber Space: A Human Right

Samantha Newbery and Ali Dehghantanha

A Torture-Free Cyber Space: A Human Right

Definitions of torture range from the emotive to the legal. The media sometimes use the term in a loose or informal sense, for example to refer to the pain felt when one's sports team loses a crucial game.[1] This dangerous practice detracts from the severity of torture as defined in law. When international human rights instruments describe the treatment of prisoners as torture, they are referring to severe suffering. News reports also use the term in a non-legal, informal sense to refer to the effects of cyberbullying.[2] In some instances cyberbullying can meet the severity of suffering aspect of the legal definition of torture, as will be explained below.

It can be argued that only when treatment meets a definition of torture contained in international human rights law and associated jurisprudence that we can say it really is torture. However, there have been instances where the law has been manipulated so that practices many people would regard as torture do not meet the narrowed definition. Lawyers working for US President George W. Bush's government achieved this in the months after the terror attacks of 11 September 2001. In his August 2002 memorandum Jay S. Bybee, Assistant Attorney General at the Department of Justice's Office of Legal Counsel, wrote that physical pain is only severe enough to cross the threshold into torture if it is 'equivalent in intensity to the pain

accompanying serious physical injury, such as organ failure, impairment of bodily function, or even death.'[3] The reason for this manipulation was the desire to support an argument that certain controversial interrogation techniques were legal and could therefore be used against terror suspects in an effort to gain intelligence from them. This took place at a time when the US was keen to collect intelligence on Al-Qa'ida as part of the War on Terror.

The 1984 United Nations Convention Against Torture (UNCAT) defines torture at length. The components of this definition can be summarised as: severe physical or mental pain or suffering; that it is inflicted intentionally in order to obtain information, a confession, inflict punishment, to intimidate or to coerce, 'or for any reason based on discrimination of any kind'; and is carried out by, at the instigation of, or with the consent or acquiescence of, someone acting in an official capacity.[4] How to ascertain when these criteria are met, especially given that 'severe' is not defined and that suffering can be difficult for victims to describe, has proven challenging for international human rights courts.

It is particularly relevant to discussions of cyber torture that UNCAT explicitly acknowledges that the suffering caused by torture can be physical or mental. Coverage of the use of torture in the US-led War on Terror since 9/11 has focused on physical actions such as exposing prisoners to extreme heat or extreme cold, physical violence and the prolonged enforcement of uncomfortable or painful positions known as 'stress positions'.[5] Although the mental suffering that these methods can cause is not ignored completely, reasons why these damaging physical methods are often the focus of commentary on the use of torture in the War on Terror might include that their effects are easier to communicate and to measure, and that US policy

documents also focus on these physical actions. Not only do these primarily physical methods have a psychological or mental effect on those who are exposed to them, but other methods of torture are primarily psychological in character. These include threatening the prisoner with execution and with aggressive dogs. Torture therefore can be, and often is, mental as well as physical in its methods and effects.

Media coverage of controversial interrogation techniques used by western states in the War on Terror has equated, and at times confused, interrogation with torture.[6] Being clearer about what practices are being discussed will benefit analysis of the impact and legality of these practices. Seeking information by conducting interrogation does not always involve torture, as routine questioning at police stations in western states usually demonstrates. As the UNCAT definition reminds us, torture is not always motivated by a desire to gain information from the person being subjected to torture: revenge has been exacted on prisoners who a capturing army believed - accurately or otherwise - were responsible for the death of their comrades; and sadism has motivated individual prison guards, for example.[7] For actions to constitute torture as defined by UNCAT, the intentionality behind the action is key. The purpose of torture is to obtain information or a confession, to punish, intimidate or coerce, or it is carried out 'for any reason based on discrimination'.[8]

Human rights law is based on acceptance of the idea that everyone has certain rights by virtue of being human. The European Convention on Human Rights and Fundamental Freedoms (ECHR), for example, states that everyone's right to life shall be protected by law and that no one 'shall be deprived of his life intentionally save in the execution of a sentence of a court following his

conviction of a crime for which this penalty is provided by law.' The ECHR prohibits slavery and forced labour, and protects the rights to liberty, security, respect for private and family life, and freedom of thought, amongst others. Article 3 of the ECHR reads, 'No one shall be subjected to torture or to inhuman or degrading treatment or punishment.'[9]

