PRIORITY Criminal Justice NEEDS INITIATIVE

A project of the RAND Corporation, the Police Executive Research Forum, RTI International, and the University of Denver

Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web

Sean E. Goodison, Dulani Woods, Jeremy D. Barnum, Adam R. Kemerer, Brian A. Jackson

EXECUTIVE SUMMARY

Historically, most crimes have taken place in a single jurisdiction, meaning that most of the evidence and witnesses necessary to solve them were usually in the vicinity of the investigator. However, as criminal activity increasingly moves online, the nature and location of evidence has changed. Some online criminal activity relies on the *dark net*, a portion of the internet that uses encryption and anonymizing technologies that are intentionally designed to frustrate tracking efforts.

For this effort, we define the *dark web* as the hyperlinked services on the dark net that can only be accessed using The Onion Router (or Tor) protocol or other equivalent technologies (e.g., https://3g2upl4pq6kufc4m.onion/, which is DuckDuckGo.com's dark web site). The online marketplaces on the dark web are functionally similar to eBay or Amazon. Payment typically is handled through the use of digital currencies (e.g., Bitcoin, Litecoin) and escrow services. When crime occurs in traditional online forums, it often leaves a trail of data that can be followed. On the dark web, however, the process of collecting those data and turning them into evidence can be difficult. To ensure that they are able to effectively perform their missions, law enforcement agencies need to be able to follow leads and conduct investigations seamlessly between the physical and digital worlds.

In 2015, researchers at Carnegie Mellon University estimated that dark net markets accounted for $100 million to $180 million per year in total sales volume (Soska and Christin, 2015; Greenberg, 2015). By 2017, the same researchers estimated that one site's (AlphaBay's) sales volume had grown to roughly $219 million per year, indicating significant growth ("Police Ran 2nd . . . ," 2017). It is important to remember that not all dark net transactions are illicit; however, because of the increasing number of illicit transactions, the dark web is now drawing the attention of law enforcement agencies. To explore the needs of state and local law enforcement to address crime on the dark web and dark net, the RAND Corporation and the Police Executive Research Forum (PERF) convened a day-and-a-half workshop with

PRIORITY NEEDS

RESULTS

- Investment is needed in training at all levels, from the most-junior to the most-senior officers. The junior levels need to know what everyday artifacts might be relevant to an investigation and the senior levels need to ensure that the necessary skills and knowledge are included in officer and investigator training curricula.
- Investment in efforts aimed at improving information sharing is needed across agencies, both within the United States and across international borders.
- There is a need to examine the benefits of investing further in existing, proven cross-organization structures that are designed to facilitate cooperation and information sharing.
- Standards organizations should develop new testing standards for forensic tools that are employed to collect evidence on computers that have been running dark web software.
- Research should be conducted into opportunities for modernizing laws associated with inspecting packages transmitted via the U.S. mail and similar services.
- Research should be conducted into the increasingly interconnected nature of crime and criminals to ensure that law enforcement is able to focus on both the highly visible tip of the iceberg (i.e., traditional crime) and the less visible—but extremely important—portion of the iceberg (i.e., cybercrime) that has the potential to affect the health and welfare of populations both near and far.

practitioners from federal, state, and local law enforcement and researchers with expertise in cybercrime. The panelists' discussions covered the following topics: general challenges, including globalization and training; technical challenges, including anonymity and access, suspect identification, and resource allocation; and legal challenges, including the multijurisdictional nature of these types of crimes.

During the discussions, the panel members identified 40 problems or opportunities and 46 potential solutions (or needs) that they felt could benefit from additional investment in research and development. At the end of the workshop, the panelists prioritized the problems and opportunities they identified. Taken together, the high-priority needs identified during the workshop represent a way to prepare law enforcement at all levels to better address the challenge posed by cybercrime, now and into the future.

WHAT WE FOUND

An expert panel of law enforcement practitioners, academic researchers, and civil rights advocates generally agreed that research initiatives targeted at improving training and information sharing are likely to have the greatest impact on the new problems posed by criminal activity on the dark web.

Lack of knowledge about what the dark web is and how criminals have begun to leverage it is a key problem. Investigating officers often overlook physical artifacts that are indicative of dark web activities when collecting evidence during a criminal investigation. These artifacts might include cryptocurrency wallets, encryption keys, or dark web addresses.

The anonymity and encryption associated with dark web activities make it much more difficult for investigators to assemble the evidence puzzle and prove that a crime has been committed.

Lack of knowledge about what the dark web is and how criminals have begun to leverage it is a key problem.

PARTICIPANTS

Jonathan Birk
Instruq.co

Andrew Crocker
Electronic Frontier Foundation

Jared Der-Yeghiayan
ICE I Cyber Crime Center

Frederick Fife
New Jersey Regional Operations Intelligence Center

Ahmed Ghappour
Boston University

Kristine Hamann
Prosecutors' Center for Excellence

Chris Kenagy
Portland Police Bureau

Mark Kruger
Portland Police Bureau

David Muehl
Milwaukee Police Department

James Nolette
Fayetteville Police Department

Giacomo Persi Paoli
RAND Europe

Quovella Spruill
Essex County Prosecutor's Office

Zev Winkelman
RAND Corporation

Michael Yu
Montgomery County Department of Police

INTRODUCTION

When modern communications technologies, such as the internet, are used by criminals to facilitate their activity, savvier criminals seek out tools that help them mask their activities and communications. Because communicating via dark web technologies incorporates encryption and anonymity by default, criminals increasingly have been relying on the dark web to evade law enforcement as they plan and execute criminal activity (Finklea, 2017). As of 2019, dark web markets, or cryptomarkets (i.e., those using dark web encryption), make up a small percentage of the illicit transactions carried out online ("Police Ran 2nd . . . ," 2017). However, these markets continue to grow in size and scope. Furthermore, such markets present unique problems for law enforcement agencies—especially those at the state and local levels—as they investigate crimes including illicit substance sales and arms trafficking.

Given the novelty of dark web markets and their recent proliferation, many agencies struggle to carry out their law enforcement missions when evidence of the crimes they are trying to prevent or prosecute exists within the dark web. To better understand these challenges, the RAND Corporation and the Police Executive Research Forum (PERF), on behalf of the National Institute of Justice (NIJ), convened a workshop to bring together a diverse group of practitioners and researchers to identify the highest-priority problems and potential solutions related to evidence on the dark web. The focus was on developing an actionable research and development agenda that will enhance law enforcement's ability to understand and investigate illicit activity on the dark web. In this report, we discuss the challenges inherent in dark web investigations and summarize the high-priority needs identified at the workshop.

