


[send to a friend](#) 

Cyber Training and Technical Assistance

By Denise E. O'Donnell, Director, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice



The Internet has revolutionized the ability worldwide to not only communicate, but also share all types of information. Unfortunately, these capabilities are also available to the modern-day criminal. These changes, generally considered good, have created a new, darker methodology for crimes to be committed by anyone with a computer, a cellphone or smartphone, a connection to the Internet, and a bit of technical expertise. The landscape is constantly evolving, and the responsibility to enforce the law and protect citizens has created a tremendous need for additional training and tools for law enforcement. Officials need to not only identify these types of crimes, but also have the tools, capabilities, and specialized skills to collect evidence, investigate, and assist with the prosecution of cybercrimes. Adding to the

complexity of many of these crimes is the reality that a suspect may not be in that the official's jurisdiction, let alone the same state, or even the same country.

In October 2012, Richard McFeely, Executive Assistant Director of the Federal Bureau of Investigation's (FBI's) Criminal, Cyber, Response, and Services Branch, confirmed the concerns about the use of the Internet and computers when he stated, "It's important that everybody understand that if you have a computer that is outward-facing—that is connected to the web—that your computer is at some point going to be under attack....You need to be aware of the threat and you need to take it seriously."¹ Director of National Intelligence (DNI) James Clapper echoed the same concerns when he testified before the Senate Select Committee on Intelligence in March 2013. As part of his testimony, he stated that those meaning to do the United States harm are increasingly gaining "cyber expertise," which they use "to achieve strategic objectives by gathering sensitive information from public- and private-sector entities, controlling the content and flow of information, and challenging perceived adversaries in cyberspace."²

As a former federal prosecutor, I understand and appreciate the crucial role the FBI, Department of Homeland Security (DHS), DNI, and the entire intelligence community play in protecting the United States from cyber threats. However, while federal agencies are uniquely situated to respond to international cyberthreats that are often

behind and linked to many cybercrimes at the local level, this battle is not just at the federal level. As with many other types of crime, it is the men and women who make up the state, local, tribal, and territorial public safety communities who are on the front line facing the challenge presented by cybercrime every day. The contributions they make cannot be overstated.

The term *cybercrime* is frequently used to cover a wide range of criminal activity and sometimes creates confusion. The term *cyber* can encompass identity theft and fraudulent schemes; cyber bullying or stalking; computer hacking; system intrusions; denial of services; and even espionage and terrorism. Because the term is so broad, experts have suggested using the term *cybercrime* with appropriate modifiers to differentiate the type of crime or intrusion and the required law enforcement response or action, such as cyber investigation and forensics, cyber infrastructure protection, cyber intrusion, and so forth. The use and consistent application of such terms would help everyone better understand the various dimensions of the cybercrime challenge and help us speak a common language in coordinating our activities. As we enhance our national capability to respond to the cyber challenge, speaking a common language is only one challenge; building expertise and capacity through training and technical assistance and coordinating our nations's resources and law enforcement response is another. We are collaborating with FBI, DHS, International Association of Chiefs of Police (IACP), and other federal, state, local, and tribal partners on these types of issues.

To specifically address these needs, the Bureau of Justice Assistance (BJA) is proud to be partnering with the IACP on the Law Enforcement Cybercrime Resource Center to help identify training, resources, tools, and technical assistance to assist law enforcement in developing the expertise necessary to meet the cybercrime challenge. The project will be a web-based portal designed for law enforcement officials to ask simple questions and get specific answers with a list of resources, no matter what level of technical experience the requestor may have.

With continued strains on law enforcement budgets, it is also important for us to work together to enhance the ability of law enforcement officers to prevent and respond to cybercrimes, intrusions, and attacks. BJA has been a leader in this area for a number of years. Since 1995, BJA has provided training, resources, and technical assistance to law enforcement to develop the technical and forensic capacity to deal with electronic crime. Over the past five years, BJA providers like the National White Collar Crime Center (NW3C) and SEARCH have offered free technical training to over 35,000 officers.³ These classes include basic and advanced training for cyber investigations, forensics, data recovery, digital evidence collection, intrusion investigations, financial crimes, and classes for intelligence analysts. Many of these trainings have been offered regionally, reducing an agency's need to travel, thereby lowering costs and reducing time officers are away from the job. Feedback from participants continues to stress the need for training and resources and has highlighted the need to provide basic training online.