The landmark case in establishing the interpretation of the term 'torture' in the ECHR was the European Court of Human Rights' 1978 judgment in *Ireland v. The United Kingdom*. Having considered a group of five interrogation techniques used against terror suspects in Northern Ireland in 1971, the Court found that these techniques had caused 'if not actual bodily injury, at least intense physical and mental suffering to the persons subjected thereto and also led to acute psychiatric disturbances during interrogation.'[10] These five interrogation techniques consisted of being hooded with a black pillowcase, exposure to loud, continuous white noise, stress positions, limited food and water, and limited sleep. It is noteworthy that these techniques were found by medical professionals to have induced psychological trauma as well as physical effects, and that the Court, too, acknowledged these effects in their judgment.[11] The Court judged, however, that these techniques 'did not occasion suffering of the particular intensity and cruelty implied by the word torture as so understood.'[12] International human rights lawyer Philippe Sands QC and former UN Special Rapporteur on Torture Manfred Nowak have both noted that human rights standards have changed since 1978 and that if faced with the same evidence in much more recent years the Court would judge that these techniques did amount to torture.[13] Certain of the ECHR's rights can be waived in times of emergency threatening the life of the nation. The prohibition of torture is not one of these rights: the ECHR's prohibition can never be put to one side.

Cyber: Severe Pain and Intentionality

Regardless of whether we take a less formal definition of torture as a subjective judgment about the severity of suffering or a formal definition provided by international human rights law, or even George W. Bush's lawyers' definition, the use of cyber methods provides enough examples to tick almost all the boxes as a means of torture and the potential to meet all the elements of the definition. Cyberbullying already causes more adolescents to have suicidal thoughts than traditional bullying.[14] There exists such a strong relationship between social media and suicide cases[15] that many models have been developed to predict national suicide numbers based on social media data.[16] Hearing of people committing suicide when their private photos are leaked online puts little doubt on how the compromising of privacy can be said to cause severe pain or suffering.[17] Threatening to publish someone's private information online can cause enough pain for the victim to consider a suicide attempt, thereby meeting the severe pain or suffering element of torture via cyber means. Online identity fraud has reportedly had a significant emotional effect on the victims.[18] Many victims state that they would have survived better being robbed at gunpoint than organised online identity theft cases.[19] Suicide attempts of internet scam victims[20] make it clear how online identity hijacking attacks can cause severe pain.[21]

Traditionally threatening people by telling them that they or their families will be killed, or threatening them with losing money or their credit have been used as means of causing pain for the reasons given in the definition of torture. Comparing this with cyber phishers' modi operandi reveals many similarities.[22] The majority of phishing websites and emails threaten their victims

by stating that not following the attackers' instruction would cause huge debt, a big unpaid invoice, or a serious court case, hence many of them can meet the pain and intentionality elements of torture. It is not difficult to see how the intentions behind these phishing campaigns can be to obtain information, to punish, to intimidate or coerce.

All the examples of cyber methods identified above primarily caused mental suffering. In some instances this leads the victim to inflict physical suffering on themselves. Consideration can – and should – also be given to whether cyber methods can directly cause physical suffering. Although there is no reliable evidence of cyber-physical suffering yet, the fast adoption of the Internet of Things and Internet of Nano Things devices which provide nano-sized smart devices that are planted in the human body to monitor and control elements essential to life would bring opportunities to conduct physical cyber torture.[23] Implantable smart medical devices such as Pacemakers and Implantable Cardiac Defibrillators are known to have many security and privacy vulnerabilities that could potentially be abused to cause severe physical pain.[24]

Cyber Torture: How Serious is the Problem?

There is already evidence of a correlation between cyberbullying, cyber phishing campaigns, digital privacy invasion and online identity fraud on the one hand and the pain, suffering and intentionality elements of the UNCAT definition of torture on the other. Understanding the frequency and size of these attacks may help in getting a good view of the importance of the cyber torture issue. 43 per cent of US school students experienced at least one cyberbullying episode during their study time,[25] 19.6 per cent of them regularly experience it every month and

3.6 per cent of students reported being cyberbullied with hurtful information.[26] Over half a billion personal information records were stolen in 2015[27] which can be potentially abused to cause severe issues for individuals. The risk of large companies' employees being targeted by threatening phishing emails reached 1 in 40.5 in 2015[28] while the number of forensic investigation cases that detect hacked Internet of Things devices continue to increase.[29]

The element of the UNCAT definition of torture that it is more difficult to prove is being met by cyber activities is the specification that torture is something done 'by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity'. In other words, this legal definition of torture is only met when it is carried out by someone working for the state in some way. Cyberbullying, for instance, does not always meet this element of the definition of torture. It is perfectly plausible, however, that cyberbullying could be carried out in an official capacity.

