时代风云

国防大学战略思想论坛讲座精选（一）

徐纬地　主编

SHIDAIFENGYUN

GUOFANGDAXUEZHANLUESIXIANGLUNTAN

JIANGZUOJINGXUAN

国防大学出版社

SHIDAI FENGYUN

GUOFANGDAXUEZHANLUESIXIANGLUNTAN

JIANGZUOJINGXUAN

时代风云

国防大学战略思想论坛讲座精选（一）

徐纬地　主编

国防大学出版社

北京

图书在版编目（CIP）数据

时代风云：国防大学战略思想论坛讲座精选（一）/徐纬地主编．
—北京：国防大学出版社，2015.8
ISBN 978-7-5626-2355-7

Ⅰ.①时… Ⅱ.①徐… Ⅲ.①国际政治关系—文集
Ⅳ.①D81-53

中国版本图书馆 CIP 数据核字（2015）第 192146 号

时代风云

国防大学战略思想论坛讲座精选（一）

徐纬地　主编

出版发行：国防大学出版社
地　　址：北京市海淀区红山口甲 3 号
邮　　编：100091
电　　话：010-66772856
责任编辑：黄建国
责任校对：吴　静
装帧设计：王联众

经　　销：新华书店
印　　刷：北京毅峰迅捷印刷有限公司
开　　本：710×1000 毫米　1/16
印　　张：16.25
字　　数：218 千字
印　　数：1-3000 册
版　　次：2015 年 9 月第 1 版第 1 次印刷
定　　价：36.00 元

目录

CONTENTS

中国人民解放军国防大学战略思想论坛

Strategic Forum NDU PLA

战略思想论坛

12-13

总第93期

主题 中国网络安全的基本态势与问题

杜跃进简介

主讲：杜跃进

时间：2012年11月8日（周四）下午：14:30

地点：教学楼二讲堂

国家网络信息安全技术研究所所长、研究员
国家计算机网络应急技术处理协调中心副总工程师

当前世界网络安全斗争基本态势如何？斗争前沿何在？主要焦点有哪些？

与世界网络大国相比，中国网络实力、网络发展目前处在什么地位？

各国在网络空间的地位主要从哪些关键指标来判断？

中国在网络安全上面临哪些主要威胁和挑战？中国网络安全最大的薄弱环节在哪里？

大家知道，美军所谓的陆、海、空、天、网五大领域，也有人将其中的网络空间称为第五空间。其实，业内人士包括我在内都认可的一个观点是，网络空间不是第五空间，它是第二维空间，也就是说为什么美军陆、海、空、天、网，还要优先发展网？因为它和所有的陆、海、空、天都是融合在一起的，它并不是独立存在的一个东西。所以，通过对网络空间的攻击或者对网络空间的威胁，其实可以直接威胁到其他四个领域。

应对网络空间安全威胁这件事情不光我们中国没经验，世界各国都没有经验。原因就是这个东西确实是太新了。它对我们的影响太复杂了。我一直是做应急的，我可以说是 CNCERT（国家计算机网络应急技术处理协调中心）的创始人之一，在应急领域里面最关键一个问题是要足够快，还有一个关键就是决策人的信息应该在足够短的时间里掌握得最全，你才可以做出准确的决策，然后才可以影响下面。但是当前，国家的决策机构，或者说国家领导人知道的信息量和时间可能还赶不上老百姓，因为信息世界把这个顺序全打乱了。因此，在这种情况下，决策人怎么决策？这些问题全是新问题。

我分四部分来介绍一下我的看法，第一部分是安全表象，就是我们现在能看见的安全；第二部分是我们看不见的那部分；第三部分是我们面临的挑战或者说我国的安全基本态势是什么；第四部分是技术上的对策，或者说制约我们应对这些挑战，还有哪些其他的问题。

一、我国网络安全总体形势

2005 年，我国建立了网络安全监测平台，这个平台有什么作用呢？用一句话来说，通过这个平台，我们中国知道了很多东西，这些东西现在是各个官方所引用的数据，这些数据都是公开的，它能够描述中国安全到底是什么样的。

