参会记录：第九届互联网安全大会（ISC 2021）

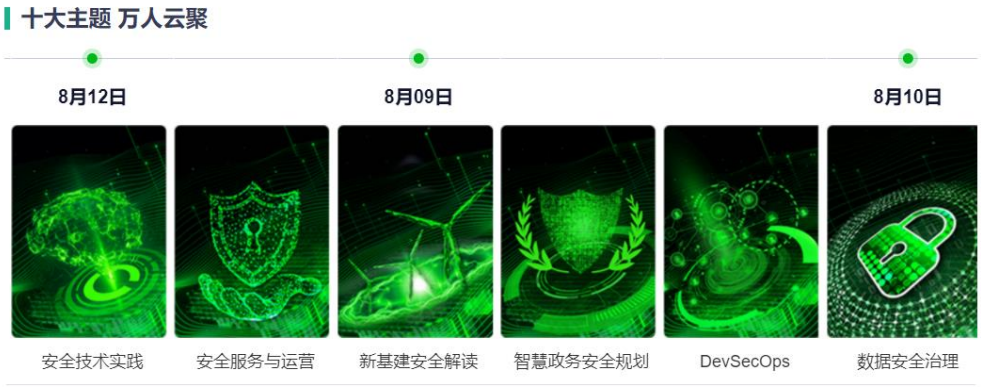
1 会议信息

会议名称：第九届互联网安全大会（ISC 2021）

会议地址：https://isc.360.com/

时间：2021.08.09 - 2021.08.12

会议围绕零信任、无边界、赛博化展开十个主题：安全技术实践、安全服务与运营、新基建安全解读、智慧政务安全规划、DevSecOps、数据安全治理、信创安全实践、物联网安全实践、安全技术分析、企业安全实践。