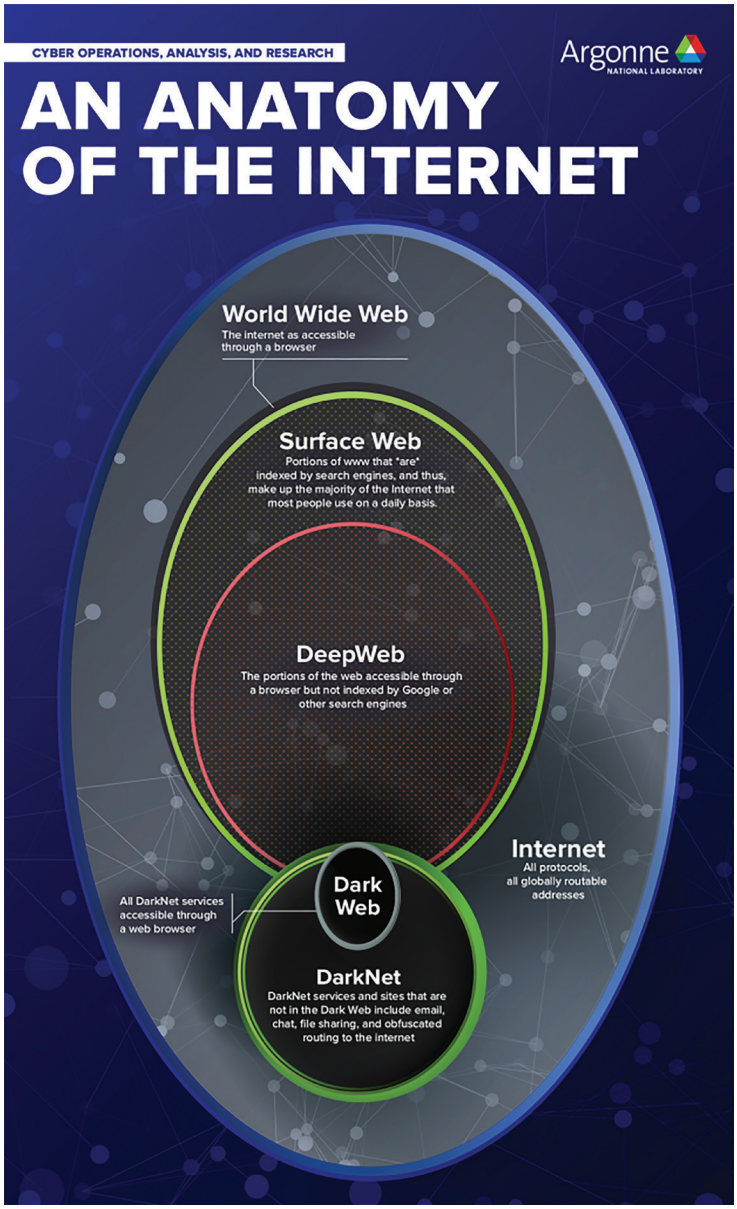
Background

Historically, individual crimes have taken place in a single jurisdiction, meaning that most of the evidence and witnesses necessary to solve them were usually in the vicinity of the investigator. However, as criminal activity moves online, the nature and location of evidence has changed. Cybercrime often leaves a trail of data that can be followed, but the process of collecting those data and turning them into evidence is not always straightforward and can be quite difficult. Often, the location of the evidence can be ascertained, but it can be challenging to obtain, particularly when the servers or systems it is located on are not in a neighboring jurisdiction in the United States, but are spread across the world (Vermeer, Woods, and Jackson, 2018). When criminal activity takes place in the portion of the internet that is intentionally anonymized and encrypted to protect that anonymity, the task of gathering evidence becomes even harder.

By design, the internet is a collection of communication networks designed to facilitate a variety of types of information exchange on several different levels (see Figure 1). The internet has a basic infrastructure containing all online activity with two major subdivisions: the World Wide Web and the dark net.

The World Wide Web is the most visible and familiar portion of the internet, and is itself divided into two subsections:

Figure 1. The Relationship Between the Dark Web and the Rest of the Internet



SOURCE: Argonne National Laboratory, undated.

The *surface web* consists of publicly accessible pages of information indexed by search engines and connected to each other using hyperlinks, while the *deep web* represents sections intentionally walled off from public view (e.g., paid content, corporate intranets, banking or health care interfaces) and other limited-access networks (Ciancaglini et al., 2015). Although the exact distribution of the World Wide Web is under debate, there is considerable agreement that only a small percentage is made up of the surface web, meaning the majority of the internet is not fully accessible to the average person.

When information is exchanged between individuals or computers on the open internet and World Wide Web, relatively little effort is required to identify the parties involved via their computers by using the addresses contained on the electronic "envelopes" that surround the information. However, subsets of the network or the activities on it were always obscured from the general public, primarily to safeguard activity that was critical to protect (McCormick, 2013). Although deep web services are not viewable or usable in bulk by the public, the origins and destinations of the traffic and the owners of intermediate servers—and, thus, the responsible parties—can be identified with slightly more effort.

The dark net is the portion of the internet that uses both encryption and anonymizing communication technologies, which are designed to promote anonymity and frustrate organized tracking efforts. Like on the public internet, services on the dark net include email, social media, and websites. Tor is the most popular communication technology of this type and was created in the 1990s by researchers at the U.S. Naval Research Laboratory. The technology was released to the public in 2002 and its original purpose was to conceal the identities of American operatives or dissidents attempting to communicate within oppressive regimes. Tor also is used by journalists working internationally, where internet controls are strict and governments might have an interest in uncovering sources or stopping antiregime stories.

The dark net is the portion of the internet that uses both encryption and anonymizing communication technologies, which are designed to promote anonymity and frustrate organized tracking efforts.

The dark web is made up of the associated hyperlinked services that can be accessed only via obfuscation services using the Tor protocol or other equivalent technologies, allowing access to websites with the domain suffix ".onion" (e.g., https://3g2upl4pq6kufc4m.onion/, which is DuckDuckGo.com's dark web site). These services also use encryption and obfuscation, which—in contrast to the World Wide Web—makes it difficult to identify the location of the servers that are associated with them.

For the average user, access to websites and services on the dark net (and dark web) requires specially configured web browsing systems (e.g., TOR browser, Invisible Internet Project [I2P], Whonix). From the dark net, users can communicate and access services back on the World Wide Web, but their communications are difficult or impossible to trace. For example, accessing a surface website through a surface web browser (e.g., Chrome, Edge, Firefox) allows the website to see the Internet Protocol (IP) address of the user's computer, thereby providing location and operating data for the user; however, accessing the same surface website with a dark web browser displays a false IP address—the user's true IP is masked by a network of relays. In this way, users concerned with surface web tracking or privacy can access sites without direct links to their individual person.