木马和僵尸网络。木马不用解释了，我们早就知道木马是能够窃密

的。在这之前都说有多少多少漏洞，漏洞是什么？漏洞是说存在可能性。从2003年开始，我们开始做木马活动的监测，这是什么？是说我发现多少溜门撬锁的行为，而不是说多少锁有问题。

最早这件事情开始于2003年。当时，我们接到公安部的通报，我国某高端研究所机器被人家植入了RA病毒，RA本身并不是一个木马，但是它可以被当成木马，它跟木马一模一样，只是说在远程教育和一些网络游戏里也用到它。当时我想这个我可以实时监测，在骨干网上看看它的活动情况是什么。结果发现这个量很大，当然，对于RA来说，我区分不出来哪个正常哪个不正常，之后我们就开始把更多木马的特征提取出来，在我们的环境下监测。

其中2007年是一个拐点，以前不是说就这么少，而是说我们的技术还不是特别成熟，对问题看不大清楚。这期间我们一直在完善。2007年是个拐点，从2007年我们看到的被木马控制的节点，中国大陆的，而且都是被境外控制的接近一百万个IP地址。

现在很多国家说中国黑客威胁论。如果我们追查回去，这个说法2007年就开始了。而中国也正是从2007的开始注意到网络窃密变得非常厉害的。都是在2007年。对于这个现象，我在最近的国际会议上说，谈中国黑客威胁论，我给你们看看我们2007年看到的是什么，看到全世界大量的到中国窃密的行为，这个行为和你们在国外看到的是一样的，它并不是说从2007年开始中国的黑客去攻击其他国家，而是从2007年开始整个世界的互联网安全进入到一个新的阶段。

僵尸网络。2004年底有一个事情让我怀疑可能是这样的案例，我就去介入调查。2004年底走访国信办的时候，我跟他们说现在有一个很厉害的东西，这东西的威胁远远不同于以前的东西，可以大规模地窃密，用它发起网络大规模攻击的话，比原来的危害要大很多很多倍。他们说这个很重要，过了元旦来讲吧。过了元旦，我就想我得给它起个名字，没名字也不行，所以起了个名字就叫僵尸网络。为什么叫僵尸网络？是

黑客可以通过一套控制体系来指挥全世界大量的计算机，按照他的意志来行动。

现在小孩都知道 Zombie 就是僵尸，植物大战僵尸。因为这个词的英文词是已经有的，你也知道说的是机器人网络。但是，被控制的那些节点叫 Zombie，我还专门去查 Zombie 是个什么东西，现在都知道 Zombie 是僵尸。

僵尸网络到现在依然是全世界最受关注的安全威胁之一。在这件事情之后，国内出了很多的博士论文，都是研究僵尸网络的。为什么它这么受重视？因为攻击者用这种方式，可以把自己的能力扩大无穷倍。现实的案例是一个荷兰黑客控制了全世界超过 150 万台计算机，他可以用这 150 万台计算机干任何事情，刷广告、发垃圾邮件、做拒绝服务攻击、做蠕虫攻击、窃密，全都可以，你能想到的任何事情都可以干，同时他的隐蔽性非常好，你基本上找不到他。

到 2010 年之后，我们把它和木马合在一起来说了。2007 年，我们看到僵尸网络控制的 IP 是 362 万，木马是 99 万，加在一起将近 460 万。僵尸网络其实跟木马一样，僵尸网络里面有一个基本的特点，就是被控制的节点是去找上游，而不像传统木马是上游来找你。假设我们这里有一个人被人家买通了，传统的方式是他来找你要情报。你的门卫一看，你又不对外，就拦住了。僵尸网络是你交出去的。你说我去小卖部，我去天安门广场，门卫也没什么好说的。但你出去是去交情报。

