Cooperación Internacional en las Investigaciones por Delitos Informáticos

Albert Rees
Sección de Delitos Informáticos y Propiedad Intelectual
División de lo Penal, Departamento de Justicia de los Estados Unidos


Agentes de Rumania descubren que el ataque provino de Vancouver
Agentes de Canadá hacen la captura
Un delincuente penetra un banco en Bangkok
Investigadores argentinos descubren que el ataque provino de Bucarest
Investigadores de Tailandia descubren que el ataque provino de un computador en Buenos Aires

Los retos de las investigaciones internacionales de delitos informáticos

- Los países deben:
  - Promulgar normas para **tipificar como delitos los abusos informáticos**
  - Comprometer **el personal y los recursos** adecuados
  - Mejorar las habilidades para **localizar e identificar** a los delincuentes
  - Mejorar las habilidades para **recoger y compartir pruebas a nivel internacional**

RETO:

Promulgar normas para tipificar como delitos los abusos informáticos

La necesidad de tipificar como delitos los ataques a redes informáticas

- La “doble incriminación” suele ser necesaria para que dos países puedan cooperar en un asunto penal concreto.

- La “doble incriminación” constituye la base para:
  - Tratados de extradición
  - Tratados de asistencia jurídica mutua

Superando la división en relación con la doble incriminación

- Los países deben ponerse de acuerdo en qué tipificar como delito
  - Estrategia de la OEA sobre Seguridad Informática
  - Resolución 55/63 de la Asamblea General de las Naciones Unidas
- Un esfuerzo para lograrlo: La Convención sobre Delitos Informáticos
  - Un punto de partida para el derecho sustancial
- Los países deben modificar sus normas para implementarla

RETO:

Comprometer el personal y los recursos adecuados

Necesidades para el cumplimiento de la ley

- Expertos dedicados a delitos de alta tecnología
- Expertos disponibles 24 horas al día
- Entrenamiento continuo
- Equipos actualizados de manera continua
  - Ya no más “una linterna y un arma”

- **Cada país** necesita tener este nivel de competencia

Las soluciones no siempre son fáciles

- Debe formularse una estrategia de seguridad informática
- Surgen problemas difíciles sobre el presupuesto (inclusive en los Estados Unidos)
- Requiere el compromiso de oficiales de alto rango
- La cooperación con el sector privado puede ayudar

RETO:

Mejorar las habilidades para localizar e identificar a los delincuentes

El problema de localizar e identificar a los delincuentes

- El paso investigativo principal consiste en localizar la fuente del ataque o de la comunicación
  - Qué sucedió puede ser relativamente fácil de determinar
  - Identificar a la persona responsable es muy difícil
- Esto se aplica a los delitos de *hacking* al igual que a otros delitos facilitados por las redes informáticas

Rastrear una comunicación

- Sólo hay dos maneras de rastrear una comunicación:

1. Mientras de hecho está sucediendo
2. Usando datos guardados por los proveedores del servicio de comunicación

Rastrear una comunicación

- La infraestructura debe generar datos sobre el uso
- Los proveedores deben conservar suficientes datos para permitir el rastreo
- Las normas y los procedimientos deben permitir que los agentes de la autoridad tengan acceso oportuno sin alertar al usuario
- La información debe compartirse rápidamente

Resolviendo el Dilema del Rastreo I: Datos sobre el uso

- Los países deberían motivar a los proveedores para que produzcan y conserven datos críticos sobre el uso

- La habilidad de las autoridades competentes para identificar delincuentes se potencia con el acceso a los datos sobre el uso
  - Los países han tenido distintos acercamientos al buscar un balance entre esta necesidad y otras preocupaciones de la sociedad
  - La industria tendrá sus opiniones sobre los períodos apropiados de conservación

Resolviendo el Dilema del Rastreo II: Acceso de las autoridades competentes

- Los ordenamientos jurídicos deben darles a las autoridades competentes poder suficiente para acceder a los datos sobre el uso
  - Por ejemplo: acceso a los registros guardados en archivos y a la información sobre el uso en tiempo real

- Conservación de las pruebas por las autoridades competentes
  - Es fundamental, porque los procedimientos de asistencia jurídica internacional son lentos
  - Debe ser posible realizarlo sin suponer “doble incriminación”
  - Artículo 29 de la Convención sobre los Delitos Informáticos