In 2010, we addressed the use of handheld devices with Drakontas and Drexel University. The focus was to provide law enforcement officers with basic knowledge of handheld electronic devices they may encounter and how they could find vital information for their investigations. This self-paced online class allows officers with varied technical experience to gain valuable knowledge. The response to that class has been so well received that some states are considering requiring this class for their officers.

Another project created in partnership with the Fox Valley Technical College, National Criminal Justice Training Center (NCJTC), provides online training for small and rural law enforcement and prosecutors in the area of cyber investigations. This project supported the development of a series of webinar events, distance learning modules, and roll-call videos for officers and prosecutors.

Jurisdictional challenges are another unique element of cybercrimes. Determining which agency should gather evidence and investigate, as well as identifying the proper jurisdiction for the investigation and prosecution, presents new challenges. As with other criminal cases, when elements of the crime cross state lines or international borders, the need to involve federal agencies is often essential. In recognition of this problem, BJA has leveraged resources by partnering with the Global Justice Information Sharing Initiative (Global), a federal advisory committee to the U.S. Attorney General on justice information, and by convening a Cyber Task

Team under Global's Criminal Intelligence Coordinating Council (CICC). CICC brings leaders from diverse agencies together to examine facts and make recommendations on how to best address electronic-based crime. It also plays a role in helping to identify agencies' roles and responsibilities, the appropriate interaction needed between agencies, and the resources that can be provided to state, local, and tribal law enforcement.

BJA's National Training and Technical Assistance Center (NTTAC) offers additional resources for criminal justice and law enforcement officials and works to facilitate the delivery of high-quality, strategically focused training and technical assistance (TTA) to achieve safe communities nationwide. BJA NTTAC-provided assistance covers a broad set of topic areas including training, information dissemination, technical assistance, and facilitation of multi-agency and cross-jurisdictional teams and working groups. This extends to the area of cybercrime training (for investigations and forensics), awareness, and possibly technical assistance. Public safety agencies and their members can get additional information at <https://www.bjatrainng.org>.

BJA looks forward to continuing to support our partner agencies and organizations in this crucial arena. We applaud the leadership of IACP Executive Director Bart Johnson and IACP board members, who have demonstrated a willingness to help elevate this issue and ensure it receives the consideration it demands through the creation of the Law Enforcement Cybercrime Resource Center. By working together, with everyone's support, we can lead efforts to help address these critical challenges. ♦

Notes:

¹"Cyber Security: Focusing on Hackers and Intrusions," FBI press release, October 26, 2012, <http://www.fbi.gov/news/stories/2012/october/cyber-division-focusing-on-hackers-and-intrusions> (accessed November 12, 2013).

²James R. Clapper, "Worldwide Threat Assessment," *Ambassadors Review* (Spring 2013), <http://www.americanambassadors.org/publications/ambassadors-review/spring-2013/worldwide-threat-assessment> (accessed November 12, 2013).

³National White Collar Crime Center (NW3C) can be accessed at <http://www.nw3c.org>; SEARCH can be accessed at <http://www.search.org>.

Please cite as:

Denise E. O'Donnell, "Cyber Training and Technical Assistance," From the Director, *The Police Chief* 80 (December 2013): 20–21.

[Top](#)

From *The Police Chief*, vol. LXXX, no. 12, December 2013. Copyright held by the International Association of Chiefs of Police, 515 North Washington Street, Alexandria, VA 22314 USA.

[Return to Article](#)

[send to a friend](#) 

The official publication of the International Association of Chiefs of Police.

The online version of the Police Chief Magazine is possible through a grant from the IACP Foundation. To learn more about the IACP Foundation, [click here](#).

All contents Copyright © 2003 - 2014 International Association of Chiefs of Police. All Rights Reserved.
[Copyright and Trademark Notice](#) | [Member and Non-Member Supplied Information](#) | [Links Policy](#)

515 North Washington St., Alexandria, VA USA 22314 phone: 703.836.6767 or 1.800.THE IACP fax: 703.836.4543
Created by [Matrix Group International, Inc.®](#)