National Institute of Justice

Moving Public-Private Partnerships From Rhetoric to Reality: CIRCAMP / CSAADF Transferability Assessment

John T. Picarelli, Ph.D.

August 2009

NCJ 230403

Discussion Paper

NIJ

Moving Public-Private Partnerships From Rhetoric to Reality: CIRCAMP / CSAADF Transferability Assessment

John T. Picarelli, Ph.D.

August 2009

NCJ 230403

Online child exploitation is a serious problem.[1] Despite significant investments in investigation and prosecution, law enforcement still finds it difficult to mitigate the production, transfer and viewing of online child exploitative materials. The COSPOL[2] [Comprehensive Operational Strategic Planning for the Police] Internet Related Child Abusive Material Project (CIRCAMP) is an effort to develop a workable solution to online child exploitation. Employing an innovative partnership between law enforcement, financial institutions, businesses (e.g., Internet service providers [ISPs]) and nongovernmental organizations (NGOs), the CIRCAMP network coordinates multinational investigations, targets financial flows to child exploiters and denies the Internet to viewers of online child exploitation.

This study explores how CIRCAMP agencies and international organizations team with the private sector to enhance investigative tools against online child exploitation. It opens with a discussion of online child exploitation and the most significant challenges facing law enforcement. It finds that the CIRCAMP network addresses many of these challenges, and both the accomplishments and criticisms of the network are discussed in depth. The study focuses on three elements of the CIRCAMP program: the level of cooperation and resulting successes from the CIRCAMP network, the use of technology filters, and the targeting of financial flows as a deterrent and investigative tool. It concludes with an assessment of the potential applicability for U.S.-based efforts against online child exploitation.

What Is the Problem?

Online child exploitation has grown immensely since the early 1990s. Suppliers and purchasers of child exploitation were able to locate one another online more easily after the formation of the Usenet in the 1980s and early 1990s. The dawn of the World Wide Web in the mid-1990s provided pedophiles a readymade vehicle for distributing child exploitation materials. The arrival of relatively inexpensive, high-quality digital cameras and camcorders has significantly reduced barriers to entry for producers of child exploitation materials. The growth of Web 2.0, specifically peer-to-peer (P2P) software packages, has further complicated efforts to halt the distribution of online child exploitation.

Recent examples of online child pornography investigations bear out the scope of the problem. The National Juvenile Online Victimization Survey (N-JOV) of 2005 found that between July 2000 and June 2001, law enforcement agencies arrested 1,713 people for Internet-related possession of child exploitation materials.[3] In FY 2007, the Internet Crimes Against Children (ICAC) task forces conducted 10,500 forensic investigations of online child exploitation, resulting in the identification of 400 victims and the arrest of 2,400 suspects.

[1] The members of CIRCAMP and others whom the author interviewed for this report noted the need to use the term "child exploitation" or "child abusive materials" in lieu of the more common phrase "child pornography." Their concern was that the public often conflates the term child pornography with more generally accepted (and in some cases legal) forms of adult pornography worldwide. The result is an obfuscation of the trauma and exploitation that children suffer in the production and distribution of these materials.

[2] Comprehensive Operational Strategic Planning for the Police.

[3] Wolak, J., D. Finkelhor, and K. Mitchell, *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Survey*. Alexandria, Va.: National Center for Missing and Exploited Children. 2005., available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

Efforts to curtail online child exploitation are distributed throughout the U.S. criminal justice system. Federal agencies are heavily invested in the issue. The U.S. Department of Justice is intensely involved in the investigation and prosecution of online child exploitation. In 2008, the Providing Resources, Officers and Technology to Eradicate Cyber Threats (PROTECT) Our Children Act provided over $1 billion for the formation of a national strategy for child exploitation prevention and interdiction and enhanced the Office of Juvenile Justice and Delinquency Prevention-sponsored ICAC task forces.[4] State, local and tribal law enforcement agencies are also thoroughly engaged in the online child exploitation issue. Overall, the N-JOV survey found that online child exploitation possession cases originated at all levels of law enforcement, with 60 percent from state and local agencies, 25 percent from federal agencies, 11 percent from ICAC task forces and 3 percent from overseas.