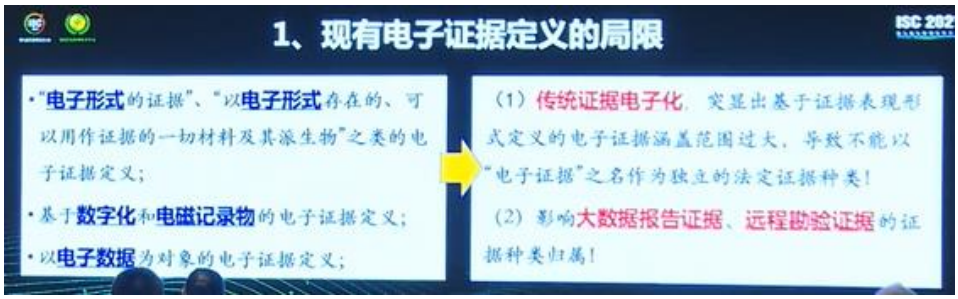


2. 一部分议题

2.1 认识电子证据的新视角

互联网并非法外之地，精准定位个人越来越容易，避免在法律的边缘左右横跳，了解一下可能会留下哪些电子证据。

（1）现有电子证据的局限



其局限首先在于电子证据的定义较为模糊，许多定义为电子证据的证据与传统证据相比覆盖范围过大。其次是很多工作没有得到法律支持，一些电子证据无法作为有效地证据。

（2）电磁波证据定义的启示

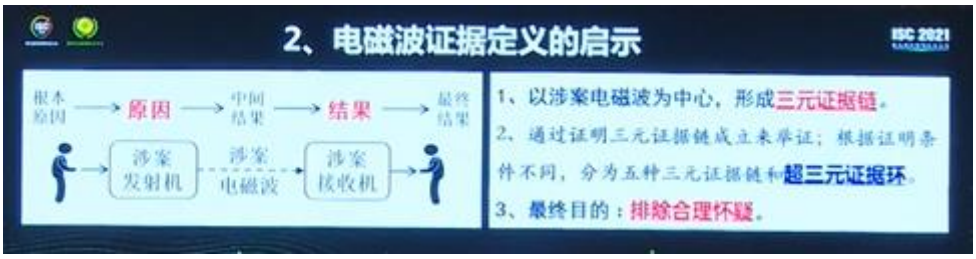
第一类：必不可少的关键作案工具：如 Wifi 钓鱼，Wifi 发送的电磁波；

第二类：与犯罪行为的实施有关的物品：如打电话进行诈骗，打电话的电磁波（此类证据通常占 99.99%）；

第三类：与犯罪行为有关的物品：如接诈骗电话的电磁波。

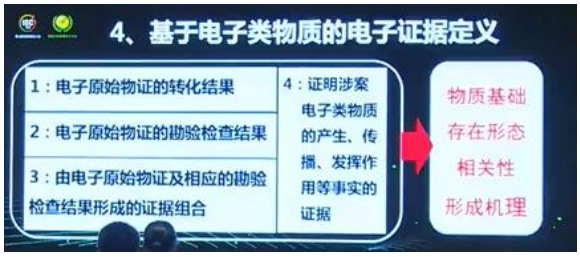
（3）如何把这样的电子类物质作为证据？

经过调查发现，这些电子类物质不是自然存在，一定需要人为操作才能产生，可以以涉案电子类物质（如电磁波）为中心，形成三元证据链。



（4）定义电磁波证据（新型电子证据）

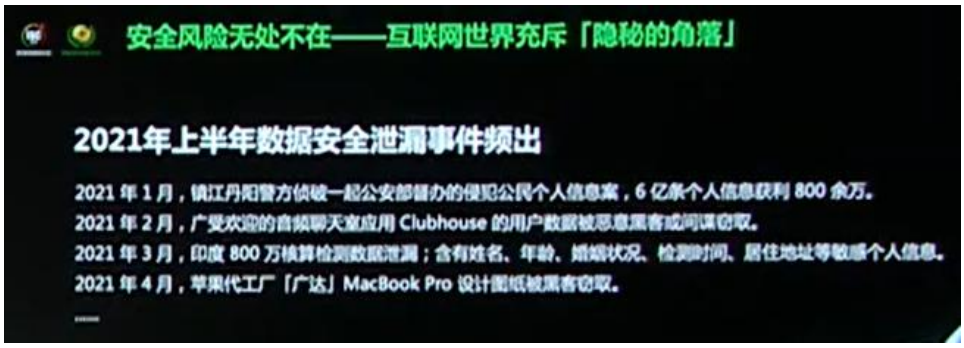
传统证据如脚印、指纹，是一种结果、最终状态，而电子证据除了包括这些状态、结果之外，还应该包括导致物质存在状况发生变化的过程。



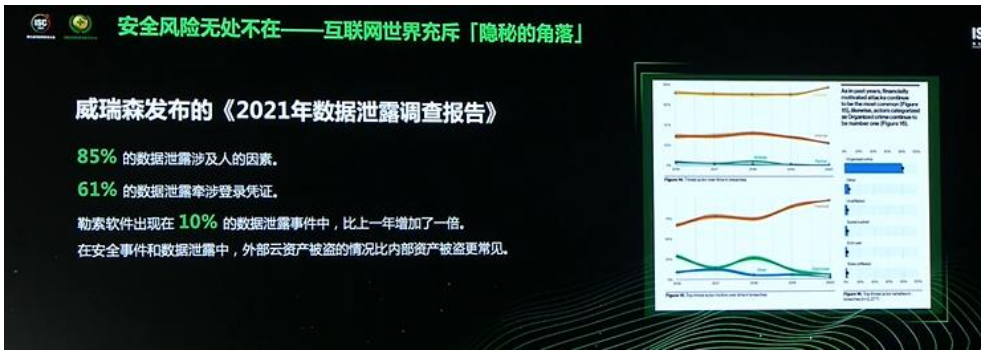
2.2 以身份为基石的零信任网络，让互联网不再有“隐秘的角落”