However, as has been the case in other areas of technology and commerce, tools designed for legitimate use can be turned to criminal purposes and therefore draw the attention of law enforcement agencies. In the years since Tor's creation, it has become a means for a wide variety of actors to access the dark web (McCormick, 2013). Such actors include younger gang members in New York City, who access the dark web to obtain financial information and commit identity fraud in lieu of open-market drug sales (PERF, 2018). Although this might be a new area for law enforcement agencies, the technical knowledge required to engage on the dark web is minimal, especially for individuals who have spent their formative years networked together by cell phones; social media; and open, public internet.

As interactions and everyday transactions increasingly have moved online, criminal activities have followed.

For the purposes of this report, the emphasis is on the illegal dark web commerce often connected to criminal investigations.

The online marketplaces that exist within the dark web are similar to eBay or Amazon. Often, they are websites that are accessible only using the Tor protocol. Payment is typically handled through the use of digital currencies (e.g., Bitcoin, Litecoin). In addition, there is often a reputation-tracking system where buyers can rate sellers and leave reviews, which is similar to the online marketplaces found on the public internet. In the early days of public internet use and online marketplaces such as eBay, dark web marketplaces offered escrow services that acted as a third-party intermediary between buyers and sellers. This allowed the seller to deposit their payment with the third party (either the marketplace or another escrow service) and release the funds only after the product was received. In the event of a dispute, the escrow service would evaluate the evidence and decide which party would receive payment (Afilipoaie and Shortis, 2015).

As interactions and everyday transactions increasingly have moved online, criminal activities have followed. In 2015, researchers at Carnegie Mellon University estimated that dark net markets accounted for $100 million to $180 million per year in total sales volume (Soska and Christin, 2015; Greenberg, 2015). By 2017, the researchers' estimate had grown to roughly $219 million per year for only one site's (AlphaBay's) sales, indicating significant growth ("Police Ran 2nd . . . ," 2017). By one estimate, 57 percent of the websites on the dark web are designed to facilitate illicit activity (Moore and Rid, 2016). This implies that 43 percent of the sites—and, potentially, the other activities—might not be related to individuals who are interested in crime. Rather, such sites might be for individuals with a keen interest in having secure, private conversations and conducting private transactions, such as journalists and political dissidents (Peralta, 2015).

In 2016, RAND Europe researchers estimated that the three largest dark web marketplaces represented approximately 65 percent of all cryptomarket listings (Kruithof et al., 2016). Researchers have found that the majority of dark web vendors typically sell relatively small retail quantities of narcotics and a smaller number engage in wholesale operations. The researchers at Carnegie Mellon University examined 35 markets and more than 1,900 snapshots of activity across multiple years, finding that about 70 percent of the sellers sold less than $1,000 worth of products, while only 2 percent sold more than $100,000 worth (Soska and Christin, 2015; Greenberg, 2015). RAND Europe researchers found that a large majority of drug market transactions on cryptomarkets were for listings under $100; however, they also found that large sales approached one-quarter of overall cryptomarket drug revenue at specific points in 2013 and 2016, suggesting that the dark web might be a source for drug dealers buying stock for offline distribution (Kruithof et al., 2016). Sales of firearms on the dark web make up approximately 0.5 percent of the total listings, and researchers surmise that the limited scale of firearms transactions might make dark web firearms markets more viable for small groups as opposed to larger criminal organizations (Persi Paoli et al., 2017).

At the federal level, the Federal Bureau of Investigation's (FBI's) 2013 takedown of the Silk Road dark web marketplace is one of the best-known cases of police response to large-scale online illicit activity. More recently, a collaborative effort among the FBI, U.S. Immigration and Customs Enforcement's (ICE's) Homeland Security Investigations (HSI), the U.S. Drug Enforcement Administration (DEA), the Dutch National Police, and Europol resulted in the closure of AlphaBay and Hansa, two prominent dark web marketplaces that were responsible for hundreds of thousands of listings for illicit drugs, fraudulent documents, and other illegal materials (Europol, 2017). These operations, which were called "the largest dark net marketplace takedown in history" by former U.S. Attorney General Jeff Sessions, involved long-term covert monitoring of criminal activities (quoted in "Police Ran 2nd . . . ," 2017). This led to the arrest of site administrators and the collection of both buyer and seller information, which was then passed on to local police (Europol, 2017). In January 2018, Sessions announced the creation of the Joint Criminal Opioid Darknet Enforcement (J-CODE) team, which would assign more resources to combat dark web opioid sales through additional special agents, intelligence analysts, and other professional staff (U.S. Department of Justice, 2018). In addition to such large-scale operations, state and local agencies have been involved in collaborative efforts to identify and apprehend

> When crime moves online, agencies need to be able to follow leads and conduct investigations seamlessly between the physical and digital worlds.

individual sellers—including the arrest of "Peter the Great," who was responsible for nearly 10,000 illicit drug transactions, in an investigation spearheaded by the Portland, Oregon, Police Bureau (PERF, 2018).

Dark web marketplaces are a new variant of the more-traditional street-level black market drug sale operations that law enforcement agencies have been dealing with for years. From the perspectives of the buyer and seller, there are several advantages gained from moving their illicit transactions to the dark web. Buyers believe that they are much more likely to get a quality product because of the rating systems of the online marketplaces (Buxton and Bingham, 2015). Sellers believe that they are at less risk of being caught by law enforcement or that they do not have to deal with violent individuals on the street (Van Hout and Bingham, 2014). Of course, the marketplaces themselves often are targeted by law enforcement agencies. When law enforcement shuts down a dark web, it tends to create displacement, and new sites are made to fill the void. In many ways, this is similar to traditional gang or drug operations, especially when there is a true market force at play (i.e., demand for a service that is being provided). However, there are still benefits to these dark web shutdowns. First, access to the marketplace records allows for potential identification of major players in illegal activity. Also, a shutdown provides a degree of temporary relief as users scramble to change their activities, whether they desist using the marketplace out of fear of apprehension or slowly rebuild their reputation on another marketplace (thereby limiting the scale or scope of products being moved). This transition period allows law enforcement to monitor discussion forums for new intelligence on where users are migrating, what additional steps are being taken to maintain anonymity, and whether users understand the full scope of law enforcement's reach.