Law enforcement faces significant hurdles when investigating online child exploitation. Child exploitation materials are often produced in foreign countries where there are limited resources for investigating or prosecuting child abuse. Criminals design distribution networks to obfuscate and delay investigation; tactics include placing servers hosting child pornography sites in different countries or countries with stringent privacy laws. Resource constraints pose another problem, taxing law enforcement agencies with length and technically demanding investigations. In addition, cooperation between law enforcement agencies — another key to a successful investigation — remains one of the thorniest problems to overcome. Another hurdle is the coordination problems that are specific to online child exploitation cases. While coordination between law enforcement agencies is hard enough even under the best of circumstances, many online child exploitation investigations involve law enforcement agencies that operate under different legal codes and with differing technical investigation capacities — factors that further complicate the situation. Investigators will also need to collect evidence from the private sector, especially the ISPs that host the Web sites and provide the infrastructure that connects them to the Internet.

What Is the CIRCAMP Network?

In response to the need to foster international coordination against cross-border forms of crime, the European Police Chiefs Task Force (EPTCF) established the COSPOL initiative in 2004. Under COSPOL, the EPCTF is able to identify pressing cross-border criminal needs and initiate efforts to form lasting international cooperative networks among law enforcement agencies in Europe. The EPCTF identified online child exploitation as one of the areas that COSPOL should encourage its members to focus on, and this led to the formation of CIRCAMP.

The overall aim of the CIRCAMP network is to leverage the resources of and improve coordination between law enforcement agencies in Europe in online child exploitation cases. The CIRCAMP network has three primary goals:

1. Detect, disrupt and dismantle networks, organizations or structures used for the production and/or distribution of child abusive files and to detect offenders, identify children and stop abuse.

[4] Public Law 110-401, 42 U.S.C. § 17601, 122 Stat. 4229, Oct. 13, 2008.

2. Reduce harm to society by attacking European distribution of child abusive material, and disrupt the methods used by the organized crime groups that are responsible for the illegal pay-per-view sites.
3. Create a common understanding towards global policing of the Internet through cooperation.

The National Criminal Investigation Service in Norway (called "Kripos") serves as the "driver" (i.e. program manager) for CIRCAMP, and the U.K.'s Child Exploitation and Online Protection Center serves as a co-driver.[5] The other member states and liaison agencies in the CIRCAMP network are:

- Ireland: National Bureau of Criminal Investigation.
- France: Central Directorate of Criminal Investigation *and* Gendarmerie Nationale.
- Sweden: National Criminal Police.
- Italy: Postal and Communications Police Service.
- Finland: National Bureau of Investigation.
- Belgium: Belgium Federal Police.
- Spain: National Police.
- Malta: Malta National Police.
- Denmark: Danish National Police.
- Netherlands: Dutch National Police.
- Poland: Polish National Police.
- European Police Office (EUROPOL).
- International Criminal Police Organization (INTERPOL).

These member state and liaison agencies participate in planning processes coordinated through the COSPOL framework. CIRCAMP is currently operating under an action plan published in 2006. The action plan has three basic elements:

1. Implementing the Child Sexual Abuse Anti-Distribution Filter.
2. Analyzing and investigating payment systems for online child exploitation.
3. Analyzing patterns gleaned from sites that distribute child exploitation materials.

CSAADF is unique because a private sector entity, Telenor, initiated the program. Telenor is the largest ISP in Norway. Telenor contacted Kripos seeking a way to filter online child exploitation from its network proactively. This filter would be similar to the system set up by the Internet Watch Foundation and British Telecom a few months prior in the U.K. Telenor developed the software and shared it with law enforcement at no cost. Telenor needed law enforcement help to identify online child exploitation sites. To help Telenor, CSAADF is working with NGOs such as Save the Children to monitor and expand the list of child pornography Web sites.[6]

[5] A more detailed listing of bureaus within these agencies and links to them is available at: http://www.circamp.eu/index.php?option=com_weblinks&view=category&id=3&Itemid=3.

