

G7 24/7 Cybercrime Network

Thomas Dougherty
U.S. Department of Justice
Computer Crime and Intellectual Property
Section
And
Legal Advisor
U.S. Embassy-Dhaka, Bangladesh

History of the Network

- Meeting of the G8 Justice and Interior Ministers – December 1997 called for creation of a network
 - “With regard to high-tech crime, we must start by recognizing that new computer and telecommunications technologies offer unprecedented opportunities for global communication. As nations become increasingly reliant upon these technologies, including wireless communications, their exploitation by high-tech criminals poses an ever-greater threat to public safety.”
 - Statement of Principles included
 - No safe havens
 - Investigation and Prosecution must be coordinated among

1997 Action Plan

- “Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.”
- “Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.”
- “Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches; and computer searches of data where the location of that data is unknown.”

The G8 24/7 Network was born

- Point to point network for urgent assistance in cybercrime matters
 - Single point of contact (POC)
 - Available 24 hours per day, 7 days per week
 - POC should be knowledgeable in cybercrime matters
- Primary purpose of the Network is to preserve data for subsequent transfer through mutual legal assistance channels
 - Described in the past as a “fast freeze and a slow thaw”

24/7 Network Protocol

- “The G8 24/7 points of contact are provided for investigations involving electronic evidence that require urgent assistance from foreign law enforcement. High-tech crimes raise new challenges for law enforcement. In investigations involving computer networks, it is often important for technically literate investigators to move at unprecedented speeds to preserve electronic data and locate suspects, often by asking Internet Service Providers to assist by preserving data. Therefore, to enhance and supplement (but not replace) traditional methods of obtaining assistance, the G8 has created the Network as a new mechanism to expedite contacts between Participating States or other autonomous law enforcement jurisdictions of a State (hereinafter referred to as “Participants”).”

How the Network Works (The Protocol)

- “To use this Network, law enforcement agents seeking assistance from a foreign Participant may contact the 24-hour point of contact in their own state or autonomous law enforcement jurisdiction, and this individual or entity will, if appropriate, contact his or her counterpart in the foreign Participant. Participants in the Network have committed to make their best efforts to ensure that Internet Service Providers freeze the information sought by a requesting Participant as quickly as possible. Participants have further committed to make their best efforts to produce information expeditiously. This is subject to the understanding that a requested Participant’s legal, technical or resource considerations may affect the extent to which - and the time frame within which – the Participant may produce evidence, as well as the process of Mutual Legal Assistance, by which the requesting country seeks release of that information though the usual MLAT or Letters of Request procedure.”

Informal Nature of the Network

- Network was deliberately designed with few rules and procedures to stimulate, rather than impede, cooperation.
- A checklist has been developed to guide participants in formulating their requests to maximize the

Checklist for Use of the G8 24/7 Network

To assist members of the G8 24/7 Network when making a request of another member country, the following checklist is a guide to information that the requesting country must provide to consider when making a request for assistance. While there is no assurance that a request made by use of this checklist will be submitted in the form of a request, the checklist will help to make requests more thorough and "member-ready".

The checklist is not exhaustive and its value and applicability will often be determined by the nature of the enquiry, the type of offence under investigation, legislative constraints in the requesting country and the availability of certain information that cannot be shared or sent over public networks.

The information is split into two categories, i.e. information which is **Priority** (that is, information that directly or indirectly presents an all requests) and information which is **Optional** (that is, useful information that the requesting country considers may be beneficial to the country where the request is being made).

1. Priority Information

1.1 Identification and Contact Information for the Requesting 24/7 Network Agency, to include:

- a) Name of requesting individual
- b) Name of request (if organization)
- c) City and country of organization
- d) Requester's case file reference number
- e) Requester's telephone number (include hours)
- f) Requester's telephone number (after hours)
- g) Requester's fax number
- h) Requester's mailing (postal) address
- i) Requester's e-mail address

1.2 Title and title of request

1.3 Purpose of the request: what action and/or evidence is required?

1.4 How the crime was committed. (In completing this section please be mindful of any confidentiality issues in your investigation)

These include the following:

- a) Is the evidence for which you seek information a crime in the Requesting country? If yes, please provide the relevant statute or criminal code reference.
- b) Is there a victim? If yes, what country are they in?
- c) The date and location of the offence please state 1. by "As above" you mean the location where the harm was suffered by the victim, or the location of the suspect.

New Network Integrity Policy

- Designed to assist those members that may be having difficulties in maintaining a reliable, 24/7 communication channel through a mentoring process;
- Not intended as a method to exclude countries, but rather as a way to keep member countries in the Network and attract new member countries.

A Steadily Growing Network

- From humble numbers in 1998 to 70 countries worldwide today.



Four Requirements for Membership

- Contact point available 24/7
- Contact point must have basic English language skills
- Contact point must have basic technical skills
- Contact point must be familiar with domestic laws and policies

A Network More Active Than Ever

- As an example – the United States had received over 100 incoming requests in the first 2 months of the 2014
- The United States had made over 25 outgoing requests to other countries in that same time period

Types of Requests

- Mostly data Preservation Requests
- Some “life or limb” Requests

Ongoing Network Projects

- UK G7 Project focused on regional trainings for members of the Network and potential new members;
- Italian G7 ongoing project focused on a secure web portal for Network points of contact

Summary Points

- Network deliberately designed as informal to facilitate rather than hinder cooperation;
- Network was established to complement rather than replace other channels for cooperation;
- Requirements for membership are intentionally few to allow for more participation in the Network;
- Primary purpose of the Network is to preserve digital evidence for subsequent transfer through legal channels.

U.S. DOJ Point of Contact

RICHARD GREEN

richard.green@usdoj.gov

+1.202.514.1026.

Computer Crime and Intellectual Property Section
(CCIPS)