到 2011 年是多少呢？890 万个 IP 被境外控制。因为要反驳中国黑客威胁论，就得拿出数据来证明。我们可以看到中国这些被控制的机器，谁在控制它？或者说谁的 IP 在控制它？主要来自日本（22.8%）、美国（20.4%）、韩国（7.1%），在 2011 年排名是这样的顺序。其中，被来自美国的 IP 控制的中国大陆计算机节点数达 885 万个。当然，我们从来没有说是美国人控制了这 800 多万个节点，而是说被来自美国的 IP 控制了这么多。而美国的很多媒体就不负责任，只要 IP 在哪儿就说是哪儿，其

实黑客是很容易跳过去的。我们可以分析谁控制了我们，他们的 IP 来自哪些国家，甚至每个月的表现是什么。这样，你可以看到有些区域对中国的攻击开始越来越活跃，有些区域对中国的攻击越来越降低；我们也可以看到我们中国被控制的这些计算机分布在哪一个运营商，分布在哪一个省。

2001 年 5 月份发生了一个事情，就是当年的中美黑客大战。2001 年 4 月 1 日，在南海上空，发生中美撞机事件，在事件之后，中国有五一黄金周。黄金周之前，有很多黑客论坛就在鼓动说要对美国发起网络攻击，当时我们也做了很多事情来阻止攻击的发生。美国人在做什么呢？他们发警报说中国要攻击我们了，然后发生了双方的相互攻击。双方的攻击很密集，确实存在因为这件事情引起的黑客大战，但绝对不是我们单向攻他们，是双方在互攻。而且中国黑客攻他们的大多数是商业网站，美国黑客攻我们的是政府网站。这些事实都可以拿在国际上去和别人说，看看到底谁是更负责任的，谁是不负责任的。

在那之后我们开始逐步研发专门的技术手段，来对网站被篡改或者网页攻击的情况进行监测。到现在为止，中国的政府网站依然是比商业网站要脆弱，为什么这么说呢？比如说所有的网站里面，不到 5% 是政府网站，可是我们每次发现被篡改的网站里面，政府网站的比例总是超过 5%，通过这个就可以说政府网站问题依然比较多。

除了被篡改之外，我们在 2011 年还发现有一万多个网站是被人家秘密控制的，其中排在第一位的来自美国，有 3000 多个来自美国的 IP 控制了我们的网站。

网站安全还有一类，就是非常重要的、很特殊的网站。网站是用户访问网络的门户，既然是门户，攻击者也可以想象到利用门户来做攻击的桥梁，这当然是效果很好了。

另外，我们还承担了咱们国家通信行业网络安全的风险评估和安全检查工作。中国是把通信行业、通信网络划分成各种各样的网络单元，

它由这么多网络单元组成。然后网络单元会给它定级，按照等级保护的要求，如果是两级以上的，要求每两年要做一次风险评估、符合性评测和安全检查，三级以上的每年做一次。

我们可以每年给政府很多的数据，包括总的统计，从统计结果来看挺好的，我们的防护达标率逐年提高。我们也能够对哪些单元存在的风险比较高给出意见，我们还能够为这些跟运营商相关的漏洞这类东西给出统计的结果，我们还可以对某种趋势给出预测，或者说给出说明，等等。所以，看起来我们对这个脆弱性和风险也知道很多信息。

我们还在关注移动互联网安全。我们对移动互联网也做了一些事情，比如说2011年，我们在网络上面监测发现，被某种手机病毒所感染的手机数目达700多万个，但是，我们从检测的角度来说，国内十几个软件商店里面有很多软件本身就是有问题的，有一些直接就是病毒，就在软件商店里下载，有一些是比较隐性的，查不出来，但是经过我们仔细分析查出来其实里面有很多问题。大概50%的用户在不知道的情况下就去主动访问网络，或者是发送短信这样的行为，造成费用流失。如果是从这些有害软件的下载量来看的话，超过两千万。