Since 2017, the dark web has attracted more attention from state and local law enforcement agencies. For example, during the October 2017 International Association of Chiefs of Police annual meeting, a large audience discussion and smaller panels were held to discuss the dark web and policing. Earlier, in August 2017, PERF held a meeting on the unique challenges of modern criminal investigations, particularly the challenges of illegal activities on the dark web. Discussions at this meeting focused on current strategies used by state and local police departments to investigate dark web drug sales, the challenges in conducting these types of investigations, and the variety of issues agencies expect to face in keeping pace with illicit dark web activity in the coming years (PERF, 2018).

When crime moves online, agencies need to be able to follow leads and conduct investigations seamlessly between the physical and digital worlds. This creates challenges for officers, who might not be trained to make the needed connections. Even recognizing when a more traditional crime, such as drug trafficking, is relying on dark web or related technologies can be difficult. Failing to recognize this connection risks missing investigative leads that could not only clear single cases but also disrupt larger-scale criminal enterprises. Although the use of the dark web to facilitate fentanyl sales has been a major gateway for U.S. law enforcement interest in these hidden marketplaces, given the current opioid epidemic, some agencies are warning of other potential illegal activities that are possible through the dark web, such as identity theft, weapon sales or blueprint distribution, hacking tools, and human trafficking (PERF, 2018). Preparing law enforcement to address these issues requires identifying the tools, training, and approaches needed and promoting their adoption across the country, followed by rigorous research to validate approaches.

WORKSHOP DISCUSSION

To explore the needs of state and local law enforcement to address crime in the dark web and dark net space, RAND and PERF researchers convened a workshop of practitioners from federal, state, and local law enforcement supported by researchers with expertise in cybercrime. Through structured discussion, the group identified (1) potential solutions to current problems encountered by law enforcement investigating this type of crime and opportunities to improve effectiveness going

forward; and (2) future needs, including tactics, techniques, new tools, and the difficulties that dark web investigations present, while keeping in mind the citizenry's rights to free speech, free association, privacy, and due process. The experts' commentary stems from years of experience and reflects the perceptions and challenges of conducting investigations with a dark web component, particularly because law enforcement at large is only beginning its exposure to this area. For example, one identified need was demystification and additional training; policing in the aggregate requires solutions, the panel members themselves did not feel mystified or inadequately trained.

Solutions include research and development opportunities as they relate to U.S. law enforcement technologies. Needs also can include changes in policy, changes in practice, training, or further research that could improve law enforcement agency performance and promote more-effective use of existing resources. In this report, we summarize the workshop discussions and present solutions along with the highest-priority needs identified, supplemented with additional research. Workshop participants highlighted some existing and emerging challenges in investigating leads on the dark web that could be addressed by future collaboration with the research community.

In advance of the meeting, the panel members were asked to complete a questionnaire and identify the most-significant challenges in several areas. Their responses were used to inform the workshop agenda. A summary of the challenges and the most common responses is presented in Table 1.

The workshop began with introductions and a description of the task at hand. Then, panel members were led through a discussion in which they considered the problems and challenges facing their agencies. The discussion was structured around the following seven themes:

1. top needs and challenges
2. crime identification
3. suspect identification
4. evidence identification

Table 1. Top Challenges and Opportunities, by Category

Category	Problem or Opportunity
Challenges in conducting investigations	• Among those charged with conducting investigations, there is limited literacy related to information technologies. • There is little officer knowledge about the subject matter. • Cross-jurisdictional coordination among investigators from law enforcement agencies is lacking (e.g., information sharing, intra-U.S. cooperation, international law enforcement cooperation).
Significant legal challenges	• It is challenging to determine the jurisdiction when a crime is detected or suspected (e.g., Does the investigator have jurisdiction? Is the jurisdiction where the victim is located, where the suspect is located, or where the various servers and storage are located?). • There are problems with evidence obtained by taking advantage of known weaknesses in software and installing exploit software on suspect computers. (This approach often is called "using network investigative techniques.")
Significant technical challenges	• Maintaining familiarity with existing and new tools and skills (including new software exploits) is difficult.
Significant civil rights challenges	• It is difficult to clearly identify the suspect and avoid nonadmissible (and potentially illegal) mass surveillance techniques. • Ensuring that warrants, searches, and other investigative techniques focus only on the suspect is a challenge. • It is difficult to preserve the privacy of nonsuspects, especially in situations where a machine has been used by multiple individuals (e.g., relative, in a public library).
Potential opportunities	• More cooperation is possible with service providers whose systems might contain valuable evidence (e.g., internet service providers, web hosting services, cloud service providers). • More-thorough investigations of crimes that do not appear to have a connection to the dark web (e.g., drug overdoses) are possible. • Patrol-level officer training could be created to identify digital artifacts[a] during more-traditional responses (e.g., domestic violence).

[a] *Digital artifacts* refers to items found in the physical world that might indicate connections to the digital world. Such artifacts include account names, email addresses, encryption keys, digital wallet addresses (e.g., Bitcoin), and associated key identifiers.

5. evidence preservation, access, and collection
6. evidence quality and provenance
7. evidence presentation.

At the conclusion of the workshop, participants had the opportunity to raise issues they thought had been missed in the course of the topical discussions. After examining the topics actually discussed during the workshop, we recategorized the aforementioned themes into six overarching topics: general needs and challenges; technical needs and challenges; crime identification; suspect identification; evidence identification, access, and preservation; and legal needs and challenges. Evidence quality and provenance and evidence presentation did not produce any significant discussion or needs and, as a result, were removed. New themes emerged with regard to working across jurisdictions and respecting civil rights. In the following sections, we summarize topics discussed at the workshop and include references to relevant literature to provide appropriate background information.

General Needs and Challenges

Rapid Changes in Volume of Use

Because computer-enabled crimes in the United States are hard to track, estimates of rates of change or increases in computer-enabled crimes are difficult to determine with high precision (Levi, 2017). However, the state and local participants at the workshop on dark web investigations noted sharp upticks in the number of crimes brought to their attention with a dark web component. For example, the FBI's Internet Crime Complaint Center receives more than 800 complaints per day from people who believe they are victims of internet-enabled crimes, with total monetary losses estimated to be more than $1.4 billion in 2016 (National Academies of Sciences, Engineering, and Medicine, 2016). The FBI estimates that, for every crime reported to law enforcement, there are six internet-enabled crimes that go unreported (FBI Internet Crime Complaint Center, 2016, p. 3). In part because of the proliferation of marketplaces, some researchers have described the dark web ecosystem as "quite resilient to law enforcement take-downs," indicating that dark web transactions might continue to present a problem for law enforcement agencies well into the future (Soska and Christin, 2015, p. 46).

