Opsec：翻墙匿名反党圣经 不被中共匪警喝茶的6+1个要素 根据超过100位被传唤“喝茶”网友的2年跟踪调查的经验总结（内含测试题）

Opsec：翻墙匿名反党圣经 不被中共匪警喝茶的6+1个要素 根据超过100位被传唤“喝茶”网友的2年跟踪调查的经验总结（内含测试题）

这篇文章写了很久一直没有发表，发表这篇文章仅为致敬我的前辈编程随想，祝愿他平安，早日得自由。也感谢帮助我完成调查的勇敢的网友们。
本文发布至公共领域，不保留版权，转载无需授权和署名

*Opsec即 Operational Security 信息安全或者操作安全的意思
这篇文章目标受众是新翻墙的网友，适用于一般的键政活动。此文的诸多操作仅从“优先保持匿名”理论讲解的角度出发。本文提到的公安技术侦查运作原理是根据超过100例传唤、判刑案例所推断，仍需要内部一手消息源补充和交叉验证。但就两年的Opsec培训的效果而言，200多位受该方案训练者当中无人被传唤过（1人没遵守建议除外）。因为本人没有调查记者的专业背景，也没有法证相关的工作经验，对调查的设计并不理想，在调查的过程中为保护爆料人的安全阻止对方提供过于具体的信息，因而数据的质量有限，希望有兴趣者能够进一步调查完善这一研究。
如果您想在固定的身份下原创大量革命内容、运营革命组织、发起革命运动等等，这篇教程所提供的Opsec是不够用的，至少应该花几周的时间学习教程和案例、配置路由器和电脑、
准备门罗币、熟练使用各种工具，并测试完备。建议参考和翻译以下内容：
编程随想 https://program-think.blogspot.com/
Darknet Bible 暗网圣经 http://biblemeowimkh3utujmhm6oh2oeb3ubjw2lpgeq3lahrfr2l6ev6zgyd.onion/
Hitchhiker's Guide to Anonymity 背包客匿名指南 https://anonymousplanet-ng.org/
Dread论坛 Opsec板块
http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/d/opsec/?sort=top&time=all
Hacktown Opsec：
http://hacktowns3sba2xavxecm23aoocvzciaxirh3vekg2ovzdjgjxedfvqd.onion/misc.php?action=ACT0
Whonix OS文档 https://www.whonix.org/wiki/Documentation
Tor Project问答 https://support.torproject.org/
Tor Reddit Wiki https://libredd.it/r/onions/wiki/index

（一）喝茶解谜 公安的技术侦查如何工作，弱点何在
直入正题，根据此前调查，中国省级公安部门以下的国保、网警、值班警察大都没有对境外社交媒体的技术侦查的官方技术资源、培训、经验，只负责按省级公安的公文指示，电话传唤当事人到派出所，或上门传唤和对设备简单的搜证（大多数时间是肉眼搜证），甚至无法判断展示的手机是不是那部“作案工具”或已经销毁证据，我的推测是调查这个问题对政治警察来说只会耽误时间（只想尽快完成数量，不想多耽搁几小时）。
对于大多数用户的技术侦查是由省公安厅利用承包商搭建的系统，对境外社交媒体进行大规模地、自动化地搜集和侦查。市级公安、国保、派出所绝大多数没有官方提供的对境外社交媒体的技术侦查资源，

很多负责传唤的警察不会翻墙甚至从未接触过这类案件，有些警察会用“自由门”很可能是上一个被喝茶的人传授的。也偶尔有人发现网警能够熟练翻墙，有自己的推特帐号且“就混在我们中间”。在很多案例中，负责传唤的警察也看不到“违法证据”，甚至连在哪个平台发表的也不知道，只是知道一个大致讯问方向，然后通过反复的威胁来传达恐惧。
从翻墙工具不下放给市级及以下的公安、不让警察看到“违法证据”这两点，即可看出中▫当局对公安人员实际上也充满戒备，需要让他们像驴一样让他们蒙着眼干活，哪怕给讯问工作带来很大困难也要防止其借工作机会偷偷了解真相。

中国公安曾在2019年高调宣布侦破首起暗网案件，不难看出此人多次犯了直接使用信用卡这种低级错误，而且实际只是一个明网色情网站，搭建了一个暗网镜像而已，而中国公安居然违法地将该类经济案件的侦查细节保密，怕宣传的神话破灭暴露自己整体泥腿子的水准。我的受访者告诉过他们亲身经历的笑掉大牙的案例，例如直接关机带走取证断电即清空的内存硬盘，或者不证据固定让当事人自己上手操作最后被在眼皮底下删光证据而不自知，不会使用当事人使用的手机而请其它案件的政治犯（是的，政治犯，不是技术犯）来帮忙取证，有的没有取证工具用微信一张一张发送手机相册里的反动证据。不要相信那些充门面的大规模监控手段代表了人员的整体水平，全世界只有中国“成功实现”了步态识别的商用（因为其它国家不可能花纳税人的钱允许银河水滴这种公司招摇撞骗）。

可以看出，公安维稳系统当中拥有对境外社交媒体技术侦查的技术资源、训练、经验的公安在总数中占的比例较低。中国的整体教育水平和质量，以及其长期依赖强制行政手段、非法取证手段、非法审讯手段和反智宣传手段来减少侦查成本，加之其对手整体缺乏反侦查训练，致使其技术侦查不是强项（何为技术强，可参考欧洲刑警入侵Encro Chat案例）且很长时间内不会发生明显改变，虽有高科技充门面但实际整体水平依然落后。因此对境外社交媒体的侦查主要依赖从国产系统后门、中国区苹果系统后门、和运营商搜集的数据所搭建的自动化工具。出于对侦查成功的数量追求，大多数网警主要使用搜集到的现成数据，在目标影响力近似的情况下，多数时候不会去几百倍的花时间调查那些Opsec不错的用户（可见大规模监视系统搭建来只是用来控制守法的普通民众）。如果在信息安全方面训练有素的用户增多，公安的技术侦查工作便会出现崩溃。

（二）与维尼熊赛跑
相比大家听过两个人被熊追赶的故事，不需要跑得比熊快，只要跑得比同伴快就能活命。当追赶的一方变成维尼熊的时候是同样的道理，但我们的目标不仅是自保，还要让自己与同伴跑得越来越快，最终让维尼熊要么饥不择食吃小粉红，要么吃草、饿死。
当公安手上有几个影响力相似的目标，如果其中有已经被大规模监视程序收录、通过20秒的公安数据库检索就能定位的目标，那些需要专人用各种手段调查几百个小时才能抓到的目标就会被放弃。就我的调查分析，警察的主要人力就在于抓那些20秒就能定位的人。
在采取防护的过程中不要着急，也不要期待一帆风顺，你有可能需要几十分钟、甚至几天的时间准备（例如选购合适的设备）、学习、理解、测试才能完成安全配置。中国公安大规模监视系统囊括的对象正是那些连20分钟的耐心都没有的人。如果实在缺乏必要的资金和硬件（例如手上只有华为小米手机），首先非常欣赏您的热情，但是建议先保持观望、静候时机，等有闲钱添置设备再说，否则只会给自己和同道带来不必要的伤害。反抗之路道阻且长，政治倾向没有暴露就是你最大的优势。
在参与活动之前，应该仔细考虑自己的能力和革命意愿，例如发什么样的内容，达成多大的影响，以及对其采取相应的防护策略，并在严格地制订计划在安全性不足时放弃该身份，确保自己未来一直与政治警察“射程范围”能保持足够的距离。在头脑最理智的时候提前制定撤退的规则很重要，很多人在影响力突破了安全防护的范围之后，被声望冲昏头脑而不知撤退，很快会被反应过来并投入大量侦查资源的对手击溃。