我们在2006年底还做了一个地下产业链的调查。按最保守估计，当时一年中国大陆地下产业链的产值是2.38亿元，它在产生2.38亿元的地下产业链的同时，给我们造成的损失是76亿元，这已经是当时最保守的估计了。其实，真正的地下产业链比这个要大很多倍，我们这里面还没有算上网络游戏。

二、网络安全威胁的发展

我把网络安全威胁分成四个阶段，刚才其实已经点到过一些。从2001年的蠕虫产品开始，到2004年是第一个阶段，我把它叫作蠕虫时代。这一阶段的攻击者没有什么动机，用金庸笔下的一个人物来形容，损人不利己，白开心。

2004 年下半年到 2007 年是第二个阶段，就是 2004 年下半年之后，一夜之间好像没有蠕虫了。是蠕虫没有了吗？不是，都变成小规模的蠕虫了，为什么呢？它变成地下产业链的一个环节了。典型的特点是 2004 年之后，各种各样的偷 QQ 号，拒绝服务攻击、敲诈等，都是这时候开始的，还有发垃圾邮件，做恶意广告，刷广告挣钱都是这时候开始的。这时候叫趋利时代，在国外叫计算机犯罪时代。

2007 年底到 2010 年，进入第三阶段。很明显的一个特点是大量窃密事件的发生。现在并不是说这个时代过去，其他的就没有了，除了第一种蠕虫换了样子之外，现在那些都混在一起，最大量的依然是趋利的，就是各种各样获利的攻击，但是为什么还要划分它们呢？在某一个时代开始，出现了一类成气候的需要重点关注的典型的案例。

2010 年到现在，已经进入到一个全新的阶段。网络战开始了。这个全新阶段的特点是什么？首先要看看我们自己发生什么变化了，这个变化就是咱们国家“十二五”规划里面的一个词叫新一代信息技术，新一代信息技术是什么？没有做很清晰的描述，但是，对于新一代信息技术本身的特点，基本上是有共识的，外面通常的共识是四个。我们自己内部的研究，觉得至少是七个，包括融合、泛在、智能、不对称、跨带、移动、隐匿等，只是我们今天要从安全的角度来看这一点。

融合意味着什么？我们现在终端融合了，我们兜里拿出来一个东西，它是照相机、是电话、是 MP 播放器、是录像机、是 GPS 定位器等，什么都是。终端在融合，网络也在融合，我们通过互联网可以看新闻媒体，甚至是到电力网络等，现在都在融合，后面的服务也在融合。这种融合意味着攻击的人可以有更多的途径来跨网攻击。

过去我们知道有一种木马是专门记录大家的键盘敲击的，尤其是偷密码，你的密码是 ABCD，你一敲它就全记下来了。后来就有人研制软键盘，我的密码不是用敲进去的，是用鼠标点的，这时候截获的是四下鼠标点击，一点意义都没有，好像挺安全的。其实黑客用非常简单的方法

就可以绕过去，你每点一下鼠标，我做一下截屏，你的鼠标当时在什么位置不就全出来了嘛，直接就送走。为什么现在可以做呢？宽带送这几张截屏一点问题都没有。所以，这都是新的特点带来的新问题。

再讲一下智能和不对称。智能就意味着机会，我们现在什么东西都智能，恨不得家里的电冰箱、马桶都智能，怎么智能的？里面有程序。网络攻击分为两大体系，一类体系是基于破密，一类体系是基于漏洞。其中基于漏洞是什么？其实就是对程序的攻击，你这个程序员经常会有想不到的地方，因为程序是你的逻辑思维变成程序，你有没想到的地方就可以被攻击者利用。所以，我经常说智能对攻击者来说就意味着机会，攻击者有可能攻到那儿。我们现在的很多电表是智能电表，直接挂在网上的，公共的 IP 地址都可以访问到，有人就演示，直接可以看到里面的东西，通过一个电表就可以分析出来这是一个工厂还是一个居民区。有些情况下，还可以直接控制这个电表，这都是智能带来的问题。