The increase in illicit activity on the dark web is not limited to any particular crime; it is spread over a variety of crimes previously conducted through different forums, such as drug and arms dealing, human trafficking, child pornography, and fraud (TrendLabs, 2016). At a PERF conference in 2018, DEA officials noted a significant increase in narcotics cases involving the dark web in the past five to ten years in particular, while FBI representatives emphasized the increasing use of dark web marketplaces to purchase malware and launder money (PERF, 2018). Participants noted an increase in peer-to-peer transactions that did not need to be facilitated by such sites as the Silk Road or AlphaBay.

Obtaining accurate information on dark web activity is a necessary—but insufficient—condition for the evaluation of programs and approaches. Given the lack of definitive quantitative data, law enforcement is expected to act without comprehensive information regarding what works and what is needed to address these dark web challenges. Although the workshop focused more on the needs side of this equation, participants did not diminish the role of rigorous research in further guiding police response.

Globalization

Like all online transactions, the dark web allows for a broad marketplace that crosses the boundaries of local, state, national, and even international jurisdictions. According to the criminal investigators who participated in the workshop, the multijurisdictional structure of illicit dark net markets presents enormous investigatory challenges, even before a case reaches court. Although domestic cases spanning jurisdictions face issues associated with the ambiguity of authority, agency collaboration, and conflicting laws or enforcement priorities, participants

According to the criminal investigators who participated in the workshop, the multijurisdictional structure of illicit dark net markets presents enormous investigatory challenges, even before a case reaches court.

noted that such challenges could multiply when expanded to the international stage. Preestablished lines of communication among various law enforcement agencies could be useful or even necessary to collect and store admissible evidence successfully across cities, states, and countries.

In the United States, cross-jurisdictional collaboration requires federal, state, and local partnerships. Internationally, ongoing dialogue among agency leaders determines investigation priorities, particularly with regard to evidence collection. Law enforcement agencies worldwide rely on Mutual Legal Assistance Treaties (MLATs), or agreements between two or more nations to share information related to criminal investigations in one another's jurisdictions. However, there are limitations to the current system for cross-jurisdictional cooperation; there might not be an MLAT between the country investigating a crime and the country where the evidence exists. In addition, the MLAT process can be slow, cumbersome, or unclear, especially for agencies at the local and state levels. The passage of the Clarifying Lawful Overseas Use of Data Act, (CLOUD Act) (U.S. House of Representatives, 2018) in the United States could lower barriers for law enforcement agencies seeking data stored in other countries because federal law enforcement has subpoena power over U.S.-based companies to obtain data, even if the company stores the data overseas.

The cross-jurisdictional nature of dark web marketplaces requires law enforcement investigators to form relationships with colleagues across agencies. Even with the challenges related to information sharing, individual state and local law enforcement agencies can play a vital role. For example, one local case could be linked to thousands of other dark web transactions. Participants noted that, if local agencies avoid dark web cases or are otherwise deterred from actively cooperating with federal or international agencies, dark web actors might be emboldened by the lack of enforcement to conduct more illicit business using the dark web.

The Need to Demystify the Dark Web for Law Enforcement

As noted by several workshop attendees, there is limited familiarity in many, if not most, state and local law enforcement agencies regarding the dark web and how it is used to facilitate criminal activity. The relative lack of experience with investigatory techniques for dark web–related crimes can make it difficult to build a solid criminal case. Participants expressed concerns about exposing themselves and their departments to retaliation by malicious dark web users and hackers when using government resources to access dark web marketplaces.

The relative lack of experience with investigatory techniques for dark web–related crimes can make it difficult to build a solid criminal case.

In response to this phenomenon, many workshop attendees stressed the need to demystify basic aspects of dark web investigations for officers or agency leaders who are unfamiliar with the dark web. To do so, trainers might find it helpful to emphasize the similarities between investigations involving the dark web and traditional investigatory methods (e.g., plain old police work). Such training could involve using familiar techniques for dark web investigations, especially those that are used to preserve digital evidence.

Command Buy-In for Additional Training

Workshop attendees emphasized the need to generate enthusiasm at the command level in police agencies to introduce new training programs and ultimately conduct successful dark web investigations. This might be particularly challenging for dark web investigations because familiarity or experience with new technologies is likely to be concentrated among younger officers. Therefore, tenured officers might be less inclined to develop an entirely new skill set. Reluctance among command officers might be further compounded by the fact that several dark web crimes involving fraud are not Uniform Crime Report Part I offenses (FBI, undated a) and often are less involved in accountability measures at the command level. Without command-level buy-in, funding and training time might not be made available.

Workshop participants discussed prior success at generating command buy-in by emphasizing the underlying similarities between dark web investigations and traditional investigations—although dark web investigations might require additional know-how about digital evidence and online access, the fundamentals are not substantially different from non–dark

web investigations. Obtaining tangible evidence through seizures from drug market investigations could encourage agency leaders to make additional training investments.

Training

Workshop participants noted that there are different training priorities for patrol units and for the more specialized units responsible for conducting in-depth investigations. For most officers, courses designed to develop a basic familiarity with digital evidence collection at a scene could be necessary. As with other technical training programs for line officers, workshop participants stressed the need to employ trainers with previous law enforcement experience. Typically, such trainers are better able to communicate technical concepts in ways that are useful and applicable to officers on patrol. Once subject-matter experts are identified, training should address the basic process of dark web transactions, such as how the dark web is accessed through Tor, how buyers and sellers communicate and exchange currency, and how goods and services are delivered. Basic awareness is sufficient for responding officers and can aid in recognizing and identifying relevant evidence during a preliminary investigation. Information, such as login credentials or other potentially useful artifacts, can be identified, collected, and cataloged after suspects have been apprehended.

Workshop participants emphasized that case studies, one-page documents, checklists, and other brief primers could be useful resources for responding officers to help them identify and collect evidence associated with dark web crimes. These materials also could be adapted for prosecutors and the judiciary to improve the level of knowledge among criminal justice practitioners. This information ultimately could help manage expectations from such investigations (e.g., of attorneys, judges, or even juries).

Participants noted the need for more in-depth knowledge of evidence collection for specialized units. These units require more-targeted training efforts that expand on evidence preservation to include advanced training on techniques frequently used by dark web actors. Among the courses that might be needed, workshop attendees highlighted training in the use of software exploits (i.e., network investigative techniques) and in conducting online undercover work tailored to dark web environments (American Civil Liberties Union, Electronic Frontier Foundation, and the National Association of Criminal Defense Lawyers, 2017).

For all types of training, workshop attendees noted a lack of qualified, available subject-matter experts, especially in less populous parts of the country. Given the substantial demand for these training programs, existing experts likely lack the capacity to serve all agencies, which has resulted in some agencies developing their own programs. Participants suggested that one way to support the development of a market of qualified trainers would be for state governments to require a certain number of hours dedicated to dark web investigations as part of state police curricula. In the meantime, workshop participants stressed the need to disseminate success stories across agencies so that departments are encouraged to pursue available training.

