目录

1. 绪论
   1. 广义网络暴力与狭义网络暴力
   2. 阐述流程
2. 互联网的特性
3. 互联网事件生命周期
4. 网络暴力盘点与分析
5. 方案与对策
6. 总结

绪论

首先，我要在这里阐述一下狭义网络暴力与广义网络暴力的区别。

狭义网络暴力：是网民在网络上的暴力行为，社会暴力在网络上的延伸。严重损害事件当事人的利益（生活秩序，精神状态，名誉等）。这可能是大部分人潜意识中对于网络暴力的定义，我在互联网上找相关资料的时候，找到的大多也属于这类。

广义网络暴力：狭义网络暴力中的暴力行为不仅可以被网民使用，还可以被其他个体或组织使用，其目的亦可好可坏。暴力在这里是一个中性词。

我在这里讨论的，既有狭义的网络暴力，也有广义的网络暴力。到了广义网络暴力层次，就不能简单地对某种网络暴力的对错下结论了。

1. 我会首先分析互联网所具有的特性，以及互联网事件生命周期的规律。分析完之后盘点一下主要的几种网络暴力类型。最后说一下相关的方案与对策。

互联网的特性

想要了解网络暴力，必须先深入了解互联网究竟是一个什么东西。互联网的特性是一切的基础。

各种类型的网络暴力的产生或多或少地利用了互联网的某种特性；对网络暴力的解决方案，背后的原理也是基于这些互联网特性的，正所谓“解铃还须系铃人”。

信息永久保存

网络爬虫之类的工具会不停地收集网民上传至互联网的信息，并在整个互联网之中传递，甚至下载到离线存储器之中。可以说一旦网民的信息被上传，想要删除这些信息已经是难上加难的了。

要是再考虑到这一点：你身边的一切设备都在无声地上传着你的信息，那就更可怕了。现在的设备应用都要求用户输送数据到服务器，用户借以换取设备应用所带来的便利，这真是一个残忍的交易。

可以说，现在几乎所有的人，都不再有隐私可言。

上资料：

* 作者：让生命活出精彩
* 链接：https://www.zhihu.com/question/49502870/answer/159741155
* 来源：知乎
* 著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。
* 对于绝大多数的人来说，我可以轻易的获取的信息包括:
* 1、你的户籍信息，家庭成员信息，所受教育记录，名下资产信息，车辆信息，四行余额。
* 2、你所用过的手机号，你所用过的各种主流账号（支付宝，QQ，微信，淘宝）（如果你密码有所雷同，还可以登录你的账户，如果不怕承担法律风险甚至可以取走你的钱）
* 3、你的淘宝送货地址，美团外卖地址，美团外卖记录，滴滴打车记录，火车飞机记录，全国宾馆记录。
* 4、你现在所在的位置（实时定位），你这一天行动的轨迹，等等。
* 这是在我们私人侦探圈，或者是个人信息售卖圈习以为常的，也是圈子之外的人不可置信的。
* 如果没有在这个圈子里面，你会觉得自己每次输入的信息都会得到妥善的保护，你会相信自己只在学校记录的学籍信息，自己仅仅在淘宝，京东等输入过得信息，必然会得到妥善的保护。
* 然而，当你第一次接触到这个行业，试图去验证你信息有多安全的时候，你才会发现，自己竟然如同赤身脱体于互联网之下，你的所有的信息，竟然全部都能够被获取，让人胆战心惊。

信息永久保存，是人肉搜索的基础：自己在互联网上的蛛丝马迹，除了方便自身的设备应用之外，其他人也能利用。利用一些社工手段，我可以轻易地取得在座各位的人身信息。

可惜的是，人们并没有限制信息只在特定区域使用的权利。这根本做不到。

网民群体的特征

网民对于网络的使用能力差别很大，存在着一个能力的阶梯。

信息检索也不是人人都会的，要是人人都很牛逼，那还得了？互联网其实千疮百孔，漏洞百出。所幸互联网上绝大多数人都是头脑简单，对网络什么都不懂的小白，不然互联网早就被毁灭了。

信息过剩

前面说过了，互联网上绝大多数人都是小白。虽然人们有选择信息的权利，但是现在互联网上信息这么多，在海量信息面前这就成了伪自由选择。强人尚且可以精准找到自己要的信息，但是大多数人都是随波逐流，被动接受互联网上各种媒体灌输给他们的信息，这叫做网民的被迫接收状态。

