G8 24/7 High Tech Contact Points

In the aftermath of September 11, it is critical that countries have the ability for their public safety officials to contact officials in other countries on an emergency basis in order to identify the source of terrorist communications, investigate threats and prevent future attacks. We live in a world where terrorists can bypass national borders through new communications technologies and plan an attack in one part of the world from a physical location thousands of miles away.

Networked computers are not only tools available to terrorists and all sorts of other criminals to advance their schemes on an international basis, but these computers may also be the target of attacks. In investigations involving computer networks, it is often important for technically literate investigators to move at unprecedented speeds to preserve data and locate suspects. Often, a criminal can only be stopped if evidence of his or her conduct is preserved within minutes, a time-frame too short for us to rely on traditional international assistance regimes.

Therefore, to enhance and supplement (but not replace) traditional methods of obtaining assistance in cases involving networked communications and other related technologies, the G8 created in 1997 a new mechanism to expedite contacts between countries. Today, close to 20 countries have joined a network of 24-hour points of contact for cases involving electronic evidence. These contacts are available at all hours, 7 days a week, to receive information and/or requests for cooperation.

This network has been used successfully in many instances to investigate threats and other crimes in a number of countries. For example, the network has been used to help secure the conviction of a murderer in the United Kingdom by facilitating the preservation and disclosure of Internet records in the United States. The network has also been used on several occasions to avert hacking attacks, including attacks on banks in the United States, Germany and Mexico. Conversely, in the context of the ongoing investigation into the September 11th terrorist attacks, the lack of a point of contact in a particular country impeded the investigation of a serious threat.

Because terrorists operate in all our countries, it is critical to expand this coverage accordingly to ensure that we can stop a terrorist in one country from using new communications technologies to facilitate an attack in another country.

* What we need:

  - "24/7" capability. Having an "around-the-clock" capability is critical not only because terrorist plans and other criminality involving computer networks can occur at any hour of the day, but also because of time-zone differences between our countries. In other words, even if police uncover a threat at noon in Tokyo, the evidence they need to prevent the activity may be stored on a computer in the United States, where it is 22:00 hours.

  - The 24/7 capability does not necessarily entail the establishment of a high-tech operations center open around the clock; rather, the capability can be accomplished simply by ensuring that an already established traditional operations center knows how to reach a high-tech expert at all hours [e.g., via home phone number, cellular phone, pager].

  - The 24/7 network have established a template with very brief set of instructions for how to use the network in each participating country. We would also need you to

complete this template.

* Who we need:

- It is, however, critical, the contact point involve more than just a an already established traditional operations center: personnel knowledgeable in investigations involving computer and electronic evidence must be reachable around the clock. The point is not simply to be able to relay an urgent request on a 24/7 basis, but also to reach someone who can act on that request.

- [If contact is being made by Lyon Group Head of Delegation or other official not familiar with contact point .... We understand that (INSERT Name of Ministry and particular unit within Ministry) is where this expertise may lie within your government.]

* How and When we need it:

- We need this information urgently, because of its potential relevance to ongoing investigations. The information we need is contained on the attached form.

FAX

To: Christopher Painter
U.S. Department of Justice
[Chair, G8 Subgroup on High-tech Crime]
Fax: 001-202-514-6113
Phone: 001-202-514-1026

From: _____

_____

Pages: _____

Date: _____

High-tech Crime 24-Hour Point-of-Contact Network
Sign-Up Form

* The G8 countries have established a network of 24-hour points-of-contact for use in terrorist and other criminal cases involving electronic evidence, and are now urgently seeking to expand this network to other countries. It is critical, however, that countries not only identify a knowlegeable contact-point, but also equip that contact so that he or she is available on a 24-hour basis (e.g., with a cellular phone or pager). Time zone differences will often mean that terrorist activities and other crimes involving computer networks and electronic evidence will take place outside of normal business hours in either the requested or requesting state.

* To join the network, please provide the following information:

1. CONTACT and TELEPHONE NUMBER [and FAX and E-MAIL, if available] (*Example: "UNITED STATES: Command Center, U.S. Department of Justice, Washington, D.C., Telephone: 1-202-514-5000, Fax: 1-202-514-5778.")*

_____

_____

_____

2. DESCRIPTION OF CONTACT (*Example: "UNITED STATES: The Justice Department Command Center is a telecommunications center that is open 24 hours a day. Its personnel can immediately connect the caller to an appropriate investigator or expert. The Command Center itself does not have electronic evidence investigators or experts.")*

3. LANGUAGE CAPABILITIES OF CONTACT (*Example: "UNITED STATES: Command Center personnel speak English only.")*

4. WHAT TO SAY WHEN CALLING CONTACT NUMBER (*Example: "UNITED STATES: When calling with an electronic evidence emergency, ask to be connected to: Martha ('Marty') Stansell-Gamm, Chief, Computer Crime and Intellectual Property Section, U.S. Department of Justice. If Ms. Stansell-Gamm cannot be located, ask for: Christopher Painter, Deputy Chief, Computer Crime and Intellectual Property Section, U.S. Department of Justice.")*

5. PLEASE PROVIDE E-MAIL CONTACT FOR DISTRIBUTION OF UPDATES TO CONTACT POINT LIST (*UNITED STATES: christopher.painter@usdoj.gov and adam.r.isles@usdoj.gov)*