主要讲述“人”才是数据泄露的根源，外部防护而内部毫无防护会使攻击者一旦攻破防御外壳就能为所欲为，应当建立零信任网络。采取的措施基本听不懂。

（1）2021 上半年数据安全泄露时间频出（可作为数据泄露事件方面的素材）



（2）数据泄露的调查报告：人是数据泄露的主导者，是数据防护中最薄弱的环节



（3）防火墙物理隔离到身份基础设施的转变

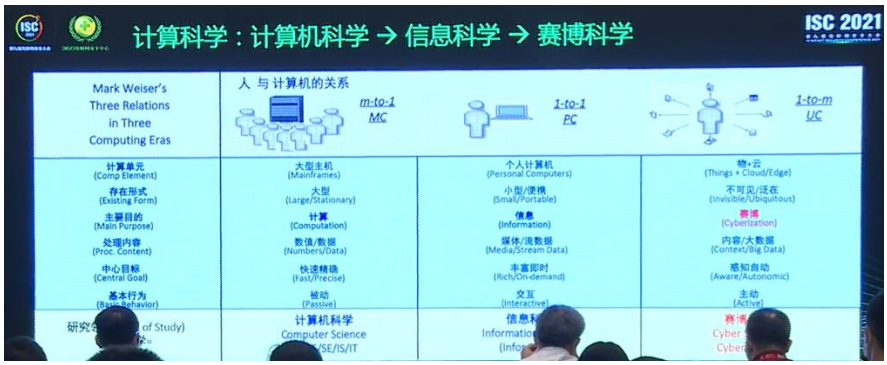
（4）零信任网络的措施

- 在用户建立信任：部署 MFA；
- 用户设备和行为可视化；
- 确保用户设备的可信度；
- 执行基于风险和自适应的访问控制；
- 身份云->身份基础设施。

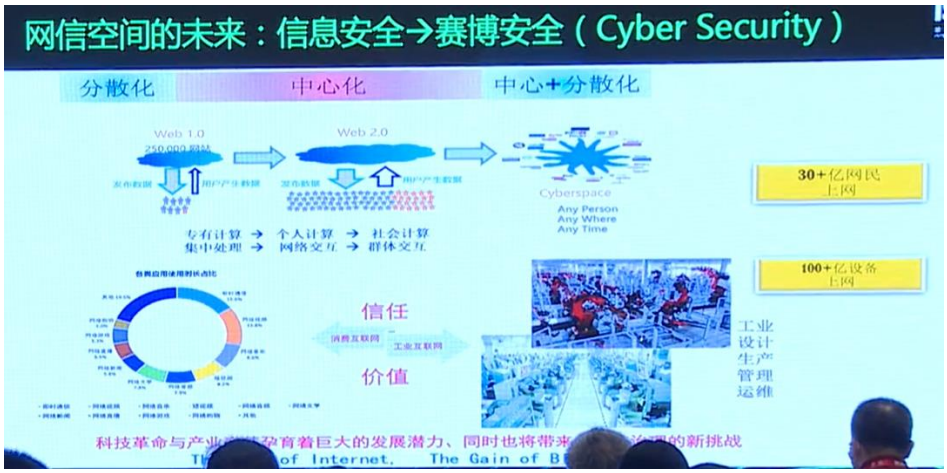
2.3 网络空间人工智能安全的挑战与应对

目前计算学科已经演化到赛博（Cyber）科学。在赛博空间中，人工智能除了面临原有的安全挑战外，还面临传感器欺骗、数据投毒的威胁，并且人工智能攻防角度也与传统攻防角度不同，如对抗攻击，使分类结果发生变化。人工智能安全的根源在于“人”，需要国家战略进行管理。伦理、道德是未来人工智能需要考虑与解决的问题。

（1）计算学科的演化：赛博科学

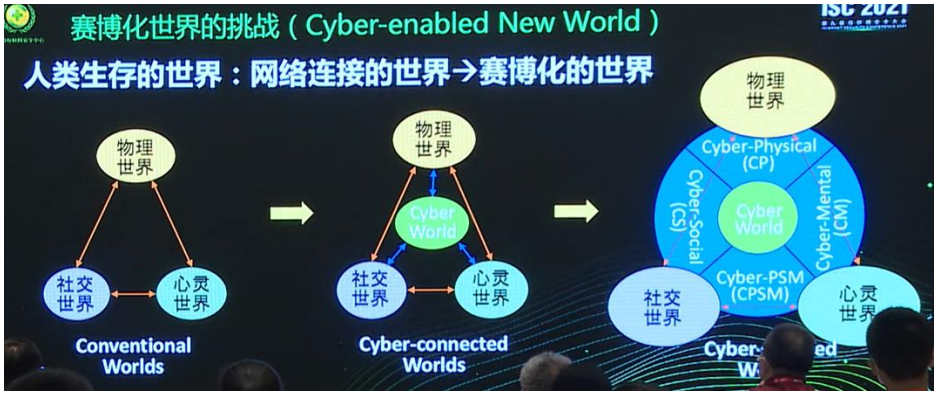


新的学生直接处于“物”+“云”的环境中，处理的是大数据。

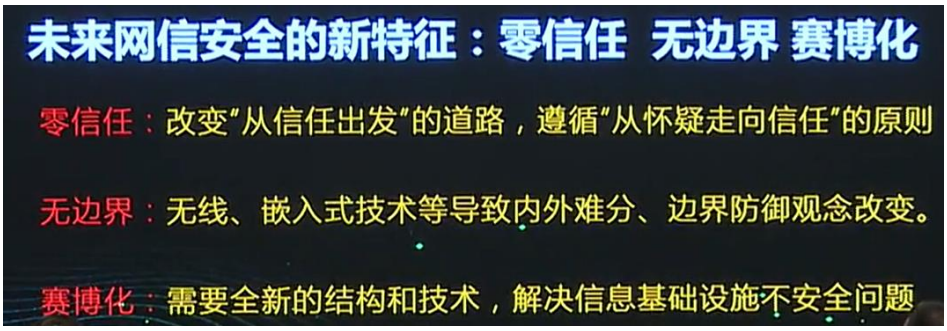


未来的探索可能与“信任与价值”紧密相连。

赛博化比网络化联系更紧密，比如远程手术、无人驾驶，由互联到互信。

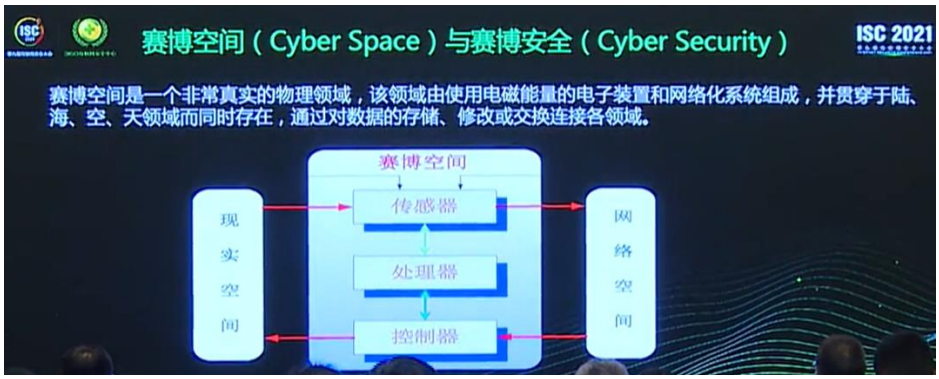


未来网信安全的新特征：零信任、无边界、赛博（Cyber）化。

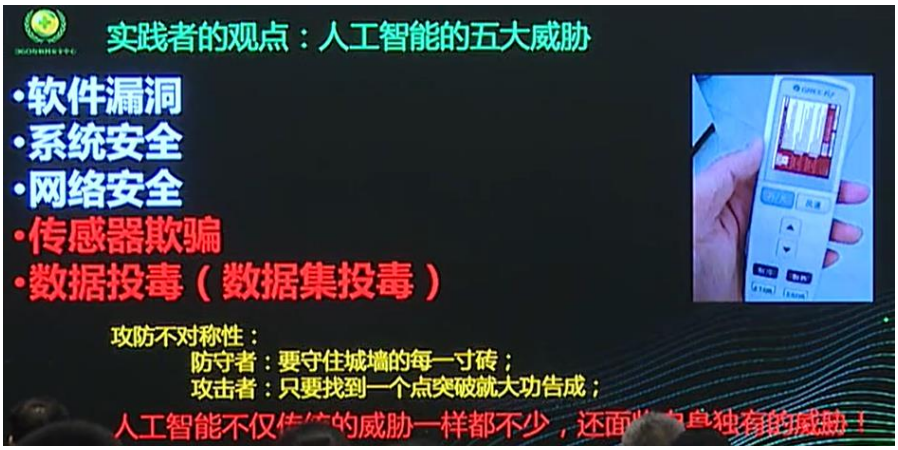