手机、邮箱、帐号等要素【政治活动专用】对匿名而言重要
通过这6+1个要素的追查全自动运行，犯其中任何一个一次都会让你身份暴露

**(1)境外社交帐号绑定【过】+86手机号，绑定【过】中国邮箱，包括绑定后马上删除、换绑和改名的
(2)使用过国产手机，苹果手机使用中国区苹果帐号，使用中资输入法，使用了非官方渠道下载的app
(3)境内社交媒体相同网名
(4)上传人脸指纹声纹等与个人身份相关的信息
(5)截屏微信,QQ私聊和、网购订单编号、外卖【单号】、购物车,【在豆瓣知乎这种存在暗水印的平台截图】容易从公安数据库检索的内容
(6)主动告诉其他网友以上信息
**

(7)以上失误发生之后坚信【删除推文/更改资料】、【更改绑定的手机号/邮箱】、【修改用户名/修改用户ID】就没事，未能销号、抛弃旧身份、建立新身份
（每个推特和Telegram帐号有公开的、不可更改的User ID，利用 https://twitterid.com 等工具或下载个人档案可以查到，因此身份暴露之后改掉username和昵称没有用）

推断的工作原理：
在使用+86手机号或中国邮箱注册推特或Telegram之后，中国公安的大规模监视程序会立刻通过推特的中国手机短信验证码承包商英富必（一家中国公司），或Telegram的手机号搜索API，或推特或Telegram配合了中国公安对+86用户信息的请求直接共享了信息，也有搜集泄露的数据库，将手机号或邮箱和帐号的User ID录入数据库。
中资手机、登录中国苹果帐号的苹果手机则是利用系统后门，上传系统内关于推特app的帐号信息，将IP地址、手机卡IMSI、手机号和境外社交软件帐号录入数据库。
中国公安使用爬虫（可以理解为点开每个链接、下载所有内容然后不断循环直到下载完所有公开内容的一个程序）会记录每个公开活动的用户的User ID、暱称、头像、简介、推文、公开聊天等信息，只要上传便会被永久记录，如果网名与境内社交媒体相同会触发大数据识别，将该网名与境内社交媒体的人关联起来，为进一步调查做准备。注意，不要因此挂出来现实中认识的仇人的名字或手机号，一旦这么做，就可能怀疑号主在此人的社交圈里了。
同上，爬虫搜集之后会跑人脸识别，在人力调查过程中如果发现类似的照片、采访录音，可以运行声纹识别（有些黑产已经在提供声纹识别服务了）。
同上，爬虫搜集之后人力调查或收到举报，会调用外卖软件、网购软件或植入隐形水印平台的后台查询。
其它网友不能为你保密，必定会因为不严谨、不同政见、个人不合、政见发生变化、个人设备不安全、受胁迫招供或当线人而出卖你的信息，而且也很难得知对方是否是网警。
删除和更改个人资料覆盖不了也撤回不了已经发送出去的记录，同时推特和Telegram的User ID是公开且不可更改的，除非注册新的帐号。

与之对应的解决方案，从创建虚拟身份开始就要严格执行

(1)使用Google Voice注册推特帐号，如果有境外网购的渠道就优先不要从淘宝购买，绑定Tutanota或Protonmail邮箱（无需提供额外信息即可注册的境外邮箱）
(2)使用Google Pixel或索尼等外国品牌且不在中国官方销售的“水货”安卓手机，或苹果手机App Store和iCloud都永远使用美国、日本等区的苹果ID，不使用中国输入法。必须只能从Google Play、Aurora Store、Fdroid、App Store四个官方渠道下载app，尽可能第一时间更新手机系统和app
(3)使用全新随机的用户名和ID，建议使用维基百科随机页面随机词汇，全新身份不要与之前身份有任何相似性
(4)避免上传含自拍、手掌、笔迹的照片、视频和录音，截屏、拍照要反复检查，尽可能就一张自己拍的照片都不要发，一定要发的话，注册小号投稿给别人
(5)不要发有关生活的内容，如果要发注册生活小号【并且不要关联大号】，或者小号投稿
(6)不要闲谈中为了社交价值（拉近关系获取好感）把个人消息告诉网友，除非能够换来关键的帮助（例如在失踪之后能找到人）

(7) 如有任何失误，必须销号抛弃旧身份，没有其它补救方案。建议对每个方案测试和熟悉之后再开始。

有余力者：
微信等中资软件会绕过部分系统的安全机制监听其它软件，亦有迹象表明可能成为投递间谍软件的管道，建议有余力者购入第二部手机，二手的Google Pixel手机只需几百元。手机上不要装任何中资软件，软件越少越好。
安全防护应该从这种容易从公安系统里检索的信息中开始。推特不像品葱、大纪元或2047，即便域名或IP泄露或者被亲共“机场”记录也并不算可疑，亦没有案例发现中国政府通过从推特或Telegram官方获得用

户的IP地址从而追踪到用户的案例，因此VPN和IP地址不是【一般用户】在境外社交媒体匿名活动的防护重点，尽力而为，当然如果你已经做到增强VPN方面的隐私和安全这是最好的。
有针对性的防护是非常重要的，对于理解有限的新手来说，如果失去重点，就有可能发生一边还在用+86注册的帐号，一边用虚拟机、防流量分析、防语言特征分析。

我曾经想向所有人推荐安全性最好的Qubes系统、Tor、门罗币等优秀工具，很多朋友也有像我一样的想把所有人培训成编程随想的急切想法，这是因为我们相信不想追随（或超过）编程随想的反贼不是好反贼。但我在实际操作中发现这么做并不可行，绝大多数人连基本的防护都漏洞百出，很容易退缩，而且缺少必要的热情、经济、技术和英语能力。很多人读过编程随想的文章，知道敏感活动该全程用Tor，但至今我从未发现一个人能跟着照做并希望以此做一番大事。不如帮大多数人先做好基本防护，在其中挑选有行动力、学习能力较强的人再进行循序渐进的培训。因此同样Opsec不错又有教学热情的同道一定要考虑受众的行动力和条件限制，一步一步来。

除此之外，在购买VPN时，有些厂商会让你填写境外社交媒体或邮箱，由于大多数人VPN是实名支付，因此注册VPN不要用反共活动通讯邮箱，最好用一次性邮箱或者单独注册。**注意不要用老王 TurboVPN等成品的钓鱼VPN**，虽然推特、Telegram的流量是加密的不受影响，但这些VPN本身会搜集IP地址和硬件信息，只是使用这些VPN都可能被传唤，因此应尽可能用V2Ray、迷雾通等开源客户端。

（三）出现失误之后科学地建立全新身份

大多数人认为点击删除、换绑手机号或邮箱，或者删除暴露身份的信息之后就安全了。事实上，点击删除之后，推特后端的数据库未必会删除记录，对于公安的数据库已经搜集到的数据，更不会随你的删除操作而删除或者被覆盖，或者因为时间久没被抓而认为所产生的数据已经被遗忘或者未被公安成功搜集，因此没有销号，或者销号不彻底而仍被传唤。最简单的办法就是注销旧号，建立全新的虚拟身份、社交关系。

很多网友会问用港区帐号有没有问题，Google Voice绑过QQ邮箱有没有问题，首先我很抱歉我不能调查的这么细，也没有办法给出负责任的答案。我的建议是，**我们离对手的射程范围越远越好，没必要非要偷懒一只脚踩在射程内**。如果对手的能力随着时间发生增长，在边缘试探的人就会成为第一个躺枪的。如果为了在重新注册帐号、不混用生活帐号这些问题上省几分钟，很可能在一两年后会面临被国保胁迫删除几年的工作成果和回忆（公开案例参考端点星案件），甚至受到严重伤害。