In the cyber world, tracks can be hidden easily, making it difficult to establish who is responsible for attacks. What cannot be disputed, however, is that states do have the capacity to conduct the kinds of cyber activities identified as meeting the severity of suffering threshold given in the definition of torture. Further, it is easy to imagine cases where they would also have the motivation for engaging in cyber torture, therefore satisfying all three elements of the definition of torture.

Freedom from Cyber Torture: The Missing Element of Human Rights Discussion

As established by the European Court of Human Rights in 1978 torture is suffering of particular intensity and cruelty. It is clear that cyber activities can satisfy this element of the definition of torture. The other elements of the UNCAT definition of torture can also align with cyber practices in that they can cause severe pain or suffering that is intentionally inflicted for purposes including punishment, intimidation, coercion or 'any reason based on discrimination' and that they can be carried out 'by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity.'[30] Cyber torture is a possibility and is highly likely to happen. The correlation between cyber activities and torture does not contest the definition of torture as established by international human rights law and associated jurisprudence. Instead, it highlights a need to think differently about torture. No longer should we conceptualise torture as something that takes place solely when the torturer and victim are in close physical proximity to one another. The cyber dimension as discussed here highlights that torturer and victim can be physically distant. The victim does not need to be a physical prisoner of a torturer to be exposed to torture. This is not entirely new: phone calls and letters might have been used to conduct torture in the past. Cyber and its quality of being widespread, however, expands the reach of torturers.

States and human rights groups must acknowledge the strong possibility that cyber torture either is happening or will happen. Given that torture is an activity carried out in an official capacity and that it is forbidden by international human rights law states have an obligation to ensure their employees are not engaged in, consenting to or acquiescing to cyber torture. As well as having this forward-looking obligation, they should ensure that disciplinary action is taken against those found to have already engaged in, consented to or acquiesced to cyber torture. Human rights

groups such as Amnesty International, who continue to campaign against torture, have a key role to play in raising states' awareness of what is taking place in their country's name. They have successfully pressured governments to institute safeguards against torture in the past. This is illustrated by Amnesty International's success in pushing for an official inquiry into the treatment of prisoners in the-then British colony of Aden in the mid-1960s during a nationalist insurgency that won independence for Aden in 1967. This inquiry in turn resulted in changes to the guidelines governing the handling of prisoners held in British custody for interrogation in the form of additional safeguards including that medical treatment should be readily available.[31]

Cyber torture also has implications for the medical practitioners who treat victims of torture. Their valuable work acknowledges the mental suffering caused by torture. It is important that victims of all forms of torture who want to receive treatment for what they have experienced can access appropriate, timely treatment and expertise. It is possible that greater awareness amongst the medical profession and amongst those who are in a position to refer victims for restorative treatment will increase the frequency with which victims of cyber torture are offered appropriate medical support.

Understanding of the means by which torture can be conducted must keep pace with cyber developments in order that successful efforts can be made to keep cyber space free from torture.

[1] For example, Jim Duffy, 'Pain Management: Motherwell Boss Mark McGhee's Ibrox Scottish Cup Torture a Boost For Fans Says Jim Duffy', *The Scottish Sun*, 24 January 2017, <https://www.thescottishsun.co.uk>, accessed 16 February 2017.

[2] Catherine Dunne, 'Cyberbullying: We Need To Stop This Internet Torture', *The Telegraph*, 27 September 2013.

[3] Office of the Assistant Attorney-General, 'Memorandum for Alberto R. Gonzales Counsel to the President', 1 August 2002, in Karen J. Greenberg and Joshua L. Dratel (eds), *The Torture Papers: The Road to Abu Ghraib* (USA: Cambridge University Press, 2005), p. 172. See also Jeremy Waldron, 'Torture and Positive Law: Jurisprudence for the White House', *Columbia Law Review* (Vol.105, No.6, October 2005), pp. 1703-09.

[4] United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 26 June 1987.

[5] For example, see Robert Fisk, 'America's Shame, Two Years on From "Mission Accomplished"', *Independent on Sunday*, 8 May 2005 and Manfred Nowak, 'What Practices Constitute Torture?: US and UN Standards', *Human Rights Quarterly* (Vol.28, No.4, November 2006), pp. 809-41.

[6] For example, see *Guardian.com*, 'MPs Demand Answers Over "Torture Intelligence"', 5 April 2005.

[7] Samantha Newbery, *Interrogation, Intelligence and Security: Controversial British Techniques* (Manchester: Manchester University Press, 2015), p. 144; *The Times*, 'At Abu Ghraib', 26 August 2004.