（2）人工智能的挑战

赛博空间：是非常真实的物理域。



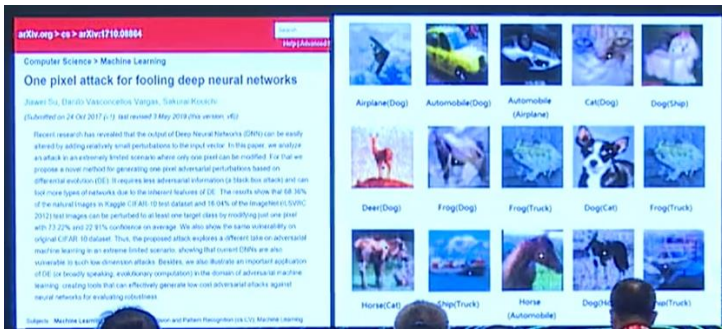
人工智能不仅存在传统的威胁，并且存在本身的威胁：传感器欺骗、数据投毒。



案例：

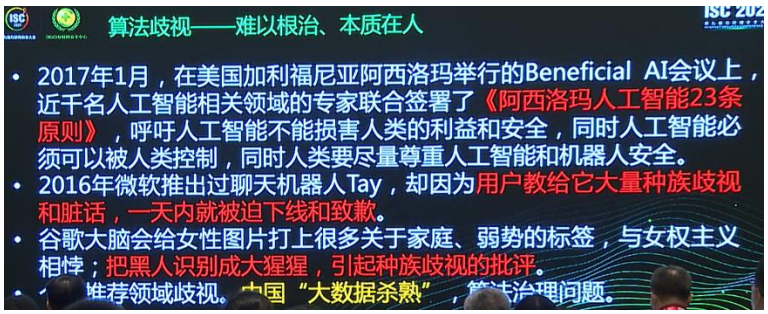
- 2017 年极客大会，虹膜识别被成功攻击；
- 加州大学伯克利分校 Down Song 教授团队研究与试验：在一个写着“STOP”的标牌上，粘贴了几块黑白胶条，人类看起来没什么，但在自动驾驶的人工智能看来，这就是一个时速 45 公里的限速牌。