对于进行了安全准备之后决定建立全新身份，必须从每一个维度切断与此前身份的联系，甚至做相当的伪装来确保无人认识。很多人新号用相似的名字；很多人在注册新号的简介上挂出以前的身份，试图找回老友；有些网友在建立新身份之后会私下告诉曾经认识的人“我是之前的xx”；有些人的新帐号一看就知道是以前的谁，这些都是失败的新身份。有很多时候未必所有网警会花时间细看，但是可能被不严谨、不同政见、关系破裂、被审讯的网友不小心泄露或直接向警察举报。
在倒台的专制国家的档案中，父母、配偶、子女、多年的朋友成为线人屡见不鲜，有的人一句话能被20个人举报，更何况素不相识且不需要对你的生死责任的网友，因此生死要把握在自己手中，唯一能为你保密的只有你自己。

没人是天生的革命者，每个人早期不熟练的情况下都会产生失误。对曾经犯下的失误的错误处理，是已经有防护意识、采取了防护手段的网友栽跟头的主要原因。因此防护的重中之重在虚拟身份建立就应该以上所有手段，避免以上的所有错误

随着活动的敏感度提升、影响力的增加，超出了之前Opsec所能保护的范围，应该考虑建立全新身份之后用更好的Opsec经营新的身份。

有些人在opsec出现失误之后，出于对回忆、朋友、关注的不舍，难以销号，甚至在被国保、国安传唤之后仍然忍不住偶尔使用，这种心情可以理解。但是要长远考虑，如果opsec没有做到位，用的越久则风险越大，销号的损失也越大，早建立新身份早受益。在有安全的本地环境的情况下，可以考虑销号之前导出备份并加密存储。

有些人会问，你让人销号是何居心，销号不正是中共希望的吗？我认为，在能够明确判断自己的虚拟身份已经被“定位”之后，自己提前抛弃旧身份好过被国保逼迫销号。销号不是目的，建立一个安全的身份，未来三年、五年、十年可以一直用该身份放心大胆地批评中国政府，与伙伴建立长久的信任和合作，这才是目的。唯有此，方可建立一个紧密的、稳步壮大的社区。当下的状况就像淘沙子一样，三天两头就少一个伙伴，2年过后除了肉翻的网友整个社区换了一批新人，大都刚积累起一些经验和认识就被收割，非常让人痛心。既然称呼自己为“反贼”，就要长远考虑如何造反。

在借助大量的案例准确地发现雷区之后，明确【知道不安全】后自己主动销号避开不必要的风险，并建立新的身份在【知道安全】的情况下越战越勇，这好过【不知道不安全】而意外被捕，以至于再也不能或不敢发言和参与行动；或在【不知道是否安全】的情况下总感觉头上悬着一把剑，继续自我审查，不敢点燃内心最深处的正义怒火。做调查的目的是在黑箱里发掘案例，分析出准确的信息，帮助人们用准确的信息指引行动。

我不希望我的同道仅仅是因为无知无畏而参与行动，或许短期内可以充人气，但长期必然让社区和有组织活动充满弱点。选择不同，很大程度上取决于一个人的视野，是更重视100个反智的、松散的、只会跟风的玩梗小鬼，还是10个精明能干的有识之士。我期望更多人能在准确认识风险和前路的艰难险阻之后，依然义无反顾地投入革命事业，成长为有勇有谋训练有素的革命战士，接受社会运动和革命事业的洗礼。

（四）有关匿名和必要性的争论

有些人喜欢实名，反对匿名，以喝茶、坐牢为荣，甚至以没受过迫害为耻。我的分享只是让那些希望匿名发声、不想被传唤的人也有机会参与革命活动，确保他们成功达成匿名的预期。解开禁锢、享受过自由表达人数增多之后，也必然有更多人会公开活动。我不反对公开身份的人继续做下去，或者更多人以公开身份抗争，在明处或在暗处，只是根据个人情况不同做出的选择和分工。借匿名保留收入、产业、职位、人脉、权限，则可保留宝贵的经济、政治等资源，亦可渗透进中共的内部进行瓦解。当然也可以根据自己需要建立多个身份两者都做。敌在明、我们在暗是重要的优势。很多人反对良好的Opsec是为自己懒于学习、缺乏行动找借口，当然有些也是为了让其他人放弃警惕的宣传。自己喜欢实名可以用微信嘛，或者去派出所备案一下自己的推特帐号，让其他人放松警惕就其心可诛了。

有很多人说“不是编程随想，谁管你，xx实名翻墙也没事嘛”，这类主张看似仅仅是反智，实则是用以降低革命者的警惕和网警的工作量的精妙宣传，也是中共能够持续破坏和瓦解反抗社区的最高效最成功的秘诀之一。事实上，不管是技术侦查部门还是负责传唤的国保，不仅数量庞大，常年饱和、超负荷工作，也是所有警种当中最忙的。不仅针对频繁发言的、有影响力的键政用户，有些人只有个位数follower、甚至只是点一个赞和追随革命人士也可能被叫去派出所问“为什么要做这种事情？！”，如果国保没完成指标，甚至常常把当自干五、看黄片的人等拉去充数。一位受访者告诉我，他所在的城市的单个派出所当天境外喝茶的名单有30多人。我能理解有些人不希望让技术的难度把人劝退，但是我深知我的同道不是

炮灰，我不希望任何有良知和潜在行动力的人仅仅因为错误的信息和判断而受到意外伤害，更不希望明明有简单易行的机会采取有效防护再行动，却偏要赤膊上阵。

有人对自己擅长“把握分寸”很多年没翻车引以为傲。在暴政之下，不唱赞歌不鼓掌再微小的反抗行为都是值得鼓励的，但另一方面也有一些鼓吹自我审查的成分，无益于扩大激进的反抗群体。我们在匿名之后，从来就不怕中共的什么分寸，好的Opsec和匿名是彻底摆脱自我审查、解放思想的良药。

有些人说“喝茶没什么大不了的，没必要过度紧张”，事实上传唤、威胁、骚扰可以非常有效地扼杀萌芽期的潜在反共者。当然不排除很多人出于自我保护心理不愿接受残酷的事实，一厢情愿自己真的相信这种说法，一个有趣的现象是，一但喝茶这些人反倒是最胆小怕事的，我认识的这类人绝大多数已经“坟头草三尺高”了。如果传唤不能有效地伤害社群、有益其维护统治的话，中国的网警、审查员、网评员为何数量如此庞大还要累到猝死？为何防火墙、金盾、反诈中心等项目为何还要每年耗资百亿？为何高智晟律师、陈光诚律师每年每个人维稳开支千万？资产□□的目标是“无微不至”地奴役世界上的每一个人，绝对不存在什么事情“懒得管”，不管有些人怎么用“老百姓”“小老百姓”“小民”“谁都不是，没人管你”这类语言对自己的身份矮化，就差把“奴才”二字贴在脑门上，翻墙了解真相和“键政”在匪警眼里依旧是严重违背奴隶的身份的事情。而相信自己“谁都不是”的人，也是在逃脱自己的公民责任。遇到这类 人不要争辩，这正是对每个人行动力评级和遴选同伴的好机会。

有些人非常执着于让其他（海外）政治活动者露脸，生怕中国政治警察工作不够方便。有没有实名露脸并不重要，个人的活动是否正当以及能够造成多大影响才是重点。论露脸，希特□□波尔布特、齐奥赛斯库、习奥赛斯库乃至胡锡进、金灿荣、张维为之流天天露脸，满街贴得都是他们的脸，并没有没妨碍他们做出人间最恶之事。匿名不能说明一个人不够勇敢。能够付出精力学习、做出准确判断，并将自己的对暴政的不满表达出来、付诸具体行动，越战越勇，这是精进、勇敢和智慧的最佳体现。中共通过数十年的缜密而血腥的镇压把线下的民运组织、宗教组织、维权群体、少数民族、社会团体打散，而匿名是维持反抗社区的生命力最后一道防线，也是重塑凝聚力的关键武器。随着匿名的社群成熟、健壮、扩大、集结起各类人群当中的同道，这些社区随时便可转化成上街暴起的行动力。匿名和隐私是自由思想的温床，许多有行动力的革命者是从爱党粉红开始，在逐渐卸下恐惧和自我审查之后，通过了解信息、发表自己的想法、辩论，逐步升级。