Although training opportunities exist on the federal level—some of which are taught or advised by our panelists—the discussion focused on expanding training. Much of the available training emphasizes digital evidence broadly, often with an eye toward cell phones, given their current ubiquity (see Goodison, Davis, and Jackson, 2015). Still, some major dark web–related training is available (for example, through the National White Collar Crime Center). However, the panel members' comments suggest that there is a potential disconnect between practitioners and training, in large part because agencies are slowly realizing the potential importance of investigating the dark web.

Workshop participants emphasized that case studies, one-page documents, checklists, and other brief primers could be useful resources for responding officers to help them identify and collect evidence associated with dark web crimes.

Technical Needs and Challenges

Anonymity and Access

A significant challenge for law enforcement is the anonymity that the dark web offers (Martin, 2014). Because identities are difficult to determine on the dark web, "buyers and vendors can use cryptomarkets to interact instantly, directly, freely and safely, without requiring any form of introduction or 'vetting'" (Persi Paoli et al., 2017, p. 69). These marketplaces often resemble "clear web" marketplaces—such as eBay or Amazon—in form and function. However, these sites are differentiated by the strategies used by participants to conceal their identities (Aldridge and Décary-Hétu, 2016). In addition to providing anonymity, the dark web can be accessed by a broad variety of users with relative ease, providing vendors with instant access to global audiences (Finklea, 2017). Basic internet literacy, a computer, and access to the internet is enough for any sufficiently motivated individual to begin supplying or purchasing illicit goods via the dark web.

Through a combination of existing technologies, the dark web provides users with a high degree of anonymity to engage in the transaction of illicit goods while evading detection by law enforcement. This is achieved through the use of such networks as Tor or the I2P, which encrypt a user's identity and shield illicit online activity from surveillance. Tor users, for example, maintain near anonymity by routing their traffic through a series of computers, or "nodes," around the globe, making it nearly impossible to trace their activity or identify their IP addresses. Network traffic is encrypted and passed through at least three nodes before it reaches its final destination. When the traffic exits the final node, it is mixed with other traffic, which both disperses and disguises the requests made by any single individual (Finklea, 2017).

Users also achieve a level of anonymity by using cryptocurrencies, such as Bitcoin, Litecoin, or Monero (Persi Paoli et al., 2017). Cryptocurrencies enable mostly anonymous, peer-to-peer transactions. All Bitcoin transactions, for example, are recorded in an online public ledger, referred to as the *blockchain*, but the identifying characteristics of participants involved in each transaction are not recorded. Furthermore, the large number of legitimate cryptocurrency users, especially for Bitcoin (Martin, 2014), increases the difficulty for law enforcement agencies in identifying and policing the trade of illicit goods and services (Persi Paoli et al., 2017).

Even if users choose to use their real names and mailing addresses when conducting transactions on the dark web, that information also typically is shielded from law enforcement by the default level of encryption that is provided to network traffic. Even when law enforcement successfully apprehends a buyer, it might be difficult or even impossible to obtain information about the seller if further identity-concealing measures are taken (Persi Paoli et al., 2017). However, when an entire market is compromised through a law enforcement seizure, both buyers' and sellers' information can be deanonymized. In response, users increasingly are employing additional strategies to protect their information while communicating and transacting on the dark web. Popular software, such as Pretty Good Privacy (PGP), enables encrypted communications between buyers and sellers above and beyond what is offered by the markets.

Basic internet literacy, a computer, and access to the internet is enough for any sufficiently motivated individual to begin supplying or purchasing illicit goods via the dark web.

Workshop participants also discussed the challenge of interdicting illegal dark web purchases shipped through traditional postal systems. The sheer number of parcels processed on a daily basis, which is estimated at more than 500 million (U.S. Postal Service, undated), presents an enormous difficulty for law enforcement officers attempting to identify and intercept the relatively small number of packages that contain illicit items (Shesgreen, 2017). Also, because buyers of illicit drugs typically purchase small quantities, the drugs are concealed in otherwise inconspicuous envelopes (Martin, 2014). Another obstacle often exploited by vendors is that law enforcement requires a warrant to seize packages from the U.S. Postal Service, which makes it a popular option for shipping illicit goods. Private companies (e.g., UPS, FedEx), do not offer the same level of protection and can be avoided easily. After items are shipped, both buyers and sellers can continue to evade law enforcement by rotating delivery points, shipping packages to alternative addresses, or

concealing illicit goods within consumer goods (Persi Paoli et al., 2017).

Crime Identification

Prior to conducting in-depth investigations, responding officers need to have a general awareness of the wide scope of illicit transactions that can be facilitated through the dark web. As discussed by workshop participants, state and local agencies are receiving reports of drug trafficking, arms sales, distribution of child pornography, ransomware, identity theft, and other illicit goods and services in their specific jurisdictions. Also, multiple workshop participants noted that local gangs have begun to use stolen identities from the dark web to open up fraudulent lines of credit to further fund their activities.

Workshop participants discussed the potential value of creating state task forces dedicated to dark web investigations, which ultimately would share information about ongoing crimes and identify links across jurisdictions. By building an information-sharing network similar to the High Intensity Drug Trafficking Area (HIDTA) program (DEA, undated), agencies could connect the dots in ongoing cases and more easily institutionalize relationships across local, state, and federal authorities. When a handful of arrests can be connected to thousands of transactions in an area, cooperation between agencies is crucial to maintaining efficient enforcement. Also discussed were issues related to operational deconfliction and systems to share both information and criminal intelligence related to dark web investigations in a manner similar to that used by the National Crime Information Center (NCIC) (FBI, undated b). Participants cited an ongoing need for guidance from federal partners on how to navigate privacy concerns when gathering information to identify crimes in progress.

When a handful of arrests can be connected to thousands of transactions in an area, cooperation between agencies is crucial to maintaining efficient enforcement.

Suspect Identification

Workshop participants noted that the methods used to identify suspects largely rely on traditional techniques to which most officers already are accustomed. By leaning on the common language and activities involved in what workshop participants described as "good old police work" and by incorporating basic knowledge of how dark web transactions take place into existing investigatory frameworks, officers can identify suspects involved in dark web transactions. Data sources available to law enforcement include email, social media, and other online engagement, which can be useful for investigators seeking to generate leads.