- 仅改变一个像素就造成识别错误：把飞机识别成狗。



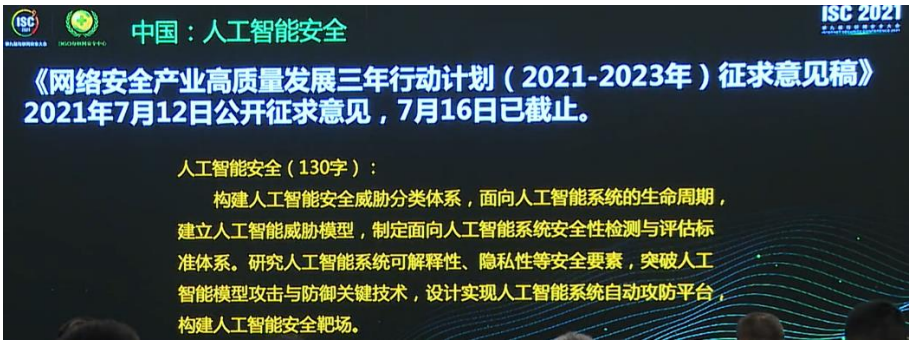
- 生成对抗，带上对抗眼镜，除了 Iphone11，手机均被解锁。

主要的问题本质在人，属于治理问题，如中国的大数据杀熟。

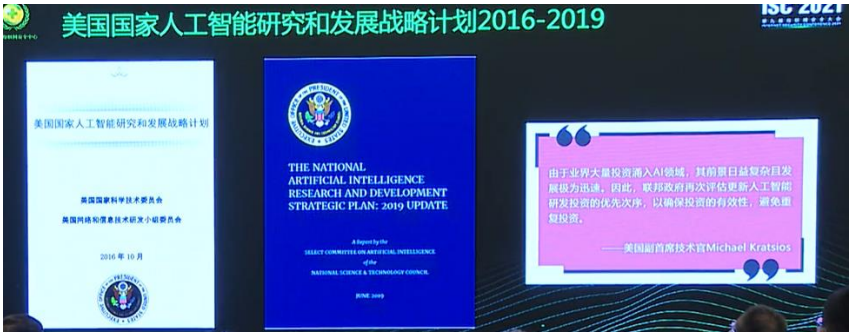


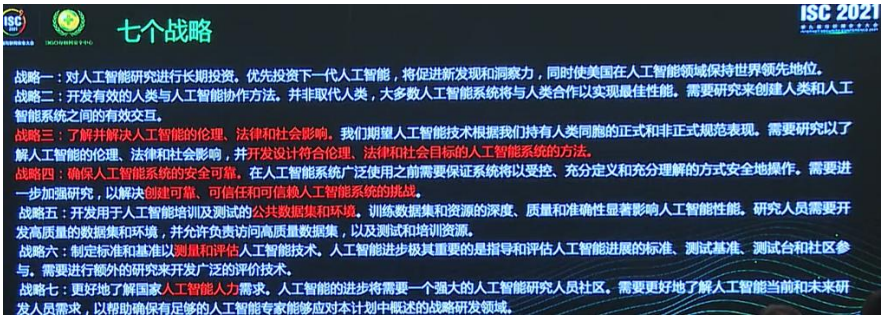
（3）网信空间人工智能安全新应对方法

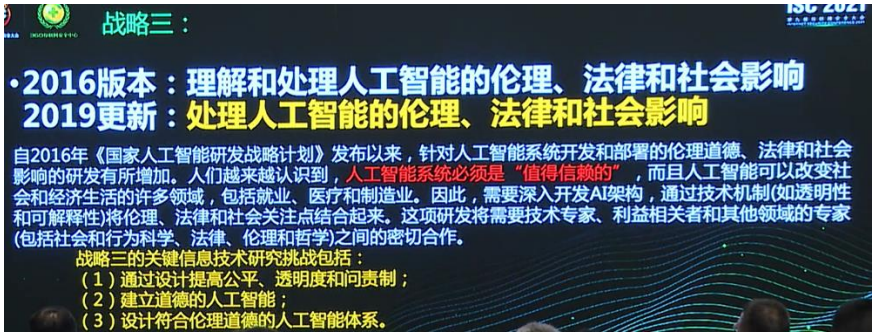
我国正处于初期阶段，国家的政策 130 字如下：



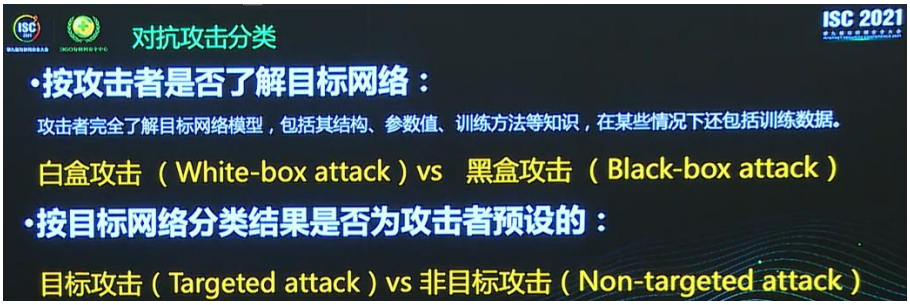
对比美国政策、7 个战略、战略解读：



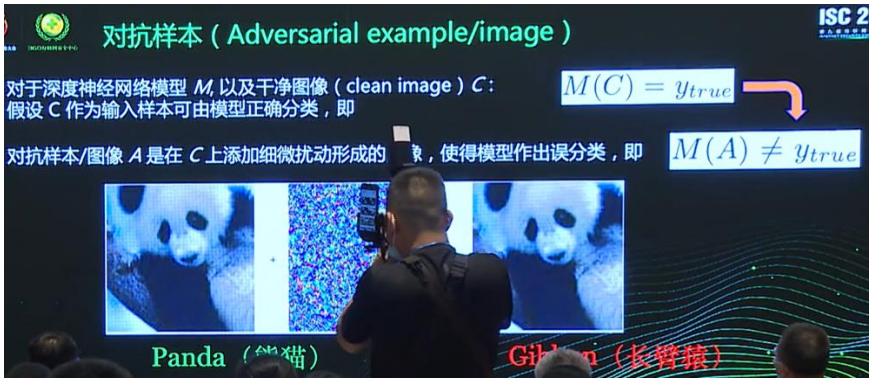




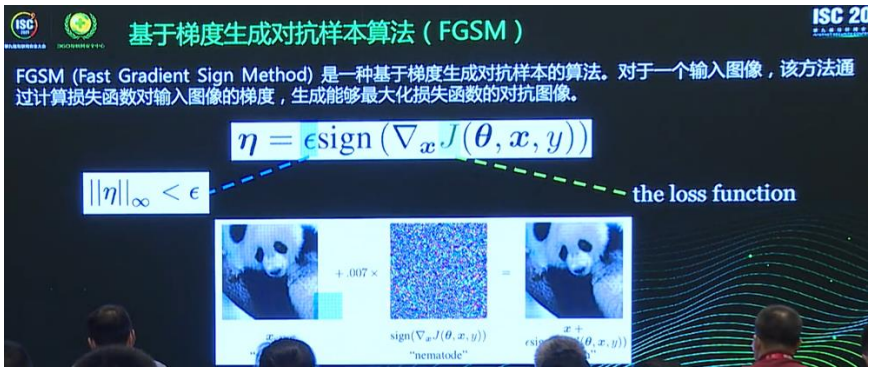
人工智能攻防和以前的攻防角度不太一样，比如对抗攻击。