信息安全的目的是保护两个要素——证据（或侦查线索）和情报。信息安全不仅关乎反抗者个人的存亡（这是【证据】能够造成的伤害），而更重要的是关乎反抗社区的存亡和反抗运动的成败（这是【情报】能够造成的伤害）。对于信息安全的理解，如果一个人的眼光只停留在一句话、一个动作对个人抓捕的影响的层面，而看不到【情报】对长期、组织活动的伤害，那么他必然不是能长久并肩作战的同道。 这里不是歧视或者排斥非技术背景的人士，任何人都有机会作出提升，最简单的便可从选用手机品牌、培养使用加密通讯软件的习惯开始，重点在于心态和付出的努力而非技术高低。有一位海外自媒体人坚持使用装了微信的华为手机上的Telegram联系其他人，并坚持使用Zoom接受其它人的“匿名”爆料，面对质疑时他回答“我没有隐私”，还笑着说“刚刚我们的对话都被监听了”；许多已经出国的“反贼”也因为个人没有安全顾虑而不愿学习信息安全；还有许多反智者认为海外活动者应该敞开让中共监视，好吸引和消耗监视资源为境内活动者减轻压力；有人自作聪明用虚拟机等手段以为能驾驭对方的间谍软件；更有甚者坚持使用云上贵州和微信并称“我照片太多中共看不过来”；有些活动的组织者坚持使用中国间谍软件Zoom或者腾讯投资的间谍软件Discord作为视频会议和团队工作软件…… **即便自己、家人、队友全都不怕死，依然需要尽可能地采取手段阻止对方获取情报，谋事不密必失败。即便一个人已经出国或者不在乎自己被抓，日常处理的信息中仍然会包含危害其它人安全的证据（线索）和危及反抗运动的情报。**

这类人眼里没有其它人的安全（尤其是在中国冒险联系他们的人），也不在乎反抗运动存亡和能否壮大。 这类人希望自觉一点，把“正在使用华为手机/安装了微信的手机与你通讯“”与我发生的通讯会被中国政府监听”贴在头像、用户名、个人简介上面，在开始通讯之前予以警告。

在不能抓捕的情况下，谋略、离间、栽赃抹黑、切断资金是最重要的破坏手段。对于境内人士，提前掌握情报进行预案，便可在难以控制的集结行动发生之前有效地控制、拘禁、封锁、分化瓦解（参考茉莉花行动）。掌握通讯、人际关系、个人信息和习惯、资金状况、活动状况等对于中共控制局面至关重要。因此，即便实名公开反中共，一个负责任的人也应该强化安全意识和信息安全，在公开场合除了宣扬 主张外，不要泄露任何通讯、资金、私人矛盾等状况，加密所有通讯，深思熟虑地决定分享或保密信息，不可不假思索地公开信息。是否在基本的信息安全投入成本，是判断一个人是不是负责任的实干家的最基本的标准。推翻暴政不可靠个人一腔热血，而是专业知识、经验、协作、资金、缜密谋划、耐心积累，这类以无知无畏为荣的现象，与义和团菜刀对阵英军的火枪、祖鲁勇士举着长矛冲向马克沁机枪阵地有很多相似之处。在敌我实力悬殊的情况下，速度、组织、秘密是打败对手的必要要素，以一盘散沙对抗每年投入万亿维稳、100年情报和反情报经验、超过30年维稳经验的政权是不切实际的。

学习和实践信息安全是高压、枯燥的，匿名与人类渴望名声、喜爱分享的天性冲突，成功的匿名是对技术实力、经济实力、学习能力、自控能力、忍耐力、缜密性、以及对自由的向往程度的考验，凡通过考验者必是你并肩作战的最佳伙伴。

（五）警察无所不能，匿名技术没用？
有些人说，编程随想都被抓到了，这些技术手段还有用吗？这种看法就像一个人穿防弹衣挡下了几百发子弹最终还是被打死，就说防弹衣没有用一样荒唐。如果中国的政治警察普遍具有这么强大的侦查能力，就不需要禁止使用境外社交媒体、Tor和加密通讯了（用如此力度长期封锁网络全世界只有中国、朝鲜、伊朗、土库曼，甚至不包括俄罗斯和沙特），也不需要给每个人的手机上安装反诈，或者采取“把隐私交给国家有何不可”“你有什么见不得人”的宣传策略。

【编程随想本身的技术局限】熟悉信息安全的人，可以从很多细节中发现编程随想很可能没有信息安全的专业背景，很大程度上为了躲避对职业的排查，而通过自学建立的形象。他采取的方案很多也并不是Best Practice，甚至有一些明显的错误（对于没有经验和训练的人来说这是很正常的事情）。
例如编程随想在匿名手机号的教程中只提了现金买SIM卡和纯净的手机系统，居然没有提及基站对手机的IMEI串号追踪（标准的操作是现金购买手机和SIM卡，接一个验证短信之后就一起扔掉）；例如主张排除俄罗斯的洋葱中继，这样会制造指纹；例如选用“program think”作为windows系统的用户名，这很可能会上传到微软；例如使用VMware和Virtualbox而不是更安全且隐私的KVM和XEN（2009年也没有Qubes和Whonix这么成熟的匿名工具）；例如使用原版Firefox而不是Tor Browser（Firefox会上传用户数据，隐私和安全较Tor Browser差得远，而且定制也会产生浏览器指纹，不过2009年也没有Tor Browser）；例如早期的截屏全都是不安全不隐私的Windows，实际只有体验过Qubes系统才知道什么是安全的方案。
例如他的教程极少涉及具体案例研究，而在西方黑客社区中有至少几十个涉及网络犯罪的法院案例的分析总结（不讨论正当性的话）。
手机卡： https://program-think.blogspot.com/2019/01/Security-Guide-for-Political-Activists.html
系统用户名： https://program-think.blogspot.com/2010/06/howto-prevent-hacker-attack-1.html

【编程随想的人为失误】也不能排除编程随想因低级失误和人为因素被捕的可能，没有自学Opsec和操作经验的人可能没有体会，实际操作未必会像理论一样完美，这种事情也经常会发生。在不断学习和数百万次的重复操作中，很多时候会因为走神、疲劳等原因犯下错误。**黑客应对这种情况的常见做法是定**

期丢弃身份和销毁全部作案工具，即便自己没发现犯下错误，不代表警察不能发现你的失误。 其次编程随想能在匿名方案不成熟且不普及、没有实战经验、现学现卖、一人之力、一枝独秀的情况下活动11年，正是说明opsec可以有效地大幅延长生命力，在匿名方案成熟且普及、积累经验、训练有素、里应外合、风险均摊的情况下，轻轻松松存活十年以上更是有了信心。自暴自弃、恐慌或造神都对未来的活动没有任何益处和建设性的指引价值，正因打倒编程随想有重要的宣传价值，中共才会如此不惜成本。**也正是因为对编程随想的抓捕不计成本，不可能应用在十个人、一百个人、一万个人身上，而且到那时抓其中一个人也没有这样重要的宣传价值了。**

【排查对象太少】除了人为失误，我的另一个猜想是中国绝大多数翻墙用户Opsec太差，防护良好的用户集合太小很容易凸显出来以排查。一个常用的例子就是如果一群人里只有一个人戴着面具，那么很容易追踪他的一举一动，只有所有人戴上一样的面具才能真正匿名。因此，对于许多用户来说，即便采用匿名工具后暂时不参与什么激进活动，仅充人数，也可以帮助真正的革命者更好地藏匿于茫茫人海，助其行动。从另一个角度来说，如果中国政府因为无法控制庞大的匿名群体而大幅收紧或关闭国际互联网，对于其对外贸易、保留外籍游客和居民、基础网络设施、以及利用翻墙网民为掩护的黑客窃密活动来说都会有致命的打击，也算是行加速主义的好事。

编程随想一直是我最尊敬的前辈，但是我从很早也开始挑他的毛病，并不是为了贬损他或者抬高自己，作为匿名反中共第一人，他的成就是无与伦比的**了解到编程随想的Opsec缺陷，才能认识到对手并不可怕，相反把编程随想造成神，间接把击败他的对手也造成神了。**我也非常懊悔没能在他被捕之前有足够的能力发现这些，并给予他警告。包括我在内的每一个写作者、开发者都不能提供完美的内容，我在早期也发表过许多错误的Opsec，错得比他还要离谱（惊讶的是居然从没有人向我提出来过）。只有花时间全面、多方地了解，形成自己的判断。除此之外，认识到你的工具、教程、个人操作必然存在漏洞，每个人每天都在犯错，要给自己、作者和开发者留一些失手的余地。Don't take my word. Do you own research.

（六）为什么有些人没被传唤
对于可控的、没有【即刻威胁】（例如组织示威抗议、组织反共活动等行动，公开案例可参考乳透社拜年祭）和收网的【即刻价值】的Opsec菜鸟或实名人士，如果国保打算将目标从“喝茶”升级为“起诉”，会选择有计划、有控制地放任发几千条甚至几万条，为的是方便积累证据判刑，好在年底、党庆等时刻冲重量级案件的业绩，所谓把小鱼“养肥”成大鱼，从我的调查中发现可以潜伏一年甚至几年才抓捕（公开案例可参考卢昱宇）。采取暂时放任对警察来说有很多好处。政治活动家中的Opsec菜鸟大多是守法者，很容易控制（例如没有逃脱追捕和偷渡的能力），也很容易监控通讯和动向，放任其在外活动就是搜集情报和挖掘反抗社区的“人形海绵”。在搜集更多证据之后，不仅可以用来起诉，还可以在搜查之后从手机上几年的电子记录中和嘴巴里发掘出其他伙伴的信息，审讯几天便可获得网警花几年时间伪装和调查都换不来的高质量情报。

同时，这些Opsec菜鸟的冒失行为配合有心之人的宣传，也可以让其他人放松警惕，让网警的工作难度大大降低，这比高科技侦查手段更有效果。反之，如果身份一暴露马上喝茶，不仅很容易反推其侦查手段、予以防范从而更难追查，在完成“重量目标”的指标时也要花更多精力调查，不如把菜鸟“养肥”后宰杀手到擒来。除此之外，提前搜集、静候时机的方式在紧急事件中也更加可控，例如有一位匿名网友在举办重要活动的前夕遭到传唤，被成功阻止，如果平时把名单上的人都用光了，届时调查很可能来不及掌控局面。除此之外，这种不确定性可以有效地给所有人心中蒙上一层恐惧的阴影。

很多人讲述反侦查策略的时候会说“中共”如何如何，但事实上中国政治警察的运作逻辑并非是最大化维护【系统整体的利益】，大多数情况下我们面对的是一套僵化的考核体系中的一员或一个小组，案件受办案警察个人的指标、升迁、偏好以及时间等影响非常大，简单来说如何办案完全取决于如何最利于办案警察个人升官发财。涉及到某个官员个人利益的时候，为了取悦该官员或直接间接受到该官员施压，政治警察通常会比危及到党国整体利益的时候工作积极得多。例如涉及习近平的案件优先级是比较高的，有网友在境外社交媒体上发了一位高官的动向立刻就被传唤（也可作为上一段落【即刻威胁】的案例），反而六四、疫情、反送中等要相对辱包没那么要紧。因此，放任菜鸟在外多一年或者发表更多言论，警察不会在乎这么做是否会对党国造成更大伤害。有时需要凑数，有时需要重量级案件，有时侦查立案的是外省的公安，很难把握准确。因此不管对手心理和逻辑如何，我们以不变应万变的方法就是做好自己的Opsec，以此为基础，安全系数越高可越加放开手脚。

我还接触到极个别案例，其中因为家人是富商、军官、政府官员，背景显赫。有的人可以在大案中化险为夷（公开案例可参考恶俗维基案顾阳洋）；有的人可以进派出所像进自己家一样频繁，依旧招摇；还有很滑稽的案例，警察问“可不可以不再发了”被理直气壮地拒绝。89年之后出生的年轻网友普遍不愿公开自己被传唤的情况，出于不想惹麻烦的心态可以理解，我个人也不主张当前正面对抗，通过负责任的人把经验教训匿名公布出去使大众知情是普遍推荐的解决方案。因此诸位不要以那些Opsec菜鸟或者实名的人为衡量自己人身安全的参考，他们具体是擅长自我审查、正在被养肥还未收网、实际已经肉翻、只是假装Opsec很差、不承认自己被传唤、背景硬，甚至是线人、网警或者外宣都有可能。除此之外，地区、时间、民族、职位对于传唤也有影响，一般“社会人员”传唤后果重于在政府国企雇员和学生，新疆网友“九条凛”则是轻易就判刑2年，年底、开会前、运动式执法也会有显著影响。控制社会是一个复杂的工程，对于一个几十万人的人治的系统，不可能用几条规律掌握和预知其所有行为。总之，还依赖初学者教程的你不要期待成功复制那些看起来无知无畏的个例。

（七）用匿名来做什么
在配置了良好的Opsec之后，我们就有了一种不再受奴役的感觉。用它来做什么呢？

对于刚翻墙的网友来说，可以浏览禁闻、禁书、纪录片，转发新闻，批评政府。批评政府重点并不在于能对中共造成多少伤害，而在于解禁自己的思想。从基础开始学习现代文明国家政治制度，学习英语，参与讨论。Khan Academy可汗学院、Hillsdale College的美国宪法课程是很好的学习资源。

在有一定积累之后，便可开始写博客、文章，制作民主图片、视频、绘画文宣，像记者一样搜集、调查、发布新闻，翻译新闻和中国人的言论，发表在Telegram频道和推特。发展自己的联系，找寻同道，分享自己的认识，互相扶持成长。
制作网站，整理历史资料，参与线上的抗议和悼念活动等。
可在线上举办读书会、观影会等，分享建设性的想法，Opsec互助教学等，发现有行动力的同道，一起筹备项目。

线上匿名活动只是暂时的战略撤退，目的是建立敌后的安全区以修整和重振旗鼓。中国公安最担心的是引发墙内舆论失控和线下传播信息，因此在形成一定基础之后，应该将翻墙工具教给信任的人，试探性地影响身边人的政见，尤其应该注重影响各行各业有成就、有才能的人，教他们如何阅读境外新闻、使用境外社交媒体，并鼓励和督促他们把翻墙工具和社交媒体去中心地（每个人都只教几个信任的人）分享给更多同事、同学和身边人。不建议直接分享本教程，但可以提供机会让对方自己发现。如何策反身边的人是一个技术活，有经验者之间应当建设性地分享话术、方法和经验。