[6] The NGOs, such as Save the Children, will contribute addresses received from the public, and the content will be evaluated (according to national legislation) by the police. Whether a domain is added to a list or not is solely the

The CSAADF program has expanded since its inception in Norway. A number of CIRCAMP countries have implemented the filter (e.g. Sweden, Denmark) and others are planning to do so.

The CSAADF filter is the linchpin of the CIRCAMP network. The purpose of the filter is not to bring an end to the acquisition of child abusive materials online. Rather, the filter reduces the incidental or casual viewing of this material and allows investigators to target more "hard core" consumers who are more likely to have the technical wherewithal and drive to sidestep the filter.

Implementing the filter has not proven technologically complicated or expensive for the private sector. The filter is often a simple Domain Name System (DNS)-level software package that the ISP implements.[7] When an incoming Web site request matches one of the Web sites on a member state's blocked list, the user is automatically redirected to a "stop" page rather than the Web site sought. The stop page, a sample of which is shown in the appendix, warns users why they were redirected and offers an opportunity to question why a particular Web site was blocked. In some cases, CIRCAMP member states have moved to more sophisticated proxy server filtering that makes it more difficult to bypass the DNS-level filter. Yet this also remains inexpensive because the proxy server software is an off-the-shelf, ready-to-use package designed to work with existing server technology.

The CIRCAMP network is both pragmatic and flexible in its approach to filtering. Since each country's criminal codes define child exploitative materials differently, each member state generates its own list of Web sites to filter based on its definition of child exploitative materials. For example, computer-generated images of children engaged in sex acts are illegal in some countries, while other countries do not criminalize these images. CIRCAMP maintains a central blacklist of sites, dubbed the "CIRCAMP Worst Of" list, that are filtered in all member states or have content that would be illegal in most countries with legislation against documented child sexual abuse. CIRCAMP plans to share this list with all INTERPOL member states in the future.

CIRCAMP also works proactively with legal businesses to curb the sources of profit from organized crime and other criminal entities profiting from online child exploitation. Under this program, CIRCAMP places test purchases of child exploitative materials from Web sites and then traces the payment through financial networks until it reaches the exploiter's bank account. While gaining valuable evidence, the test purchases also provide a way to prevent future purchases of online child exploitative materials. Specifically CIRCAMP, in cooperation with the European Financial Coalition, among others, works with banks, credit card vendors and other financial institutions that these test purchases travel through to ensure that the systems are no longer available to child exploiters and other criminals.

The level of cooperation in CIRCAMP is quite extensive. The CIRCAMP network has its own coordination Web site and holds two to three annual meetings to monitor progress and revise

---

decision of the police. For an example of how NGOs collaborate with law enforcement to fight online child pornography, see: Albinsson, M. "Visual Route Helps Save the Children." *Law & Order* 50(12):39-42.

[7] The Domain Name System is a registry of Web sites on the Internet. It translates URLs into Internet Protocol addresses so that networked computers can provide the information that users want to view. Put another way, the system is the phone book for the Internet.

action plans. Action plans contain goals and objectives as well as measures that can indicate levels of achievement. As noted earlier, cooperation goes beyond the law enforcement arena and includes both private sector firms and NGOs. CIRCAMP also files two progress reports annually, which will soon contain performance measures.

Criticisms and Concerns Regarding CIRCAMP

Some concerns about CIRCAMP arose during the study. A minor concern was the scope of CIRCAMP. Thus far, CIRCAMP has only focused its attention on Web sites and has chosen not to address other avenues for distributing online child exploitative materials. Although it is hard to estimate how many child exploitation files are transferred via Web sites as opposed to other mechanisms like peer to peer (P2P), numerous studies nonetheless point to the increasing popularity of the P2P environment. CIRCAMP does not ignore this problem and has made efforts to expand its focus. For example, CIRCAMP is now exploring other mechanisms for accessing the Internet, such as mobile phones. In the end, CIRCAMP is trying to better police one section of cyberspace, and thus, if the ability to distribute child exploitative materials via Web sites was significantly degraded, then CIRCAMP could turn its attention to P2P and other avenues of distribution.