不对称。不对称是一个国家的问题，尤其是像美国这样的。我们都知道美国对我们的不对称优势，通常是说我们的操作系统、核心芯片、数据库是依赖它的。实际上它对我们的不对称资源远远大于那个，在新一代信息技术下，这种不对称变得更加明显。首先，最重要的是整个基础设施的运行就是不对称的，它掌握着全世界的基础设施运行的撒手锏的能力。其次，全世界的数据都在往它那里流，从阿富汗到非洲到欧洲，数据全往它那里流。这种数据是极其珍贵的战略资源。通过这些数据，它可以分析某个国家，比这个国家自己都了解自己本身。而这种新一代技术会让这种不对称加剧，这些都是新一代信息技术带来的特点。

与此同时，对手其实也在发生变化，我说我们原来做安全的人有一个非常大的误区，就是以为安全是杀病毒。从来没有想过现在的安全不是这样的。假如某一个人想要对另一个人干某一件坏事，我们的传统思路只是说他这个坏事是怎么干的，有人往我家里扔个砖头我拿出去就行了，有人往家里放一个窃听器我扫出去就行了，就没有想过这个窃听器

是什么时候进来的，是不是把你家的秘密情报已经偷走了，就没有想过除了这个窃听器之外是不是还有别的窃听器，都不想。所以这是一个很大的错误。我们一直说，你要做安全威胁的分析，就要知道你的对手是谁。2010 年之后，很明显，国家之间的对抗成为一个现实了。在 2011 年的国际会议上，卡巴斯基做完报告之后，有人问他，你对安全的预测是什么？他说的是这句话："政府攻击和反政府攻击。"这与过去最大的区别是什么？其实是动机，因为动机不同，所以会展现出来和过去完全不一样的攻击。有些目标你从来就不会想象到。那些"白开心"，他可能碰都没有机会碰到过，他也没有能力攻到这儿来。犯罪分子会觉得这个东西一点价值都没有。所以，动机不同就会导致选择的目标和方法会非常不一样。

其次，如果背后是政府发起的攻击，政府手里所拥有的资源，完全不是任何黑客组织——不管他们技术多强——所能够拥有的。我随便举一个例子，假如我是美国政府，我拥有的资源是什么？随便点一个，我拥有全世界域名服务器的 A 根的运行权，我在 A 根里面只要动动手脚，很快隔一段时间，比如说它针对中国的话，全世界没有任何人能访问到中国的互联网，中国人自己也访问不了，全世界其他国家也访问不了。如果是政府来干的话，它有这样的资源。当然，它要掩盖，说这是技术失误。连导弹打到我们的大使馆都能说不是故意的，这种事情更可以说了。

如果是日本，它要做这种攻击，它可以干什么？它控制不了那个根，它也有它的方法。网络是基于互相信任的关系才能够运转起来的，其中一个例子是路由。为什么你在互联网里面随便找一个 IP，它能够通过去？是有人指路，这个路是怎么形成的？网络里面有很多单元，它们是互相信任，信任之后互相广播这个信息的。一般的黑客不太有机会来攻击到这个部分，不是完全没有机会，是很难。如果是政府在里面，那就容易了，你原来信任的一个运行伙伴在里面，他可能出于政府的指令，做一

条错误的信息加进去，可以让任何一个网站不能访问，可以让任何一个网站跑到别的地方去，可以让某一些流量在你这里绕一圈再回去。2010年，美国人炒作说中国电信把美国的很多官方数据拐到中国流了一圈监视完再流回去，当然这是瞎扯了。但技术上行不行？可以，就是靠路由的攻击。这种事情黑客干不了。“震网”病毒已经有人说黑客干不了，因为谁见过西门子的工业控制系统？谁知道那里的PRC怎么编程？没有人。反政府组织也做不了。但如果是政府在这个里面，会跟过去很不一样。这已经是一个新的阶段了。