Resolviendo el Dilema del Rastreo III: Compartiendo Pruebas

- Los países deben mejorar sus habilidades para compartir datos rápidamente

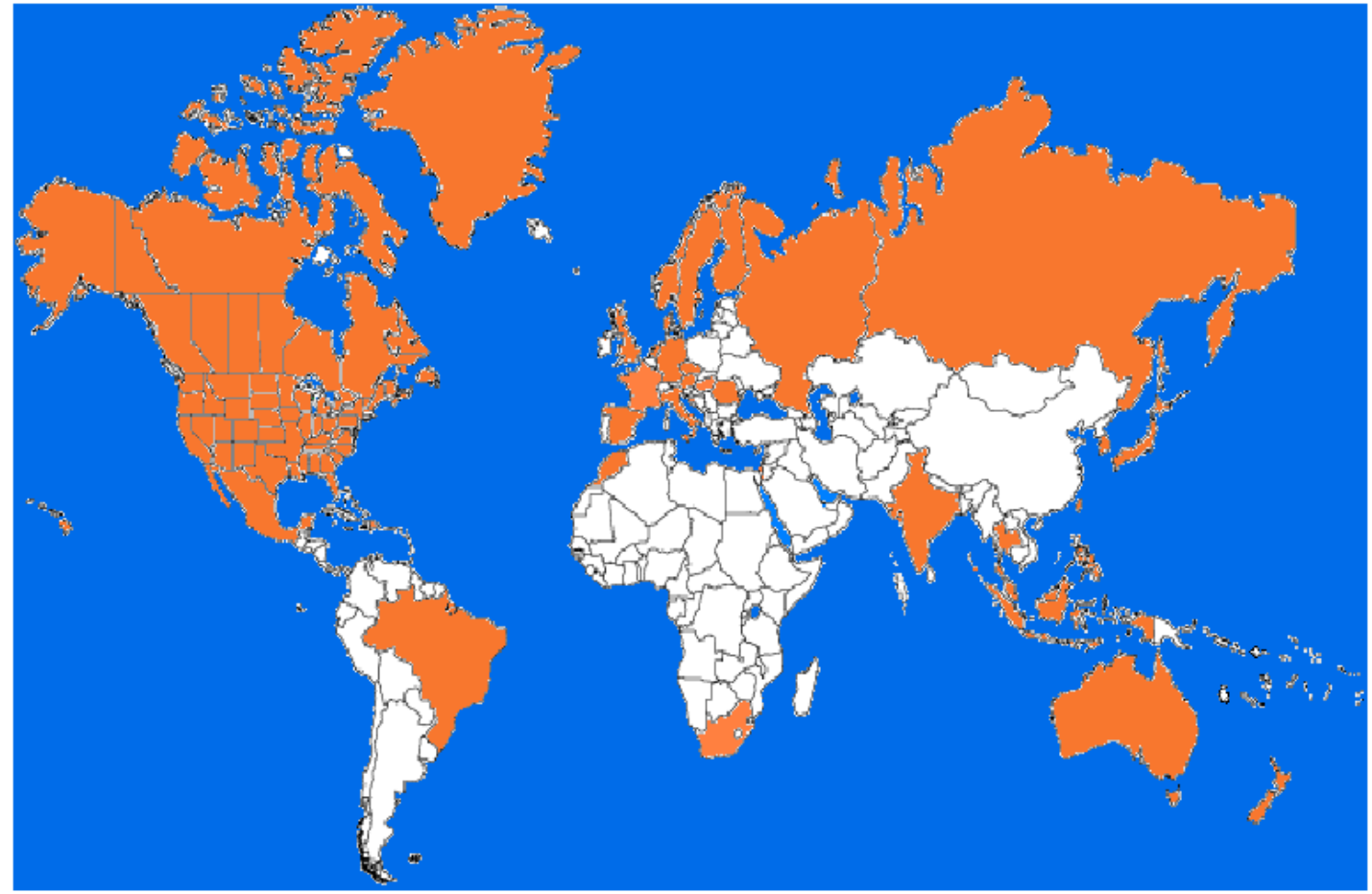
- Si esto no se hace rápidamente, el “rastro” electrónico se perderá
  - La mayoría de los mecanismos de cooperación tardan meses (¡o años!), no minutos
  - Artículo 30 de la Convención sobre Delitos Informáticos: revelación ágil de los datos sobre el uso

Resolviendo el Dilema del Rastreo III: Compartiendo Pruebas

- Cuando las autoridades competentes reciben una solicitud, deben poder:
  1. Conservar todos los datos sobre uso doméstico
  2. Notificar al país solicitante si el rastro conduce a un tercer país
  3. Suministrar suficientes datos al país solicitante para permitirle pedir asistencia del tercer país

- Los países deben poder hacer esto entre ellos rápidamente, y de manera continua (24 horas al día, 7 días a la semana)

La Red 24/7 del G8 para Delitos de Alta Tecnología



RETO:

Mejorar las habilidades para recoger y compartir pruebas a nivel internacional

Recoger y compartir pruebas

- ¿Las pruebas recogidas en un país serán admisibles en los tribunales de otro país?
- Existe potencial para problemas probatorios
  - Recolección de pruebas digitales
  - Rastreo de comunicaciones electrónicas a través del planeta
  - Técnicas forenses informáticas
- Es posible que los tratados sobre asistencia jurídica mutua vigentes en el momento no contemplen adecuadamente las pruebas electrónicas

Soluciones para la recolección y el intercambio de pruebas

- La Convención sobre los Delitos Informáticos
  - Funciona como un tratado de asistencia jurídica mutua para aquellos países que no lo tienen
  - Las partes del tratado acuerdan brindarles asistencia a los otros países para que obtengan y revelen pruebas electrónicas

- Desarrollando estándares técnicos internacionales
  - Organización Internacional para las Pruebas Informáticas

Recolección unilateral de pruebas

- Información disponible públicamente
- Obteniendo pruebas electrónicas sin el consentimiento del dueño
  - Aceptación del G-8 y el Consejo de Europa

Medidas informales de cooperación

- De investigador a investigador
- Ventaja: es un método rápido
- Desventajas:
  - Frecuentes restricciones normativas locales para brindar asistencia
  - Puede ser difícil ubicar un investigador que pueda y quiera brindar asistencia

Otras medidas de cooperación

- Investigación conjunta
- Algunos puntos de contacto de los Estados Unidos en su país
  - Agregado jurídico del FBI (LEGATT), un agente del FBI
  - Agregado jurídico del Departamento de Justicia, un fiscal
  - El Servicio de Inmigración y Control de Aduanas (ICE)
  - Servicios Secretos (USSS)
- INTERPOL y otras organizaciones semejantes

PARA MAYOR INFORMACIÓN

Albert Rees

+1 (202) 514-1026

albert.rees@usdoj.gov

WWW.CYBERCRIME.GOV

Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice