

## 危害国家安全案例警示

### ◆ 案例一：郑州某军工专家被西方某大国策反为间谍，提供一次情报 5000 美元

张某是郑州某军工科研单位的高级专家，出国访学期间被西方某大国 M 国的情报人员拉拢、策反，出卖大量我国国防、军工等国家秘密。最终，他被郑州国安部门抓捕，以间谍罪被判有期徒刑 15 年。

### ◆ 案例二：危害军事安全：军舰泄密事件

2014 年 4 月，23 岁的张某在微信上添加了一个自称“记者”的人。此人以需要新闻报道材料为由，请张某为其提供军舰照片。张某被优厚条件吸引，想方设法进行拍摄。

在境外间谍机关的指使下，张某设法进入某军工企业。到 2014 年 8 月被采取强制措施时，张某已向对方提供目标照片 500 余张，其他敏感照片 200 余张。

2015 年 2 月 12 日，张某因“为境外刺探、非法提供国家秘密罪”被判处有期徒刑六年、剥夺政治权利三年。

### ◆ 案例三：危害国土安全：日本公民来江西非法测绘

2007 年 3 月、2009 年 8 月，两位日本公民佐藤正光、水上和则未经测绘行政主管部门批准，先后两次分别以考古、学术交流为名，携带高精度手持卫星定位仪到江西省南丰、鹰潭、上饶、铅山等地进行非法测绘活动。

江西省国家安全机关联合测绘部门对其审查，发现对象采集的坐

标点位数据中有 2 个绝密级、4 个机密级、1 个秘密级，一旦外泄，将对我国土和军事安全构成严重威胁。

#### ◆ 案例四：危害网络与信息安全：“海莲花”境外黑客组织

名为“海莲花”（OceanLotus）的境外黑客组织，自 2012 年 4 月起针对中国海事机构、海域建设部门、科研院所和航运企业展开精密组织的网络攻击。这很明显是一个有国外政府支持的 APT（高级持续性威胁）行动。

“海莲花”使用木马病毒攻陷、控制政府人员、外包商、行业专家等目标人群的电脑，意图获取受害者电脑中的机密资料，截获受害电脑与外界传递的情报，甚至操纵该电脑自动发送相关情报，从而达到掌握中方动向的目的。