这种阶段如果给它起一个名字，可以叫非常有目标攻击。非常有目标攻击和过去的损人不利己，或者说和过去的一般计算机犯罪分子有明显区别，一般的计算机犯罪分子就是获利，偷QQ号、偷游戏装备等，没有特定目标。到了窃密的时候，已经是一定程度上有目标了，是要偷军事情报，还是要偷科技情报，或者是要偷某一个项目的情报，已经有一定目标了。但是现在就盯着你，可能你在全世界看到的所有攻击程序里面，从来没有见过这种只在这一个人这里发生过，他是完全针对这个人构造的。你可能会看到一个攻击事件，从骗局设计开始，完全是针对这个人的，他今天去哪儿了，明天去哪儿了，他在公司里是什么位置，他目前正在干什么事情，他大概掌握什么情报，他周围的朋友是什么，有什么社会关系等，最后才在恰当的时候用恰当的方式，控制这个人的邮箱服务器。

比如说真实案例，刚才说到的“震网”病毒。最新的研究结果，人们认为2012年才被发现的“火焰”病毒其实是给“震网”病毒打前站的。“火焰”病毒不像我们过去的病毒。过去的蠕虫一撒撒那么多。但“火焰”病毒定向性很好，你看它最后在全世界感染的非常有目标性。

过去病毒的特点是什么？过去的病毒是它也不知道会破坏谁，CIC的作者破坏的计算机可能包括他亲戚朋友的，怎么就“震网”病毒只破坏一两个呢？这就被西方人叫网络导弹，也有人把它叫智能新攻击武器。

我们现在都在做内外网隔离，或者说单向导入，如果真的能够做到内外网隔离，或者真能做到纯粹的单向导入的话，能解决你的这条通路不通，攻击者没有办法建立一条通路直接控制到你的内部网络里面去，但是解决不了什么问题呢？解决不了“震网”能力，它不需要通，它带进去就够了，这个病毒程序是很聪明的，它对你了如指掌，只要进去就能实现破坏的能力，这就是新一代的攻击。

在这之后，其实 APT（高级持续性威胁）在国外已经是越来越热了，国外的会议上讲 APT 的案例，非常非常多。除了“震网”没有人说是中国人搞的，剩下的全部说是中国干的，说中国控制了 103 个国家，布置了一个间谍网络，专门偷外交人员的情报。这个研究谁做的呢？加拿大蒙科研究中心，背后的资助者是谁呢？达赖集团。某些人说中国的黑客控制了美国 F－35 研究项目里面的机器，还有人说中国的黑客入侵了美国的智能电网，等等。全部是抹黑中国的。

APT 一般来说大家认为它普遍使用社会工程学攻击，社会工程学攻击也是无法用我刚才说到的那些监测系统监测到的。社会工程学攻击相当于是骗术了，我给你发邮件，我给你编故事，高级的攻击是我根据你当时的情况来编故事。如果有人突然跟你说你中奖了，现在可能没有人相信了。现在他们是怎么做的呢？坏人趁小孩在学校上课，手机打不通的时候，说你们家小孩出事了，或者说你们家小孩被绑架了。你这时候电话打不通，所以这就稍微高级一点了。在网络里面的社会工程学攻击还有很多非常高明的例子，比社会上的骗子高明多了。

另外，这些 APT 很多都是掌握所谓的 0day 漏洞，就是从来不为外人所知道的漏洞，以前大家都说窃密，说中国黑客威胁论就是在说窃密。但是到了今天已经不光是这个案例了。

这么多案例，为什么没有针对中国的？中国没有吸引力吗？绝对不是，中国现在太有吸引力了，有无数的人会对攻击中国感兴趣。但是，我们没有能够从里面挖掘出来针对中国的高级攻击。所以，我们看上去