[8] United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 26 June 1987.

[9] European Convention on Human Rights and Fundamental Freedoms, 4 November 1950.

[10] European Court of Human Rights, 'Ireland v. United Kingdom', Series A, No. 25, 1978, paragraph 167.

[11] Newbery, *Interrogation, Intelligence and Security*, p. 120.

[12] European Court of Human Rights, 'Ireland v. United Kingdom', Series A, No. 25, 1978, paragraph 167.

[13] Philippe Sands, *Torture Team: Deception, Cruelty and the Compromise of Law* (London: Allen Lane, 2008), p. 215; Nowak, 'What Practices Constitute Torture?', p. 837.

[14] David McNamee, 'Cyberbullying "Causes Suicidal Thoughts in Kids More Than Traditional Bullying"', *Medical News Today*,11 March 2014, <http://www.medicalnewstoday.com>, accessed 16 February 2017.

[15] Jo Robinson, Maria Rodrigues, Steve Fisher and Helen Herrman, Suicide and Social Media: Findings from the Literature Review, July 2014, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.673.5500&rep=rep1&type=pdf>, accessed 16 February 2017.

[16] Hong-Hee Won, Woojae Myung, Gil-Young Song, Won-Hee Lee, Jong-Won Kim, Bernard J. Carroll and Doh Kwan Kim, 'Predicting National Suicide Numbers with Social Media Data', *PLOS ONE* (Vol.8, No.4, 22 April 2013), <http://journals.plos.org/plosone>, accessed 16 February 2017.

[17] Kate Briquelet and Katie Zavadski, 'Nude Snapchat Leak Drove Teen Girl to Suicide', *The Daily Beast*, 6 October 2016, <http://www.thedailybeast.com>, accessed 16 February 2017.

[18] Identity Theft Resource Center, 'Identity Theft: The Aftermath', 2013, <http://www.idtheftcenter.org/images/surveys_studies/Aftermath2013.pdf>, accessed 16 February 2017.

[19] Herb Weisbaum, 'ID Theft Can Take Heavy Emotional Toll on Victims', *Today*, 20 November 2014, <http://www.today.com>, accessed 16 February 2017.

[20] *BBC News*, 'Suicide of Internet Scam Victim', 30 January 2004.

[21] Mark Button, Chris Lewis and Jacki Tapley, 'Not a Victimless Crime: The Impact of Fraud on Individual Victims and Their Families', *Security Journal* (Vol.27, No.36, 23 April 2012), <https://link.springer.com/journal/41284>, accessed 16 February 2017.

[22] D. Kevin McGrath and Minaxi Gupta, 'Behind Phishing: An Examination of Phisher Modi Operandi', paper presented to First USENIX Workshop on Large-Scale Exploits and Emergent Threats, San Francisco, 15 April 2008, <https://www.usenix.org/legacy/event/leet08/tech/full_papers/mcgrath/mcgrath_html/>, accessed 16 Feb. 2017.

[23] Steve Watson and Ali Dehghantanha, 'Digital Forensics: The Missing Piece of the Internet of Things Promise', *Computer Fraud & Security* (Vol. 2016, No. 6, June 2016), pp.5-8, <http://www.sciencedirect.com/science/journal/13613723>, accessed 16 February 2017.

[24] Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno and William H. Maisel, 'Security and Privacy for Implantable Medical Devices', *IEEE Pervasive Computing* (Vol. 7, No. 1, January-March 2008), <http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=7756>, accessed 16 February 2017.

[25] Cyberbullying Research Center, '2015 Cyberbullying Data', 1 May 2015, <http://cyberbullying.org/2015-data>, accessed 16 February 2017.

[26] US Department of Education, 'Student Reports of Bullying and Cyber-Bullying: Results From the 2011 School Crime Supplement to the National Crime Victimization Survey', August 2013, <http://nces.ed.gov/pubs2013/2013329.pdf>, accessed 16 February 2017.

[27] Symantec, 'Over Half a Billion Personal Information Records Stolen or Lost in 2015', no date, <https://www.symantec.com/content/dam/symantec/docs/infographics/istr-reporting-breaches-or-not-en.pdf>, accessed 16 February 2017.

[28] Symantec, 'Attackers Target Both Large and Small Businesses', no date, <https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf>, accessed 16 February 2017.

[29] Watson and Dehghantanha, 'Digital Forensics', pp. 5-8.

[30] United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 26 June 1987.

[31] Newbery, *Interrogation, Intelligence and Security*, pp. 34-61.