Workshop participants noted that initial investigators responding to a scene need to be cognizant of useful items, such as login credentials or other identifying information, that might help prosecutors link suspects to specific dark web transactions. This was the key for Portland Oregon police in the "Peter the Great" investigation, where they ultimately apprehended a vendor implicated in thousands of illicit drug sales via AlphaBay (PERF, 2018). Training investigators to look for certain applications on phones, PGP Keys, and usage of cryptocurrency might better prepare officers to identify useful evidence. However, agencies should be aware that the time and staff resources currently required to comb through massive amounts of digital data could present a challenge to budgets for larger or more-frequent investigations.

As in other types of investigations, workshop participants stressed that assembling the investigatory puzzle sometimes becomes easier when suspects use lax security protocols or make other mistakes. However, given that encryption and anonymity are what dark web users often are looking for, and given that there is a general lack of police training and experience with conducting dark web investigations, such mistakes by suspects might not be readily identifiable by investigators who are unfamiliar with the technologies involved. Furthermore, investigators who are less familiar with anonymity measures prior to engaging with buyers and sellers on the dark web might unwittingly expose their own identities to suspects under investigation.

Evidence Identification, Access, and Preservation

Digital evidence collection and preservation present several challenges beyond general concerns about crime scene contamination. There are challenges with forensically acquiring the relevant technical data about network activities and turning those data into clear and compelling evidence that is understandable by the general public (i.e., nontechnical audiences).

If undercover investigators on the dark web appear to violate laws while attempting to establish and build their online reputations, juries that are presented with this information might have an unfavorable view of evidence obtained in this manner.

Such challenges include dealing with increasing quantities of data; inscrutable data formats; and cross-jurisdictional coordination, both among agencies in the United States and agencies in different countries (Goodison, Davis, and Jackson, 2015; Vermeer, Woods, and Jackson, 2018). Workshop participants stressed that, in addition to the technical difficulties related to processing digital evidence, inconsistent policies and protocols for data collection and retention could hinder evidence handling across agencies, leaving law enforcement officers unclear on what information they can collect and how long such information can be held. Workshop participants described being constrained by uncooperative technology companies that are unable or unwilling to provide user data. Workshop participants also described using multiple methods to confirm evidence in dark web cases to establish culpability.

Like all evidence, digital evidence collected in dark web investigations should be obtained using acceptable forensic methods. Participants noted the importance of acquiring live computers, meaning computers currently engaged on the dark web rather than computers that have been disconnected or shut down. Obtaining live machines is important for accessing information before suspects have the opportunity to conceal, obscure, or delete incriminating data. Additionally, capturing data requires careful attention from qualified personnel to avoid contaminating or losing data that often can be volatile or temporary. As discussed earlier, investigators on the scene also should be trained to look for specific dark web browsing or Virtual Private Network (VPN) applications on phones, PGP Keys, and indications of cryptocurrency transactions.

Challenges related to the availability and duration of evidence also present difficulties for investigators. Unlike the surface web's Wayback Machine (Wayback Machine, undated), there is not a free-access archive for historical content on the dark web. Therefore, investigators need to document the listings that might be useful as evidence so that they can be used as admissible, compelling evidence later on. Workshop participants noted that absent new developments, prior court precedents have not definitively established the types of evidence agencies can collect or determined how long such evidence can be held. Participants described instances in which private industry contacts were able to keep similar information on individuals for longer than law enforcement policies typically allow. For example, participants noted that law enforcement agencies typically are constrained in terms of how long they are allowed to retain license plate information. However, private companies can store this information indefinitely and even sell it back to the law enforcement agency that might have been required to destroy it.

Participants also highlighted downstream concerns regarding the presentation of digital evidence in court. If undercover investigators on the dark web appear to violate laws while attempting to establish and build their online reputations, juries that are presented with this information might have an unfavorable view of evidence obtained in this manner. Network investigative techniques also might be considered invasive or cause juries to question whether investigators obtained probable cause, further complicating the likelihood of conviction. Workshop attendees noted the importance of communication across the criminal justice sectors, if only to manage expectations for what evidence can be provided and how as part of investigations with dark web components.

Resource Allocation

Aside from the costs necessary to devote personnel to dark web investigations, agencies also must consider the resources needed to hire and support qualified individuals who can efficiently investigate such cases. Multiple workshop participants noted that pooling resources within task forces in a model similar to HIDTA might be a prudent response. However, reliance on state forensic evidence labs or subcontractors might not be

Investigators should maintain awareness that, when their methods are presented in an open court, criminals quickly obtain and disseminate information about the methods employed.

sufficient in today's environment. Participants noted that state labs often are backlogged with thousands of requests and that subcontractors do not address the issue of having investigators and prosecutors who can explain complicated evidence in court. Without a clear explanation of dark web evidence, agencies might risk having judges or juries deem digital evidence "junk science."

Participants highlighted that most small-town departments likely would not have the resources to devote an officer to digital-evidence collection or even to assign an officer to a task force, let alone the resources for dark web investigations. However, these same agencies might benefit from the "trickle down" of information gained from investigations outside the department or from identifying and developing personnel with existing cyber skills. Several participants described actively recruiting potential hires with technical expertise and even reevaluating previous hiring and recruitment rules to consider hires from nontraditional backgrounds. Others described more-active pushes for grants to buy equipment or hire new personnel with an eye toward addressing the current opioid crisis in a dark web setting. Even with an increased emphasis on recruiting and retaining staff with valuable skill sets, attendees estimated that law enforcement agencies might not be able to offer salaries and benefits that can compete with those available in the private sector.

Adaptation and Fluctuation

Although law enforcement successfully shuttered several popular cryptomarkets, dark web users can adapt in novel ways or establish new illicit marketplaces with relative ease. For example, workshop participants noted that after the law enforcement shutdown of Silk Road 1, participants quickly moved to other cryptomarkets, such as Agora, Cloud-Nine, Evolution, Hydra, Sheep, and Silk Road 2. Additionally, cryptomarkets are highly dynamic in their own right. Attendees noted that such markets might open and close without fanfare or warning, regardless of law enforcement intervention.

Another problem is that law enforcement activity, when detected, might prompt reactive measures and countersurveillance (Buxton and Bingham, 2015). For example, dark web users can adopt more-advanced security measures on existing sites. To avoid detection, vendors can move away from cryptomarkets and sell exclusively in peer-to-peer vendor shops (Persi Paoli et al., 2017). According to workshop attendees familiar with conducting dark web investigations, information about how to avoid detection by law enforcement is exchanged routinely, not only on the dark web forums but also on popular websites on the clear web, such as Reddit. Real-time information exchange, in effect, "facilitates real-time responses to developments in law enforcement" (Martin, 2014, p. 359).

