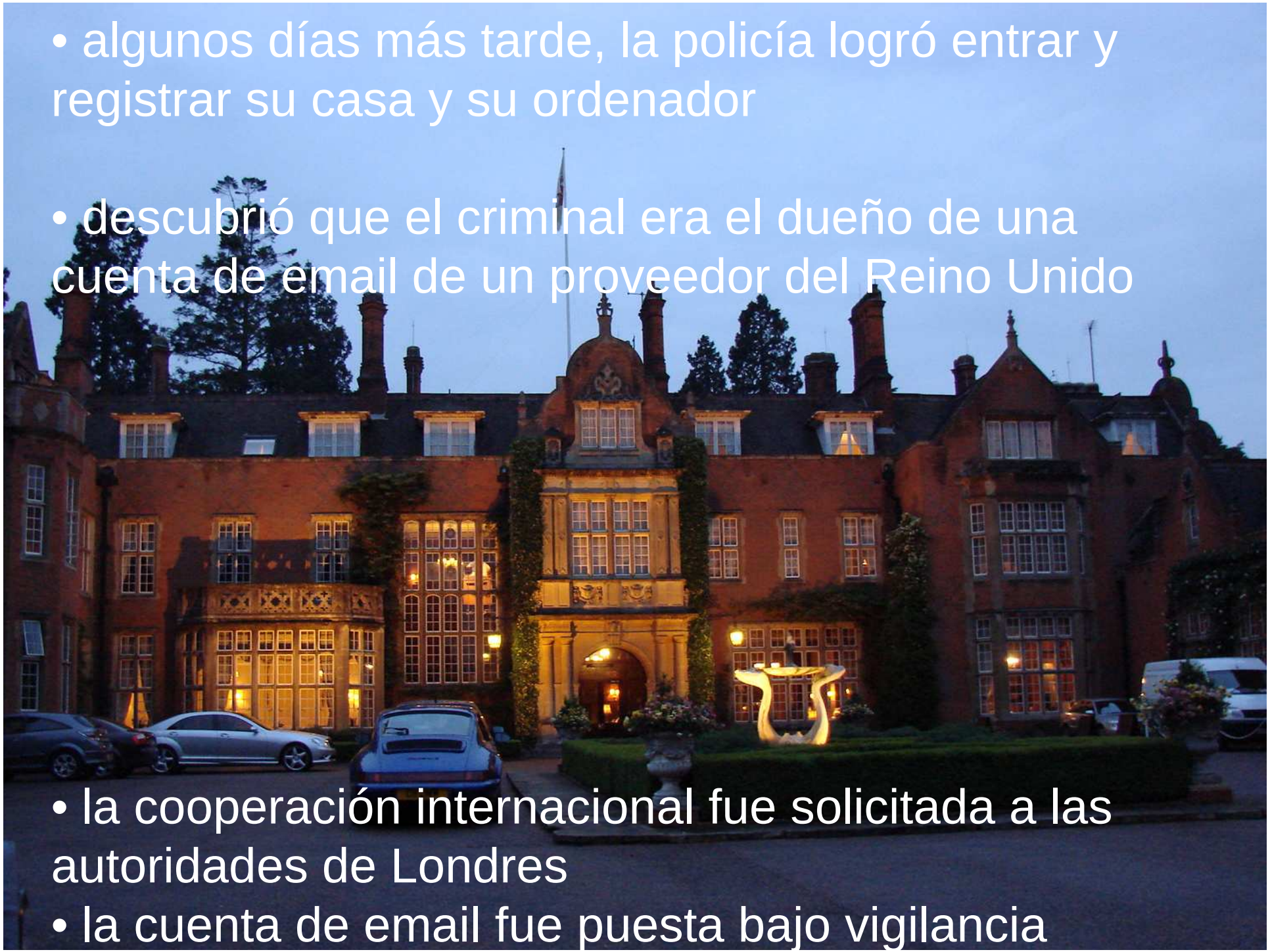
cooperación internacional

caso 1

- no es un típico “caso de *cibercrimen*”
- pero se recurrió a las herramientas de cooperación internacional de la Convención de Budapest

en el año 2005, un ciudadano de Noruega atracó un banco en Oslo



• algunos días más tarde, la policía logró entrar y registrar su casa y su ordenador

• descubrió que el criminal era el dueño de una cuenta de email de un proveedor del Reino Unido

• la cooperación internacional fue solicitada a las autoridades de Londres
• la cuenta de email fue puesta bajo vigilancia

