

高度隔离防护设施内 让不明物质“身份毕露”

设在国防科技研究院内的高度隔离防护设施1997年建成。设施内除了有东南亚唯一一间获联合国认证、主要测试化学物质的预验实验室，还有可进行涉及大量有毒化学物质测试与研究工作的消毒实验室、生物实验室，以及辐射及核子实验室。

苏德铭 报道
tohtm@sph.com.sg

如果本地某处突然发现疑似化学武器的物质，该如何鉴定物质是否真的有毒？政府机构应如何应对？如何断定需疏散多大范围的公众？

设在国防科技研究院内的“高度隔离防护设施”（High Containment Facility）是可帮助迅速解答以上种种问题的关键。

该设施由数个符合国际安全标准的隔离实验室组成，是本地唯一可负责接收、测试和鉴定不明生化、辐射及核子物质的实验设施。

高度隔离防护设施于1997年建成，并在过去20年不断加强各方面的能力，以求更高效地测试不明物质。国防科技研究院日前开放设施让媒体参观，并介绍了当中的设备与其性能。

可同时测查八种毒素

以测试化学物质为例，不明物质会先送到“预验实验室”（Preparation Lab），在一两个小时初步确定是否有毒，以及当中是否含有某些较危险的毒素。

为加快测试毒素速度，国防科技研究院也研发了全球首创、可同时测查八种毒素的技术。

由于所测试的物质可能腐蚀性极高，也可能散发有毒气体，因此实验室内的设施全由钢铁所制，气流设计方面也确保空气绝不往外流，以免毒气外泄。

该实验室高端的隔离与测试技术在2003年获国际认可，获颁联合国化学武器监督机构“禁止化学武器组织”（简称OPCW）的“指定实验室”（Designated Lab）认证。全球目前只有19间实验室获此认证，而国防科技研究院的预验实验室是东南亚唯一一间。

拥有上述认证意味着若有必要，其他国家可把不明物质委托于此进行测试，确定其中成分。据知，国防科技研究院的高度隔离防护设施过去三年曾接到三次这样的委托，但物质来自哪一个国家并不详。

国防科技研究院项目署长陆永强博士指出，预验实验室须符合国际标准，无论测试任何物质都得在14天内交出完整的分析报告。就算是从未发现过的新物质，也须在报告内完全“解剖”，把其化学成分列出。

“为了严守时限，我们接到不明物质后往往会不分昼夜地尽快进行多种测试与分析，压力相当大。”

他回忆：“还记得约两年前，我们突然接到大批如水泥块般的测试样本，不似我们一般熟悉的液体或泥土，因此得立刻想出新测试方法，那是我们遇过最艰巨的挑战之一。”

陆永强也透露，高度隔离防护设施的约60名人员须轮班，确保设施全天运作，以备突然接到不明物质得立刻测试。



国防科技研究院研究员在消毒实验室准备进行测试，鉴定个人防护器具是否能有效防止毒气渗透。（海峡时报）

“我们也在不断探究如何提升测试效率，毕竟发现可疑的危险物质时，政府机构需要尽快知道物质的特性，才能决定如何安全应对，包括传达正确且准确的信息，避免公众过度恐慌或胡乱猜测。”

另外，高度隔离防护设施内也有一间“消毒实验室”（Decontamination Lab），可进行涉及大量有毒化学物质的测试与研究工作的，包括鉴定个人防护器具（Personal Protective Equipment）是否能有效防止毒气渗透。

研究员会在一具人体模型的不同部位贴上装有化学液体的试管，再让模型穿上个人防护器具进入充满毒气的密封室，之后根据试管中液体的化学反应来鉴定保护器具的有效性。

除了测试化学物质，高度隔离防护设施也有测试如沙斯（SARS）、中东呼吸综合征（MERS）和伊波拉（Ebola）等病毒的生物实验室，以及测试钚（Plutonium）和铀（Uranium）等核材料的辐射及核子实验室。

维修和保养是一大挑战

后者在测试效率方面近期也有新突破，经过两年研发后，成功把测试钚的时间从两至三天缩短至六个小时。

国防科技研究院总裁张志浩受访时说：“高度隔离防护设施的维修和保养是一大挑战，因为得确保在过程中所有运作都不受影响，也不会造成安全风险。因此我们得不断精心规划，在增添后备设备的同时，也及时更换较旧的器材。”



国防科技研究院的预验实验室是全球19间获联合国化学武器监督机构“禁止化学武器组织”认证的实验室之一，也是东南亚的唯一一间。图为国防科技研究院人员示范在该实验室内测试不明化学物质的过程。

高科技提升军队网络安全

科技的使用能提升军队的作战能力，但同时也意味着需提防网络袭击，否则关键的机密资料被敌军或恐怖分子盗取，或器材被他们远程操控，后果将不堪设想。

为避免这类状况发生，国防科技研究院在网络安全方面开发了两项新技术，分别为电脑系统和通讯设备高效加密，确保资料不被盗取、信号不被拦截，以及能发现潜伏在电脑硬件主板的“超隐秘”恶意软件（malware）。

国防科技研究院日前开放让媒体参观，也向记者介绍了这两项技术。

其中一项是特制的“加密晶片”（Crypto Chip），电脑或通讯设备只要装上，系统中的资料以及传送或接收的信号将会加密，成为外人无法解读的乱码。

国防科技研究院高级研究员郑康宏说：“加密程序是我们特别编写的，机器复杂也极难破解。就算用最先进的超级电脑，也需要几

百万年才能破解吧。”

他指出，晶片也有防破坏装置，只要探测到有人企图用激光切割或以其他方式打开晶片，便会自动删除所有资料，以防盗取。

他也提到，无人机（drone）在军队中的使用日益普遍，因此更有必要确保网络安全，不让他人远程操控。

在发现恶意软件方面，国防科技研究院研发了电脑硬件主板BIOS的验证软件（BIOS Verifier），可快速探测BIOS是否遭恶意软件入侵。

国防科技研究院超级研究员叶峻铭指出，市面上的防毒软件（anti-virus software）只扫描电脑硬盘（hard disk），但近几年却出现能直接潜伏在BIOS上的恶意软件，一般的防毒软件无法发现。

“附在BIOS上的恶意软件能操控电脑，也能盗取资料，这在军队中绝不能发生。这样的验证软件便是多一层保障，确保电脑不被病毒入侵。”