A second issue with CIRCAMP is the resources required to operate it. Individual member states reported varying degrees of difficulty in establishing and maintaining the filters and other programs that comprise CIRCAMP. For example, starting up the filtering program was a major time investment. The agency had to obtain legislative authorization for the program, approach each ISP to obtain their participation and then build and maintain a list of filtered sites for the ISPs to implement. The agency also sometimes had to work with technologists at each of the ISPs to ensure the filtering software was enacted. Participation in CIRCAMP requires a commitment of personnel time and is not something that can be done on a part-time basis. However, once filtering and other programs are put into place, the time and resource commitments for CIRCAMP drop dramatically, apart from the time required to maintain the blocked list.

Last, the filtering program and the concept of filtering in general have brought on a series of criticisms. The most frequent criticism is that outside experts are not able to evaluate the program and judge its effectiveness. Since it is currently not possible to measure the volume of online child exploitative materials, it is not possible to evaluate the true impact of filtering. While logs can collect a range of information about hits against a filter, without the larger context of the extent of child exploitation these numbers are not useful for evaluation. A number of entities have latched onto this and other arguments to argue against the use of filtering. But a deeper concern lies in the act of filtering itself. A range of organizations have registered their displeasure with governments censoring, filtering or otherwise controlling the content of the Internet. While some of these organizations ground their arguments in constitutional protections afforded child exploiters, the more common arguments against filters are that they can be easily manipulated, can be expanded to deny protected speech online and often deny access to legitimate content on the Internet. CIRCAMP has attempted to address these concerns. Most of the member states have formal memorandums of understanding with the ISPs that state that neither party can filter Web sites that do not contain online child exploitation material.

Moreover, CIRCAMP has established an anonymous reporting device so that citizens can lodge a complaint when they feel a Web site is unfairly blocked by the filter.

Findings

The study found that CIRCAMP has made good progress in each of its program elements and is meeting all of its goals. It has successfully coordinated the efforts of its member states. The CIRCAMP network has made steady progress in its three core program elements — the CSAADF filter, the analysis of child exploitative Web sites and the cooperation with the private sector. The coordination among member states in each of these areas is both real and robust. Moreover, while some criticisms of CIRCAMP arose, most were constructive and already under consideration within the CIRCAMP network. As a result, CIRCAMP has made concrete and measurable results towards meeting its goals and has advanced European efforts to fight online child exploitation.

CIRCAMP's Progress in Meeting Its Program Elements

The CIRCAMP network provides a forum to discuss hurdles, identify best practices and obtain legal and technical assistance.[8] For example, privacy concerns and legal codes have in some cases served as a barrier to full implementation of the filter among CIRCAMP member states. As of its business meeting in May of 2009, there were five member states that were not operating filters. Although two of the five member states are implementing the filtering program shortly, the other member states have no plans to filter due to a lack of political will and to concerns about the privacy of Internet users. This has led to CIRCAMP adopting not one but two ways to achieve progress on implementing the filter. Some member states have their law enforcement agencies maintain and update the list of filtered sites. Following the lead of Norway, these states prefer to have law enforcement officials confirm the presence of child exploitative materials on a Web site before it is added to the blocking list. Other member states prefer not to have their governments involved in filtering the content of the Internet and so they turn to NGOs to generate the blocked list. For example, the U.K. asks the Internet Watch Foundation, an NGO, to maintain the list of blocked sites and provide the list to law enforcement and ISPs.

The case of the Netherlands reflects how CIRCAMP's flexibility has met with success in implementing the filtering program. The Netherlands began filtering Web sites hosting child exploitative materials in April of 2007, following an early 2006 Dutch Lower House decree requesting the Minister of Justice to filter "child pornographic" material. Dutch law enforcement obtained the cooperation of three ISPs in the Netherlands. Six months after its implementation, the Dutch Ministry of Justice commissioned a report evaluating the filter.[9] The report stated that the Ministry could not evaluate the impact of filtering on the distribution or consumption of child exploitative materials online. Moreover, the report noted that only a statutory law could authorize the program because it impinged on the privacy of Internet users according to both European and Dutch constitutional rights. The Lower House decree was deemed an insufficient legal basis for the program, and the result was the suspension of the filtering program. However,

[8] States that are not members of CIRCAMP but are interested in implementing a filtering program can also seek out CIRCAMP's assistance.