• días después, el criminal accedió a su cuenta de email para mandar un mensaje

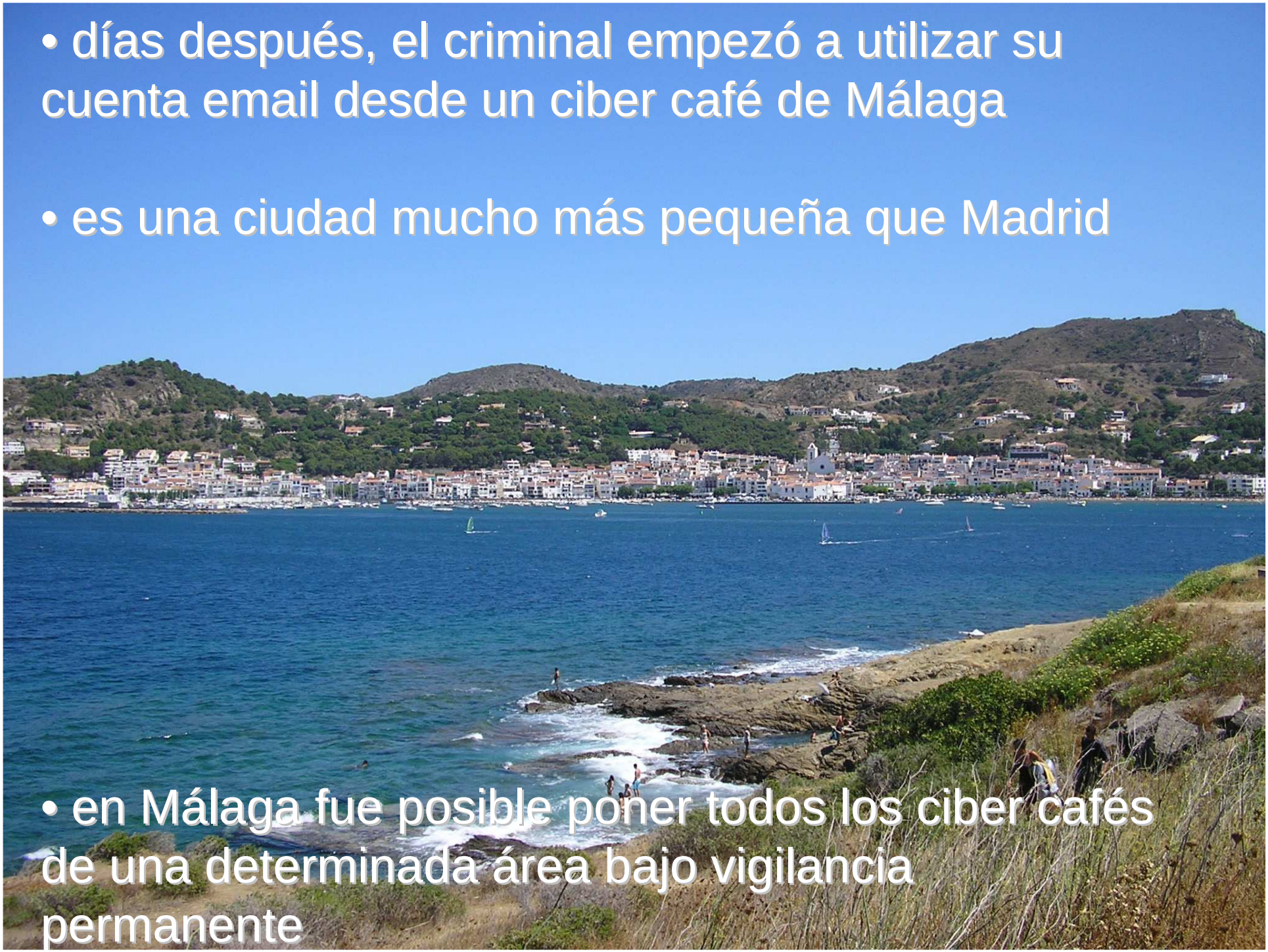
• en el Reino Unido, la policía obtuvo del ISP la información necesaria para concluir donde estaba el criminal

caso 1

- las autoridades españolas y británicas implementaron un sistema de alerta, cuyo objetivo fue conocer, cada vez que el criminal utilizaba su cuenta de correo electrónico, donde estaba
- así, cada vez que utilizó su cuenta, la policía británica obtuvo la dirección IP del equipo en el origen de la comunicación y lo comunicó de inmediato a la policía española
- entonces, la policía española obtenía del ISP español datos sobre el propietario o usuario de la dirección IP

- todas las conexiones se hacían desde un ciber café de Madrid

- intentando acercarse del café muy rápidamente, durante mucho tiempo a la policía no fue posible llegar antes de que el criminal se fuera


• días después, el criminal empezó a utilizar su cuenta email desde un ciber café de Málaga
• es una ciudad mucho más pequeña que Madrid
• en Málaga fue posible poner todos los ciber cafés de una determinada área bajo vigilancia permanente

caso 1

- después de algunos días de vigilancia, la policía británica anunció que el criminal estaba *online*, usando su cuenta de email y providenció su dirección IP
- muy rápidamente, el ISP de España informó la policía española sobre la ubicación concreta del ciber café
- los oficiales de policía en la calle pudieron identificar y detener el criminal, que al final fue extraditado a Noruega

caso 2

- un típico “caso de *cibercrimen*”