知道很多攻击，可是我们根本就不知道对我们的高级持续性威胁。显然，这是我们的发现能力不足以应对现在这一阶段的安全威胁了。

到今天，尤其是“火焰”病毒出来以后，全世界都在讲 stuxnet（“震网”）、Flame（“火焰”），全世界都在讲 APT，非常非常热，只是不再讲过去中国那些了。从这里面我们学到了什么？我们学到了一个很大的事情是这几个事情都是潜藏好多年之后才被发现，那我们完全有理由相信此时此刻一定还有很多东西潜藏着，我们现在没有发现。我们同时就可以想到，将来某一天发现的时候，可能会发现这些事件不都是针对伊朗的，不都是针对中东国家的，可能是针对我们中国的，可是等到你发现的时候已经晚了。

什么是网络战？他在前期到处渗透的时候算不算网络战已经开始了？可能还不算，他在按下按钮的时候，他的手早就掐在你的咽喉位置了，他说好，我要发动网络战，你已经完全没有任何的反抗之力了。那这个怎么算？所以，我们完全有理由怀疑现在一定还有哪些东西我们不知道的，是人家有意识地在不断的积蓄力量，不断地埋伏在那里，等到有一天我们已经没有还手之力的时候再用。这才是《孙子兵法》里面的不战而屈人之兵，不用动用真的军队，直接就把你的运输系统瘫痪了，或者直接把你的金融系统瘫痪了，或者把你的能源系统瘫痪了。未来网络战可能会冲在最前面，但是可能会有完全不同的形态，会起到非常不一样的效果。

中国说的最多的自主可控，自主可控不等于安全。我的意思不是说不要搞自主可控，而是意在点出我们国内另外一个非常大的隐患，就是很多人以为这个东西是我自己做的就安全了，别人做的，他可能做过手脚，我不知道，当然有可能不安全。问题是我们自己做得太差的话，不是一样的吗？现实情况就是我们自己的软件漏洞百出，一点都不夸张地说，漏洞百出。新一代信息技术和过去不一样，以前你做一个什么东西自己用，跟谁都不连着，你再差，别人也不怎么用。现在全都连在一起

的，我们做的漏洞百出的东西，往网上一挂，当天晚上全部数据被偷走，怎么偷走的？我们很多重要的系统，不管你是时间系统，都被人家秘密控制了，你自己都不知道，那不还是不安全吗？是自主了，但是其实没有变成可控，这是我们国家安全的一大隐患。

我从2007年开始就呼吁我们中国要重视安全编程，要重视软件安全。我们当时是鼓动电子工业出版社出了几本安全编程的书，后来我隔了两年出国回来，我说你们的书卖得怎么样？没人买，没有人要求你做一个安全的程序。程序员搞那个不是闲着没事吗？

另外我们再看一看我们自己的用户单位。我不久前参加国内一个非常重要的系统评审，花了好几个亿，有好多个项目。我就看它最后软件的测试部分，我看见了它的安全测试，就四条，这四条打比喻相当于什么呢？这个门有锁没有？有锁。锁不打开能不能进去？进不去。类似这样四条。我说你这个跟没有测是一样的，你这都是正向思维。好人看见门口有个门卫，他不让你进去你就不进了，坏人根本不是这样的，坏人哪会从那里进？坏人会装成好人进，坏人去看你的窗户有没有关。这是我们国家极其重要的系统所谓的安全测试，我说了这个问题之后，当时有十几个专家，其中有一个专家说我们那边已经出过事了，就是软件设计有问题，把一个最高级的警报发错省了，你们想想会出现什么样的后果吧。

不光是产品本身，我还有几个问题，就算是将来我们的操作系统、芯片、数据库全是国产的了，总得有个时间周期吧，而且这个东西是个产业的问题，我做好了产业就用吗？产业不用就形不成规模，所以它有很长的过渡期。在我们最终的理想达成之前，我们管不管安全？我们的芯片搞了多少年了，现在还是用的国外的操作系统。所以，不能说等到全部都自主可控了，并且安全了，我们安全就有了。

而且一说自主可控，我们熟悉的都是我刚才说到的操作系统、芯片，等等。但是我要说的是，我们基础设施本身在运行上面也不自主可控，