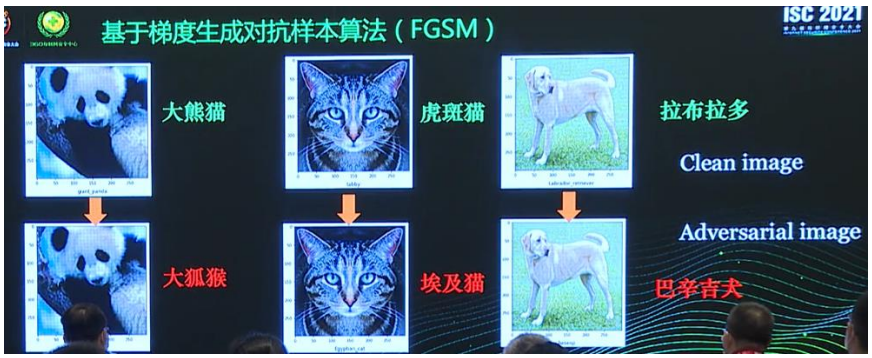


对原始图像做微小扰动，使分类结果错误，如下图把大熊猫识别为长臂猿：



简单的算法为例：**基于梯度生成对抗样本算法（FGSM）**

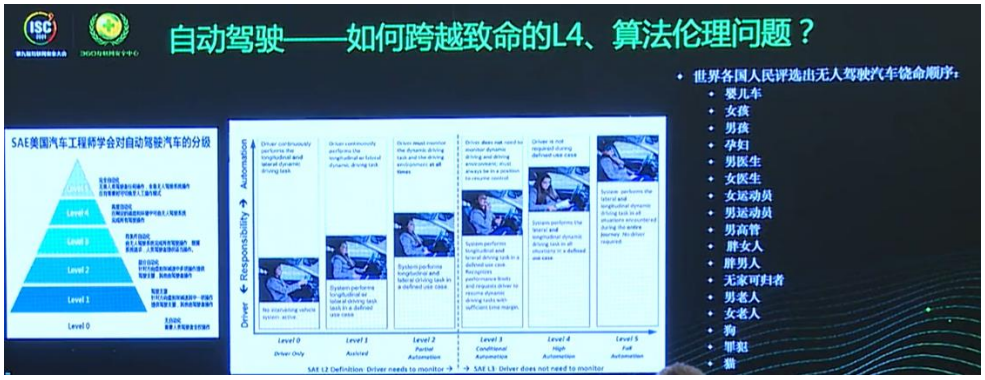




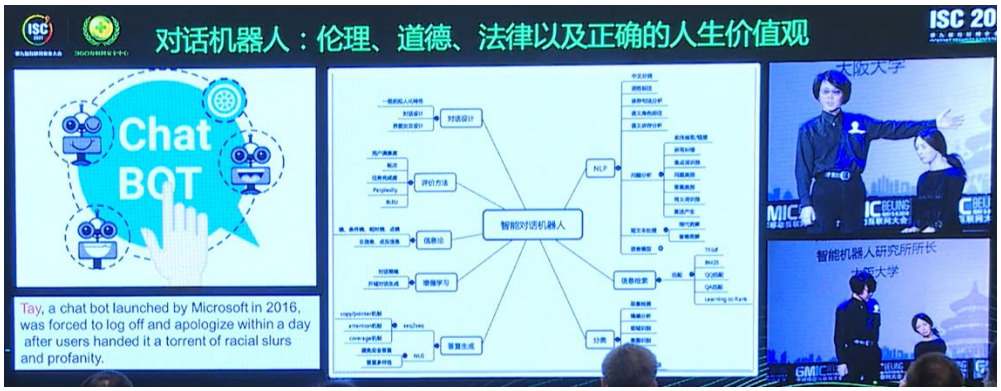
自动驾驶：如何跨越致命的 L4、算法伦理问题？

机器做不了的，人来负责->L4，99.99%都能处理，只有很小的部分需要人处理，人的大部分注意力都不在处理上，在精力不集中的情况下可能会处理不好。

交通事故判断应该交给机器还是人来做？



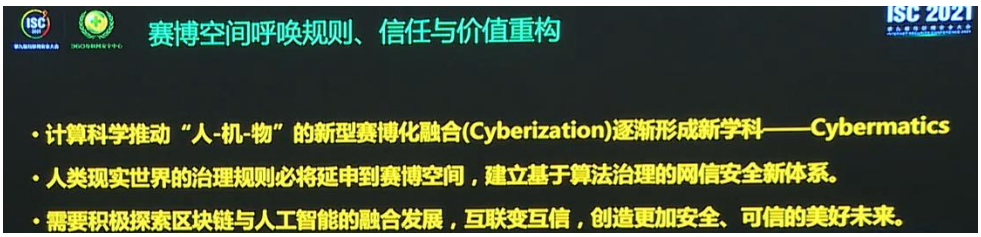
对话机器人：仅一天就关闭，因为有人教她说脏话，种族歧视、不正确的价值观


对话机器人：伦理、道德、法律以及正确的人生价值观
ISC 20
Chat BOT
Tay, a chat bot launched by Microsoft in 2016, was forced to log off and apologize within a day after users handed it a torrent of racial slurs and profanity.
智能对话机器人
大阪大学
智能机器人研究所所长

人机混合技术：


人机混合、数字克隆人：Cyber-Health与脑机接口
他/她是谁？
- 人有心脏和大脑
- 机器人只有AI/程序
- 混合人呢？半人/半机（Mixtures: Partial human/partial machine）
数字克隆人？（Digital Clone：Body & Mind）

结语：


赛博空间呼唤规则、信任与价值重构
ISC 2021
• 计算科学推动“人-机-物”的新型赛博化融合(Cyberization)逐渐形成新学科——Cybermatics
• 人类现实世界的治理规则必将延申到赛博空间，建立基于算法治理的网信安全新体系。
• 需要积极探索区块链与人工智能的融合发展，互联变互信，创造更加安全、可信的美好未来。