开放

任何人都能上网。现在互联网已经非常普及了。截至2016年6月，中国网民规模达到7.10亿（上折线图）。这么多人，只要连上网就能上网，完全没有什么“审查机制”在阻挡。

并且，任何人在能力充足的情况下，能够做任何能够做的事情，能够进入互联网下几乎任何领域。只要技术允许，就能做。结果便是：互联网上存在大量不同阶层的人物，鱼龙混杂。

匿名

虽然有信息泄露的威胁，但是考虑到网民群体中能力差距的存在，我们可以认为互联网是相对匿名的。大部分人都有侥幸心理，信息泄露就泄露吧，泄露的人那么多，搞破坏的人那么少，不会轮到我头上。

用经济学的话来说，因为匿名，所以暴力的成本是很低的。

大多数的网络暴力都基于网络的匿名性。

实际上，因为线上线下的这种相对独立，所以就有了“虚拟空间”的说法。不过这种说法现在也过气了，侧面说明线上线下独立性实际上越来越低。

互联

互联网之所以重要，是因为它让我们更加紧密的联系在一起。自古以来人与人之间联系的强化总会带来人类力量的提升。在这里，网络媒体的能力超越传统媒体，使得网民的互联实际上产生了强大的力量。

互联网事件生命周期

这个东西的灵感来自于产品生命周期PLC。（上PLC图）。产品有寻入，成长，成熟，衰退，那互联网事件为什么不可以呢？

开始：反映某一事件的信息开始出现。

传播：各种事件之间有关注量的竞争，关注者多的胜出。在这过程中从众现象越来越明显。

顶峰：达到一定规模，出现其他势力的介入，存在对原事件的二次创作（模因）。从众现象达到极致。到了这个阶段一般是没法阻止的。

消亡：事件的目标达到时，或关注价值消失时，自行消亡。

网络暴力种类

言语攻击

言语攻击，就是骂人、嘲讽、鄙视之类的，又叫做“喷人”。经常用言语攻击别人的，就被称为“喷子”。

这是最常见，最主要的网络暴力。下至网民互撕，上至商业战争，美国总统也爱开喷。

言语攻击的动机。网民在互联网上喷人的动机有很多，无不外乎两种：维护利益和娱乐。

对骂：个人利益间的冲突。一部分原因是出于对于某种问题的谈判失败，导致撕破脸皮开喷，这是在维护自身利益。除此之外，根据网民群体的能力分布来看，以喷人为乐的网民也是大量存在的。这种网民用弗洛伊德理论来说，就是在宣泄力比多（性能量）。

群骂：群体利益间的冲突。互联网强大的互联特性，使得网上超大规模社群的存在成为了可能。甜豆腐脑派和咸豆腐脑派，都是囊括至少数百万人的大圈子。这些社群之间的互动就是网络舆论的主要内容。

讨伐：大量网民骂少数几个人。比如说“铜须门事件”，是一场道德暴力事件，铜须就受到了万人唾骂。互联网的开放性使其本身成为道德讨伐的利器，每一个参与者都急迫地维护道德正义，但是他们这时往往受群体无意识的支配，形成红卫兵思维：只要动机正确，即使忽视手段的不当性也没什么问题。网民自发的多数言语攻击活动都是不计后果的，这点要加以注意。

讨伐也是实行网民舆论监督的手段。比如说“王勇平事件”，就是那个温州火车相撞说“我反正信了”的铁道部发言人。

辱骂微软小冰：这个比较有意思。对方是AI，和AI对骂，不是傻吗？显然这里不存在维护利益的动机。喷子辱骂小冰不是因为机器人抢走了他们的饭碗，而是为了娱乐。大部分人上网，都是来找乐子，或者是发泄的。只要臭骂一通能带来快感，宣泄愤怒，至于对方是谁，又有什么关系呢？