- pero las herramientas de la cooperación internacional no pudieron ser usadas

Estonia ratificó la Convención de Budapest en el año 2003

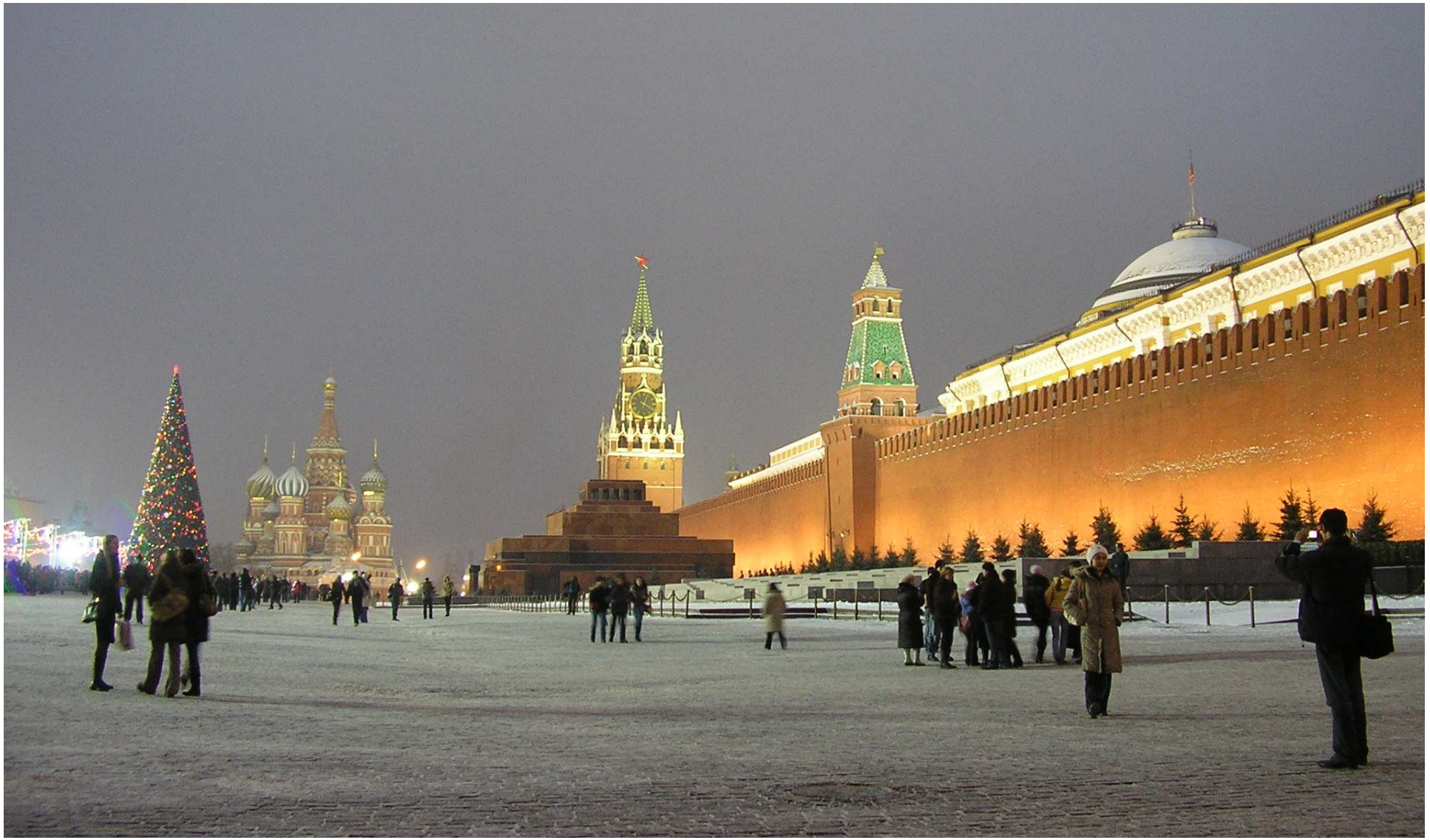
Estonia sufrió un muy importante ataque, del tipo (DDoS - *distributed denial of service*) en Abril y Mayo del año 2007

caso 2

- este ataque causó perturbaciones muy importantes a la vida cotidiana de la gente y al gobierno
- páginas *web* quedaron *fuera de servicio*, los servidores se han saturado
- varios ataques utilizando *botnets* fueron ejecutados – muchas páginas *web* estonias no estuvieron disponibles algunos días

caso 2

- se identificaron algunos IP sospechosos
- pero solo se logró hacer comparecer ante juicio a una persona, a la que se condenó
- en realidad, era el único ciudadano estonio entre los sospechosos que fue posible identificar



todos los demás sospechosos usaron IP de un Estado que no firmó la Convención – y por lo tanto, cuya ley no permitia cooperar con otros Estados en investigaciones