[9] See Stol, W. et al. "Governmental Filtering of Websites: The Dutch Case." *Computer Law & Security Review* 25(2009):251-62 for an English-language summary of the report.

the Netherlands plans to restart the filtering program in 2010 based on the U.K. model and is working to bring NGOs and the private sector together to implement the program.

The flexibility seen in CIRCAMP also helps it in its relationships with the private sector. Some member states reported that their ISPs were reluctant if not hostile to the idea of filtering the Internet, regardless of the merits of such programs, for reasons that included protecting the privacy of consumers, avoiding regulation of the Internet and safeguarding the freedom of speech. This falls in line with a number of NGOs that are dedicated to preventing any regulation of the Internet. Other ISPs were reluctant to implement filtering for international Web sites since they were unsure if their companies had "jurisdiction" beyond national borders. In those countries that have implemented filtering, however, the ISPs have ranged from agnostic to enthusiastic about the program. An interview with one of the more active ISPs in a member state currently filtering the Internet as a part of the CSAADF program revealed that, despite the initial concerns that their legal counsel held regarding the idea, this ISP enacted filtering in light of its corporate social responsibility. Put simply, the ISP felt that its responsibility to help law enforcement prevent the revictimization of exploited children through online child abusive materials outweighed any potential trampling of constitutional rights.[10] To date the ISP has not been sued, even though it handles over 50 percent of the Internet traffic in its country and blocks over 15,000 potential Web site visits daily. The ISP is currently looking to expand its filtering agreements with other countries globally, especially those in Asia.

The most significant pieces of evidence supporting the progress of the filtering program are found in the statistics CIRCAMP has collected. First are raw numbers of what the filtering program has been able to block since its inception. According to CIRCAMP, just one member state's filtering program has blocked nearly 3 million attempts to access child exploitative host sites, an average of nearly 30,000 per day. This has included some 39,142 unique images of child exploitation totaling 7.4 gigabytes of data. Given that pictures are often measured in hundreds of kilobytes, this is a significant number of images blocked. So while these numbers are not directly translatable to successful interdiction, they indicate the robust nature of the filter presently.

The other central thrust of CIRCAMP is the development of a more robust working arrangement with banks and other value transfer systems to deny child exploiters the ability to profit from online sales. In Sweden, for example, the police will attempt to locate a payment system after they identify a Web site hosting online child exploitative materials. If they do, they then turn to the financial community to ensure that these sites are no longer able to use the Swedish banking and financial sectors to profit from sales. CIRCAMP has also begun conducting "test purchases" of child exploitative materials from Web sites to track the flow of money from the purchase to the exploiter's home bank account, noting the links in the chain between, and working with the financial institutions to deny exploiters future access to any sites that host child exploitation materials.

[10] The Groupe Speciale Mobile association, the world's largest trade association for mobile communications, supports the filtering of Web content to remove online child exploitation materials. For more on the Mobile Alliance against Child Sexual Abuse Content see http://gsmworld.com/our-work/public-policy/protecting-consumers/mobile_alliance.htm.

Last, CIRCAMP is making progress constructing and analyzing patterns of distribution and consumption of online child abusive materials. The CIRCAMP network maintains an online collaborative space that is secure and easily accessible to all of its members. When a member state identifies a Web site hosting online child exploitative materials, the state can notify other member states and post the evidence on the collaborative site. Member states can then review the evidence and add to the case file as needed. The CIRCAMP network is also supporting the analytical efforts of EUROPOL and INTERPOL.

CIRCAMP's Progress Towards Meeting Its Goals

The steps forward that CIRCAMP has taken in its programs have translated into tangible progress towards meeting its goals. The filtering program has shown signs of successfully disrupting the distribution of online child exploitative materials and of fostering a common understanding of how to police the Internet. For example, an analysis of the traffic to sites CIRCAMP is blocking shows that traffic from those countries participating in the filtering program has dropped precipitously. Indeed, the analysis demonstrates that rates of distribution and consumption of online child exploitation have trended downward after member states have implemented the filtering program.