用单独的帐号建立学校、区域、同行群组和频道，培养大家使用境外社交媒体的习惯，倡导大家用Telegram和Twitter代替微信等工具。与其它组员保持联系，进行一定了解，但是联系中应该格外谨慎，这种群组中钓鱼的力度会很大，决不能暴露任何可追查的信息，重要成员更不能与其他人见面。在维权、示威、抗议、罢工行动中，临时才从零开始推广境外社交媒体不仅很难顺利使用，耽误时间，还很容易被追查源头和骨干成员，因此应该提前准备。当微信群开始被打压之时，就是让每个人在社区内去中心传播翻墙工具和通讯工具的机会。除此之外，去中心化的Element短时间内难以被防火墙封锁，因此可以给不能翻墙的人使用，部署服务器非常简单，网络上也有一百多个现成的服务器，配合Telegram传播，在“群体事件”中可以大显身手。媒体人、艺术人、律师、程序员、医生等有专业才能者是我们最重要的伙伴。

建立紧密的联系之后，可以轻易动员关系网络进行文宣制作、印刷、投递，与靠谱的人有分工、有计划、秘密地做，在同一时间协调发布，在维稳部门面前占领先机。管理群组、联络、搭建服务器等风险较高的工作应当采取里应外合的手段，由熟悉的、可信任的境外网友来做，重在提早准备。分化后逐个击破是中共管用维稳的手法，如果个人和社区训练有素，便可让维稳部门一时难以摸清带头者、组织结构、关系网络找到弱点和突破点，也无法切断信息传播，短期内无法有效镇压。即便使用断网的手段成功镇压，在事后也会让社群更具有凝聚力。颠覆政权之路道阻且长，区域性的行动最终都会因对手庞大的体量以及数十年不断优化的维稳体系而溃败，目的在于借机传播境外通讯工具、激化矛盾、结识同伴、试水温和积累经验，有行动力和影响力的同道们应当Be Water，适时撤退保存实力，不可一步登天。

在“群体事件’发生之后，不仅应当迅速地把诉求、和警察镇压的证据传播出去，也要及时与可信的同伴分享经验和总结教训，把经验和细节积累起来，在自己的圈子中广泛传播，给未来的”群体事件“以参考和鼓舞。当不同的学校、区域、行业都经历了“群体事件”的洗礼之后，各个事件中的核心人物便可组织起来，有计划地同时发难，罢工、罢课、罢市、抗议、示威、游行同时进行，届时便是一起打出政治诉求的机会。

除此之外，对于希望走得更远的同道，匿名之后可以让你更安心地做一个的博主、公民记者、组织者、培训者，运行一个项目，发起一项运动。

使用各种手段推翻暴政是天经地义的，不要对颠覆政权的思想感到害羞。唯有大规模地匿名，才可孕育出难以消灭的地下党，这是我们在信息时代的丛林游击战。采取去中心的方案不是怯懦，而是风险均衡和分工，成功的社会变革绝不可能仅靠一人的牺牲达成，而是靠大众的共识。有行动力的骨干更应认识到自己的所处位置的重要性以及长期的使命，不可受感情支配，导致出师未捷身先死。有些人抱着“反正都是被镇压何必冒险去做无用功的想法”放弃行动的希望，甚至因此甘做线人。因此应当稳步积累、长期发展，让大众看到进展，才能在机会来临的时候调动起整个社会。提早暴露自己、把自己搭进去是大忌。再次借用反送中的一句口号”不是因为有希望才抗争，而是因为抗争才有希望“。（香港人、台湾人社运非常有经验，应当虚心学习，反送中、占中、太阳花乃至整个台湾民主化历史应当是每位反贼的必修课，六四自然也是，推荐民视的台湾演义系列纪录片）

（八）政治警察（国保等）是什么玩意

不要对中国的政治警察怀有恐惧和敬畏心理，他们不代表真理、正义、良知，只是既得利益者和暴政的打手（还要蒙着眼睛干活）。他们当中的大都是中国病态的教育体制的淘汰者，是“关系户”。他们普遍极度缺乏训练和专业性，满口脏话逻辑混乱，只会滥用权力和暴力，且几乎从不遵守法律程序也不懂法，只是拿着两三千元工资混吃等死的泥腿子。

有网友在喝茶的时候，建议警察把哪些话能说、哪些不能说印成小册子在小区里发，这样大家就不会“犯错”了，政治警察说这是违法的，可见也知道自己的工作违法；相当大比例的政治警察告诫被传唤者，可以翻墙看但不能发文，可见他们也不信自己“翻墙违法”的法律；有的人问政治警察外网的传言是否可信，对方回答“不可全不信”，可见也知道自己在扼杀真相；还有政治警察借机向女生索要私人的照片、联系方式甚至性骚扰；有的警察建议女生在境外社交媒体上多发软色情别发政治；有的政治警察畏惧对方家庭背景不敢让对方删贴；有的案件稍微严重，政治警察趁机索贿数万元……他们不关心你的言论真假、是否夸大、有无伤害社会（否则官媒记者和政府发言人都要被判刑），只是因为你的言论触碰了有权有钱者的利益，而利用这些马仔让你噤声。

许多政治警察自己知道做的事情不正当，怕被曝光、追责、倒台后清算，因此不出示证件，不报自己的姓名、部门和职位，甚至不开警车、穿警服。从这里这就可以看出谁是国家的主人。在有代议制的自由世界，政府官员的财产要公开，公民的财产属于隐私；官员要被人用选票打分，而公民不能被评分和歧视；政府官员必须实名，政府的文件可以由信息自由法公开，甚至媒体和出版物中的泄露的政府文件还受言论自由和出版自由保护，而公民的隐私不容侵犯……而在中国，一切都是反着来的。

诸位应该明白，我们的智力和认识在他们之上；我们的行为比他们更加正当、合法；我们有正经的、收入更高的工作，不像他们放弃了自己的灵魂，甘当一个背书单、不认字、念稿念错页、离了小本本不会说话的独裁者的马仔。他们破坏有良知的人的生活安宁和自由民主思想，燃烧掉大众的未来为自己一人取暖，这样的人没有资格对我们进行“批评教育”。政治警察随时也可以成为举着身份证的维权者和维稳对象，有时也会过劳猝死。

人行走在世间，总是与风险相伴，即便逃避属于自己的公民责任，也避免不了半夜吃烧烤或存款消失维权被暴打，或者半夜悄悄开闸放水被淹死，也无法让下一代避免毒奶粉、毒疫苗、豆腐渣工程毒害。承担公民责任是风险，当羔羊默不作声地被宰杀也是风险，人的生命宝贵，更应该将这一生活得有质量、有尊严、顶天立地。人不应该像奴隶一样窝囊，遇到不公应该让官员下跪，而不是向官员下跪，应该烧国旗，而不是举国旗。只有更多人承担起属于自己的责任，投入反抗暴政争取民主自由的洪流中，每个人才能享有本来就属于自己权利和长久的安全。

（九）如果已经被传唤，怎么办？
大多数情况下，传唤之后没有进一步的后果，因此不必紧张，电话传唤的事态不严重。一般的解决方案是立刻删掉帐号和应用程序、否认帐号是自己的并不再在新帐号上发言。我此前认为否认之后马上删掉帐号或者停止发文，会让警察发现你在撒谎，从而有更严重后果，但实际调查中发现只是报上去便不再管了。可以看出传唤主要是搜集口供、挖掘物证和传达恐惧的作用，对每个案例处理不会投入太多精力。除非当面表示对抗，可能激怒对方被公报私仇而拘留。在与警察谈话中，应当对其爱党政治观点表示附和，并无比配合、礼貌，但一问三不知。不要试图去说服警察或表示对抗，他们知道自己在作恶，但凡有点良知的人也不会做这样的工作，你说服不了他。