煽动

与言语攻击相反，煽动仇恨，或者说是“引战”，都是经过精心策划的。

个人、组织、企业、国家机构都能够执行煽动。这就到了广义网络暴力的层面了，什么“伊朗网军”“俄罗斯网军”，都是国家层次的网络暴力机关。

泄露他人信息、人肉搜索和线下报复

据称草根网民的人肉搜索，是猫扑首创的。

人肉搜索一般有三个等级：泄露他人信息、人肉搜索和线下报复。泄露信息最多，并且无时不刻在发生；人肉搜索少了；线下报复最少。像是前面提到的“铜须门事件”以及砸日系车事件，就是三样都有的，这类事情一般容易搞个大新闻。

对于人肉搜索的危害，社会谈论的也够多的了，但能说这一套不好吗？不能轻易下论断。如果没有这些，警察怎么跨省抓犯人呢？

营销活动

这应该是最容易被忽视的网络暴力种类了。一些机构或个人为了利益做的一些有预谋的活动，其中的代表就是炒作。好的营销，比如说公益广告什么的，我不否认。但是营销活动特殊就特殊在于，它造成的是无形的伤害。举个例子：

小学性教育课本事件：一些微博大V通过断章取义，截取一部分图片的方式攻击性教育课本，称其内容淫秽，成功引起家长反感，并最终令其被取缔。这些微博大V的动机是娱乐大众，却不想成为了良心课本被取缔的导火索。你们知道出这么一本课本有多不容易吗？这对教育界造成的损失，或比前面任何一种暴力更大。

其他一些网络暴力：

造谣传谣

黑客活动

~~暴力膜蛤~~

不多说了。

方案与对策

最后我们来谈一谈对于这些问题的方案与对策。没有完美的策略，必然会有所取舍。

法律

基本手段

对于法律来说，越暴力的事情越容易抓。法律的本质上就是一种自上而下的手段，它管不了小事。法律不是万能药，那种一遇到问题就呼吁加强监管、完善体制或是法律的行为是不负责任的。

失败的例子：网络实名制

依据：开放性

例子：防沉迷系统。技术上难以实现，管控对象太多，容易被绕过，只能实现局部实名。并且它一刀切，违背了网络的开放性和匿名性。

成功的例子：500次转发谣言判刑法律

依据：互联网事件生命周期

利用互联网事件生命周期来分析的话，我们会发现在源头阻断谣言的发生是很困难的，实际上依然还是有很多谣言转发超过500次却未被处理。这个法律最重要的作用就是可以压缩谣言影响的进一步扩大，以及在谣言的顶峰时期对其进行狙击。在这一点上，这个法律是成功的。

媒体

主要手段

意见领袖

比海量的网民更容易塑造、控制。

舆论控制主要指的是这个。

依据：信息过剩

伪自由选择，网民实际上并不知道自己想要什么（by乔布斯），多处于这种无意识的被动接收状态。

舆论控制有风险。

干预网络议题生命周期

开始：敏感词，验证码

这也算，想象一下没有这些东西会怎样，大量垃圾信息将会充斥网络

例子：爆吧事件

开始/传播：删帖等

简单粗暴

可能被利益集团利用，以打压报道，湮灭真实

传播/顶峰：网络水军，禁评 ~~近平~~

引导舆论

一把刀，借刀杀人，谁都能用

顶峰：强硬手段

顶峰：快速冷却事件

危机公关，涉事企业/官员认错态度良好等

技术

GFW：不必多说

敏感词，验证码，智能删帖等

教化

辅助手段

注重改变网民的想法

公民维权

信息保护意识：虽然你我的信息已经大量地泄露了，但至少得要注重自己的隐私权啊。

公民规则

一般适用于一些互联网社群的内部，难以应用至全网。改变不了整个互联网，就改变局部。并不是所有人都有理性基础的。

垂直社区建设

例子：美国两党电视台，军事网站，虐猫秘密网站

原理：开放，互联，网民群体特征

这绝对是个好主意。既然不能阻止网民上网，那就把他们限制在一个个相对封闭的社区，让喷子不出来“害人”，起到一个筛选的作用。比如说某些网站的评论区，简直就是喷子疯人院。因为网络的互联性质，这种事情几乎是在互联网内部自发形成的，不过监管者也可以加速这一进程，比如说建个强国论坛什么的233。

教化可以在素质比较高的社区里进行。比如说普及文明议事，组织圈子全体学习罗伯特议事规则什么的，怎么高级怎么来。每个贴吧基本上都有吧规，一般都能起到管理本社区的任务。