A separate analysis of one member state showed that the largest percentage of users (33 percent) originated in the U.S., followed by Germany. Those with some of the lowest shares were the CIRCAMP member states that have implemented filtering programs. Moreover, 50 percent of the blocked domains are hosted on computers located in the U.S. In raw terms, the U.S. hosts 1,148 blocked domains while the next closest country, Germany, hosts 199 domains. It is worth noting, however, that these numbers are in part a function of the fact that volume of hosted domains in the US is far larger than those in Germany.

Cases against online child exploitation have resulted from CIRCAMP member states participating in the network, further suggesting progress towards its goals. While the absolute number of cases is low, this belies the emphasis on CIRCAMP as a multinational network as opposed to a task force. The cases that CIRCAMP has pursued have often tapped the collaborative network that CIRCAMP supports. Moreover, the evidence collected from the partnership with financial institutions has also proven valuable in member state investigations.

Implications for U.S. Agencies

CIRCAMP offers a comprehensive approach to online child exploitation that deserves the attention of U.S. law enforcement communities. The coordination of law enforcement agencies across jurisdictions and the collaboration of public and private entities provide a way to leverage scarce resources against online child exploitation. Linking the public and private sectors further expands the effectiveness of the combined efforts of these states. Overall, CIRCAMP is making sure progress towards its goals through a collaborative approach to reduce online child exploitation.

Online child exploitation remains a serious and pressing problem for federal, state and local law enforcement in the U.S. As with any cross-border issue, management and coordination of resources are key requirements of any successful response. The breadth of the problem is

significant, crossing numerous U.S. jurisdictions and international borders, and it is one of a growing multitude of such criminal acts that compete for resources. But the cross-border nature of online child exploitation also ensures that any one case will involve two or more law enforcement agencies and at least as many private entities such as ISPs or financial institutions. Thus, significant coordination among a variety of actors within and outside the law enforcement community is key to a successful response.

The public-private partnership approach of CIRCAMP offers U.S. law enforcement a comprehensive and coordinated model for responding to online child exploitation. Parts of the CIRCAMP approach already exist in the U.S. The Internet Crimes Against Children task forces are similar to CIRCAMP in that they attempt to foster multijurisdictional cooperation and train local investigators to better recognize online child pornography cases. The ICAC program is a national-level effort limited to cases generated from the U.S. The U.S. Department of Justice's Project Safe Neighborhoods. largely builds on the ICAC task forces, but focuses on public awareness.

Likewise, the International Center for Missing and Exploited Children (ICMEC) leads an effort known as the Financial Coalition Against Child Pornography (FCACP).[11] Established in 2006, the goal of FCACP is to eradicate the commercial viability of child pornography by following the illicit flow of funds and shutting down the payment accounts that are being used by these illegal enterprises. The program relies on the well-established CyberTipline, run by ICMEC's sister organization, the National Center for Missing and Exploited Children (NCMEC), and expands it by allowing financial institutions to access the list. Armed with this information and training from ICMEC, members of the FCACP are better positioned to deny transactions funding child pornography.

Finally, a number of U.S. state governments have expressed an interest in or implemented filtering programs for online child exploitation. In June of 2008, New York State reached agreements with large ISPs such as Verizon, Sprint and Time Warner Cable to block access to child pornography and delete existing images from their servers based on the NCMEC CyberTipline list.

In sum, the CIRCAMP model offers U.S. law enforcement agencies seeking to improve their efforts against online child exploitation a road map for moving forward. The combination of interagency coordination, technology use and coordination with the private sector has proved to be an effective approach to combat online child exploitation. CIRCAMP's willingness to provide both technical and policy advice to U.S. law enforcement agencies is a further enticement to trying this program in the U.S.

[11] For more, see: http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3703.

Appendix

Example CSAADF Warning Page (Norway)