平时应该尽可能准备两台手机，一台日常使用，一台Google Pixel或非中国区帐号的苹果手机翻墙。日常使用的手机可以也安装翻墙软件用于伪装。应对地铁站盘查（个别案例）、学校公司盘查和传唤的时候，交出日用的手机并主动解锁即可。翻墙用的手机遭到搜查之后，如果想继续用于匿名活动，应该彻底重置系统，并建立全新的谷歌、推特帐号，备份数据和转移不要嫌麻烦。
如果敏感度较高有上门风险，应该时刻保持警惕，遇到可疑人士敲门不要应声，先用猫眼查看，让家人也不要给陌生人开门。一般不会遇到过破门的案例，但宿舍和旅馆管理人员会交出钥匙。警察也没有能

力破解Pixel和非中国区苹果手机，省级和大城市公安的技术部门可能会利用后门解锁国产手机，没有Bitlocker或Veracrypt加密的windows可以被任何人读取（系统密码不是加密），一般不会使用数据恢复。对于危险等级更高的网友，应该面对突击搜查进行预案和反复演练，在任何环境下都应留足反应时间，不要在有陌生人能近身和窥视的环境中操作，并确保在紧张的状况下也能迅速地删除记录。

很多人喜欢对聊天记录截屏，在非敏感的场景中或许还情有可原，但如果用于发表政治活动，则是截屏、聊天记录越少越好，即便有加密和安全的技能也应当定期清除。信息自从看过第一遍之后，就已经发挥了大部分的价值了，即可删除。日后留的越久、攒得越多，对自己的价值越小、风险越高，警察假若数字取证，能获取的信息也更多，对自己和他人都没有好处。华为小米等国产手机、登录中国区帐号的苹果手机、装了微信等国产软件的手机上尤其不建议保存聊天截屏或者乳包图片、视频等，许多国产软件多次被发现有上传浏览器记录和扫描文件系统的行为，甚至主动删除截图（参考拼多多）。有两位网友向我反馈，即便用非中国版华为手机，在本地存储的乳包视频被识别出来然后悄悄删掉了，因此中国公司的手机和软件应该尽可能减少购买和使用，并鼓励其他人也这么做，以免为虎作伥。

对境外社交媒体的证据应当全部否认，因为传唤当中所用的“违法证据”的采集非常粗糙，一般是只有手机号孤证和一堆对言论的截图，不会仔细核查，有些承认了就赚到了的碰运气的成分，因此警察自己对境外社交媒体采集的证据也没什么底气。有两位网友使用了亲戚的手机号注册了推特，国保在喝茶的时候直接找到了他们的亲戚，看得出来并没有通过IP记录等其它辅助手段侦查（侦察了也没法独立作为证据，因为IP很容易盗用）。如果拿不到口供和证据，一般会放弃你去找其它人的麻烦。

【这一段是偏刑事案件反审讯的经验，传唤远没有这么严重，只是为了阐述任何情况下都不能配合的原因，以供参考】出于利害关系考量，你（和家人）的话语永远不可能用于证明你的清白（或许你的仇人的话语有可能帮助证明你的清白），永远只会被挑出对你不利的只言片语证明你有罪，因此全世界任何一个律师都会鼓励你在警察面前保持沉默，在中国这种没有“第五修正案”、动辄诱供逼供的国家则是尽可能少说，免得对方给扣上一个“态度恶劣”的罪名。警察不会因为“态度好”“配合”获得更多绩效而对你网开一面，或者在笔录上为你美言，也不会在乎是否真正抓到了所谓违法的人，在程序能被上级接受的情况下把越多的人判得越重，警察个人的工作才越成功，才能更快升官发财。在中国有“态度恶劣”的罪名，应对这一问题，只要别让对方抓到把柄证明你“知道但是不说”即可。面对刑事案件审讯的经验——“在警察面前保持沉默的确看起来可疑，但是让一个只跟你相处几个小时就再也不见的警察【感觉】你【可疑】，好过没扛住压力承认之后让相处几年的狱警【知道】你【有罪】”，传唤虽然远没有这样的刑事案件严重，但道理是一样的，多说、认罪永远无益。我的一位朋友曾经组织人手帮受迫害者联系记者而遭遇抓捕，他的同伴因为仗义想把责任都揽到自己头上，但最终承认的证据让一伙人都遭到重判。境外的同道也要小心地隐藏证据（线索），否则政治警察如果抓不到你，便会让联系密切的境内同道承担你的惩罚。
看一下法治国家的公民如何回复警察，这不是妨碍公务，而是行使权利：https://youtu.be/watch?v=d-7o9xYp7eE https://youtu.be/watch?v=YWUx3-b0F_Y https://youtu.be/watch?v=QKtMLhN_zeE
看一下警察国家是如何打造的：
https://web.archive.org/web/20220204152705/https://www.zhihu.com/question/68654101/answer/904276417

不管警察多么言之凿凿，不要承认任何的证据（线索）。技术侦查的人手比例低，一般不会做讯问这种耗时且没什么门槛的工作。除非是专案组个例，负责传唤的警察自己不做技术侦查工作，甚至都不是当地的同事做的，因此他们自己也不知道证据怎么来的、是否靠谱。有些网友向我反馈，警察展示的帐号的确不是自己的，但还是逼他承认。甚至有遇到多个案例警察拿着我的帐号截图逼我的订阅者承认这是

他的帐号，言之凿凿地说绑定他的手机号或邮箱（事实上我没有盗用过任何人的手机号或邮箱），目前来看可能只是想碰运气随便诈一个人交差。如果一时迫于压力承认了，可能就被当成我然后落网判二十年了。

虽然说相当大比例的人承认了帐号是自己的，并签了保证书，事情也就结了。但如果事后缺业绩了或者改变主意，就可能再抓回去而且没有否认的余地。有个别情节严重的网友承认并签保证书回家之后，不久公安改变主意又将其拘留。
一位对付传唤经验丰富的中国律师告诉我，在跟警察谈话期间，关于别人的信息一律表示不知道，关于自己的信息一律表示忘了，不重要的可以说一点，密码一口咬定一个错误的（如果遭到突击搜查）。不像在微信上，我们有一定的匿名优势，更要利用好对方取证困难、对自己的证据没有信心这一点。除了参考我的“业余建议”，建议也提前与好本地的律师和人权律师熟悉和咨询（本地的就不要提前咨询了）。假如发生闪失，在那一天到来的时候，充分了解和准备过的你会更从容。

一定要对与警察的电话录音（设置自动录音或每次打电话都对手机录像），在警局以外的地方一定录像或者视频电话并要求对警官证拍照并备份给可信的人，以对自己有更好的保护，如果日后申请政治庇护可以用来作为证据补充自己的陈述（仅传唤一般不满足政治庇护的条件，具体请咨询目标国家的移民律师）。在派出所、公安局里录音拍照有一定风险，量力而行。尽管没有任何法律依据，但是政治警察期望传唤被保密，尤其不希望看到证据流出，如果想要正面对抗则要巧妙，可以保留到出国后再公布。

（结语）
对于缺乏经验、不了解公安的侦查手段的新人来说，短期内Opsec是一项持续投入但看不到效果的工作。把自己想象成一条大鱼，虽然一生吃过几万条的小鱼，只需一次吃到鱼钩便无法活命。而在吃到鱼钩之前，不会认识到数万次进食每次都仔细辨别陷阱有多重要，吃到鱼钩之后也再没有机会再使用这样的经验。但我们终要小心地成长，保护好自己和同道宝贵的生命，终要长成巨鲸，卷起惊涛骇浪掀翻小池塘。

长期以来，人们出于恐惧不敢分享自己的喝茶经历，亦没有系统化的统计和分析，导致无数的“鱼”咬过鱼钩之后经验没有积累下来，使得公安可以一直用同样的基本侦查手段不断地定位新用户，社区也一直持续受到破坏和瓦解。西方的黑客社区会认真地搜集和分析每一个抓捕案例，总结易于实施的教程，抛开他们的活动的正当性和合法性不谈，这些方法在技术上非常有效很值得学习。两年前中文反中共社区只有是一批松散、没有经验、没有训练的新人，两年过后还是没有经验的新人在重蹈覆辙。我在许多其它反中共群体中也经常发现这样的现象——只管做自己的好事但很少搜集反馈、分析和总结。有战略和计划， 方能发现光明的方向。事实证明如果积极调查，很容易发现中国政府极力隐藏的弱点。

对于有经验的、已经学会的，首要工作是用不引起恐慌的语言把6+1个要素反复强调，挨个给每个用户传达、提供帮助、教学甚至给予督促，让他们必须滴水不漏地做好这几个简单的工作。经济上有余力的个人和组织可以批发一些Google Voice帐号，进行简单核查和筛选之后分发给境内难以安全购买Google Voice的网友。沙特记者卡舒吉生前曾经邮寄匿名的外国SIM卡给沙特异议人士，帮助他们匿名注册帐号，让沙特政府如临大敌，将其在沙特驻土耳其大使馆内肢解，我们要做的是类似的事情。

帮大批20秒就能被定位的人提升到专人投入几百个小时调查都抓不到的水准，只要照做，便可让喝茶的人数减少98%以上，或者让网警技术侦查在完成同样指标的情况下把工作量提升几百倍。

视频案例学习：
我在中国时的隔三差五遭遇的幸福生活 https://www.youtube.com/watch?v=X8dElaDgUYg
P2P受害者进京维权 半夜警察踹门查房传唤 https://www.youtube.com/watch?v=NIXriRgH7Cw

下面我们虚构一个人物，习近平（不影射现实中的任何人物，如姓名、身份证号、外号有雷同纯属巧合）
测试题
1 推特/Telegram要求习近平使用手机号验证，习近平人在中国，应该使用 CDE
A 自己的中国+86手机号
B 用自己的手机插香港/英国/韩国等外国SIM卡
C 找不在中国的朋友让他用外国SIM卡
D Google Voice
E sms-activate.org等平台的虚拟手机号
【解析】B选项中，多数人不仅SIM卡是实名的，插了SIM卡的手机的IMEI序列号也会随SIM卡实名，因此在日常使用的手机上再插匿名的外国SIM卡，这张SIM卡和上面的手机号也会随之实名。在中国所有外国SIM卡都会“借用”中国三大运营商的基站收取短信，完全受监控。除非现金购买手机和SIM卡，插匿名SIM卡接一条验证短信就手机和SIM卡都扔掉，否则不可能实名。

2 推特/Telegram要求习近平验证邮箱，应该用 E
A 个人用的网易/新浪/QQ邮箱
B Outlook、iCloud邮箱
C 工作邮箱
D 网购用的Gmail邮箱
E 键政专门注册的Protonmail / Tutanota邮箱

3 应该用什么输入法 DEF
A 百度
B 搜狗
C 讯飞
D 微软/苹果输入法
E Rime（小狼毫/中州韵/鼠鬚管/同文）输入法
F 谷歌 Gboard

4 应该在什么操作系统中使用 CDF
A 华为/小米/Vivo/Oppo/一加
B 登录了中国/香港/澳门区icloud或app store的苹果手机
C 登录了美洲/日本/台湾/欧洲/大洋洲帐号的苹果手机
D Google Pixel、索尼手机
E 中国销售的Windows系统电脑
F 给电脑安装非中国区的官方Windows或Windows10Ame

5 可信的应用市场有哪些 DEFG，重磅推荐F和G
A 华为 App Gallery等
B 豌豆荚等

C ApkPure
D 非中国区苹果 App Store
E 谷歌 Play Store
F F-Droid
G Aurora Store（安卓）

6.下面哪三个是推特、Telegram、谷歌的官网 ACE
A twitter.com
B twitter.net
C telegram.org
D telegram.com
E google.com
F gogle.co

7 微信ID为Winnie0615的习近平想匿名注册推特，请问下面哪个用户名和username是匿名的 F
A 习近平
B President Xi
C Jinping
D Winnie615
E 1101011953061530l9
F 佐藤一郎

8 佐藤一郎如果想保持匿名，可以做什么 EG
A 晒自拍
B 晒小学毕业证
C 晒网购记录、外卖、购物车
D 晒手上握着的包子
F 上传背书单的录音
E 转发乳包梗图
G 批评中国政府
H 截屏知乎、豆瓣、微博，然后用佐藤一郎推特帐号发布
I 晒自己写的论文《中国农村市场化研究》
J 分享与杜美霜女士的微信私聊截屏
K 6月15日晒生日蛋糕

9 北京八一中学发生抗议活动，应该如何上传视频的同时不威胁到佐藤一郎帐号的匿名性 BCD
A 直接上传到“佐藤一郎”推特帐号
B 小号投稿给其它推友
C 注册临时的Protonmail邮箱投稿给自由亚洲电台、美国之音、德国之声、大纪元等
D 用佐藤一郎身份的Telegram或Protonmail投稿给以上媒体

10 佐藤一郎与网友“楚晨”聊得特别投缘，逐渐建立信任，哪些事情不威胁匿名 ABCDILM
A 一起制作乳包梗图
B 一起制作民主文宣

C 交换禁书、禁片
D 交流反共心得
E 交换手机号、微信
F 一起打王者荣耀
G 互发裸照
H 微信、支付宝、银行转账
I 教对方Opsec
J 在6月15日告诉对方自己过生日，让对方给自己发生日祝福
K 聊工作、攀老乡
L 参与聊天室公民议题辩论
M 翻译中国人的言论

11 佐藤一郎的帐号绑定过+86手机号，若想继续匿名活动，此刻他该怎么办 D
A 继续使用
B 解绑该手机号，去电信运营商注销该手机号，并继续使用
C 解绑后更换为Google Voice虚拟手机号，并继续使用
C 解绑之后换绑Google Voice，删光所有推文，并更改用户名、ID，并继续使用
D 销号，使用Google Voice和，采用以上6+1条措施，注册新的帐号

12 圈内外号“包子”的佐藤一郎在销掉不安全的旧帐号之后，想注册新的帐号，如何取名保证新的帐号匿名 E
A “佐藤一郎新号”
B “Adam Smith（佐藤一郎转世）”
C “佐藤二郎”
D “曾经的佐藤”
E “Adam Smith”
F “我是包子”
G 第一条推文：“大家好，这是包子的新号”
H 个人简介：“曾用名佐藤一郎”

13 经网友提醒后，佐藤一郎发现自己第一条推文“大家好，这是包子的新号”就犯下了致命错误，此刻他该怎么做以便日后能继续匿名发文 D
A 网警会忘掉的，发更多推文淹没该消息，然后继续使用
B 网警没看到，立刻删掉该推文，然后继续使用
C 删掉推文之后更改用户名、昵称，然后继续使用
D 抛弃旧身份，建立全新身份

14 假如佐藤一郎是苹果手机用户，他应该如何使用 D
A App Store使用美国区苹果ID，iCloud使用中国区苹果ID
B App Store使用中国区苹果ID，iCloud使用日本区苹果ID
C App Store和iCloud都使用中国区ID
D App Store和iCloud都使用美国区ID

15 假如佐藤一郎是苹果手机用户，他想下载中国区的应用，应该 BC

A 只将App Store切换到中国区，下载完之后马上切换回去

B 放弃下载该应用

C 用另一部手机下载该应用

16 如果佐藤一郎被当地国保打电话传唤，可以 A

A 删除帐号和手机本地记录或带另一部手机去指定派出所，然后礼貌诚恳地否认掉一切指控

B 承认“错误”，签保证书

C 试图说服国保

D 承认但是拒绝销号