Once investigative methods reach the public domain, criminals using the dark web have ample opportunity to change their own methods accordingly. Investigators should maintain awareness that, when their methods are presented in an open court, criminals quickly obtain and disseminate information about the methods employed. Once court filings are posted online, there is no way to limit who has access to past investigatory methods. Workshop participants noted that *parallel construction*—a practice used by investigators to limit potentially secret or sensitive methods from being part of public court documents—typically is not sufficient to limit what criminals can learn about investigators' methods from the public record.

Legal Needs and Challenges

The Multijurisdictional Nature of Crime

Dark web investigations are subject to many of the same issues that affect other criminal investigations in which computers are involved, especially with regard to digital-evidence collection from cloud service providers (Vermeer, Woods, and Jackson, 2018). For example, vendors in Australia simultaneously can sell to buyers in various countries in Europe and in several communities across the United States. Responsibility for illegal activity might cut across not only local and state law enforcement agencies but also various agencies at the federal level and law enforcement agencies across the globe. Workshop attend-

ees highlighted the importance of multiagency partnerships, such as those employed in the Silk Road, AlphaBay/Hansa, and "Peter the Great" cases, in developing leads and gathering evidence. Moreover, partnerships require coordination across a variety of stakeholders, which might add layers of investigative difficulty because of competing priorities, obligations, policies, and laws.

Entrapment

Entrapment is a concern whenever law enforcement officers engage in covert, undercover activity during investigations. The nature of dark web transactions and the nascence of such investigations could lead to additional challenges related to entrapment. Because they are anonymous forums, cryptomarkets thrive on the ability of buyers and sellers to build a reputation. Once a sale is complete, users can rate one another and leave feedback on various aspects of the process, such as the quality of the packaging, speed of delivery, and ease of money exchange, which is displayed publicly in the marketplace. Buyers and sellers build their reputations over time through many transactions, which establishes their legitimacy in the otherwise anonymous marketplace. This creates a challenge for law enforcement officers: They cannot enter a cryptomarket and begin buying or selling high-profile items without first demonstrating their trustworthiness. Participants discussed how law enforcement could take over an arrestee's marketplace account, assuming the arrestee's identity and using the established reputation as a gateway to lure more-significant criminals.

Some participants expressed concerns regarding the potential scope of law enforcement operations on the dark web. As seen in the AlphaBay/Hamsa case, law enforcement was able to take over a marketplace as a tactic in an investigation. Although no legal challenges have been brought against law enforcement regarding these tactics, the continued operation of an illegal marketplace exposes law enforcement to the risk of entrapping otherwise innocent individuals, especially if some of the individual marketplace users also are government agents.

WORKSHOP PRIORITIZATION

Identification and Prioritization of Problems and Opportunities

During the discussions, the panel members identified 40 individual problems or opportunities. As each problem or opportunity was identified, panelists were asked to identify potential solutions or needs. As a result, the panelists identified 46 potential solutions, or needs, that they felt could benefit from additional investment in research and development (some problems were associated with multiple solutions or needs). In this context, research and development (R&D) should be interpreted as broadly as possible. It should not be construed to refer merely to the development of hardware or software; rather, it also should refer to training curricula, new policies, and best practices.

To prioritize the problems and opportunities and corresponding needs, we relied on the Delphi Method, using techniques similar to those employed in earlier Priority Criminal Justice Needs Initiative expert panel reports (RAND Corporation, undated a; Jackson et al., 2016). Toward the end of the workshop, panelists were presented with a complete list of needs that they generated and asked to assign two scores to each pair. The scores were on a 1–9 scale where 9 was the highest score. First, the panel members were asked to estimate the potential impact solving the problem or taking advantage of the opportunity could have and, ultimately, the impact to the law enforcement mission as a whole. Next, the panelists were asked to estimate the likelihood of success of solving the problem or taking advantage of the opportunity. The panel members' individual estimates and comments were consolidated and presented to the group for additional discussion. The panelists were then given a chance to adjust their selections based on the discussion in the room. This second round of selections also was consolidated and ultimately separated into three tiers (high, moderate, and low priority). For a complete discussion of the methodology we employed, see the Technical Appendix at the end of this report.

Because they are anonymous forums, cryptomarkets thrive on the ability of buyers and sellers to build a reputation.

We have divided the 46 needs into the following four categories:

1. training (14 needs)
2. organizational cooperation and information sharing (14 needs)
3. development of tools (7 needs)
4. other (11 needs).

Across the board, the majority of the highest-priority problems or opportunities and their associated solutions or needs were focused on developing training, checklists, and cheat sheets that would help officers and investigators improve their recognition of criminal situations and artifacts where dark web technologies played a role. In Table 2, we list the problems and opportunities associated with training and their related needs. Of the 14 needs in this category, 12 were top-tier (i.e., high-priority) needs and two were second-tier (i.e., moderate-priority) needs. None of the training needs fell into the third tier. This indicates the panel members' strong preference for investing in training and their high confidence that this problem can be addressed with additional training.

Table 2. Needs Identified Related to Training

Tier	Problem or Opportunity	Associated Need
1	Handwritten codes or other small digital artifacts (e.g., Bitcoin wallet IDs, PGP keys, dark web addresses) often are the key to finding a larger cache of evidence that is hidden away in a computer or on the dark web.	• Develop training for both junior and senior officers that shows them how to recognize digital artifacts that could be beneficial to investigations.
	Law enforcement officers are not being trained to recognize when there are relevant digital artifacts that might be useful in an investigation.	• Develop basic training that examines previous cases, how the dark web fits into those cases, and how those cases were solved.
	The investigative puzzle is getting more difficult to assemble with the types of evidence found in dark web investigations.	• Develop checklists and training (e.g., continuous learning) that are intended to keep officer skills up to date so that they can effectively organize the pieces of the puzzle.
	Authentication of anonymized digital evidence can be difficult.	• Create a "cheat sheet" for how to preserve digital evidence.
	There is an inherent officer bias toward preparing to collect and manage physical artifacts rather than digital artifacts.	• Develop training for both junior and senior officers that shows them how digital artifacts are beneficial to traditional investigations.
	Officers do not have sufficient training to ensure that they are familiar with digital evidence and artifacts.	• Develop training standards that include the minimum number of hours for each curriculum.
	Existing multipage publications are too long to make an impact and be consumed by the average officer.	• Ensure that longer publications are accompanied by shorter publications that include easily digestible key facts and information (e.g., laminated sheets that can be hung on a wall, one-pagers).
	There is a lack of understanding about how digital evidence artifacts can be managed and accounted for in a way that is very similar to how physical evidence is managed.	• Develop model policies that can be used to manage and account for digital artifacts.
	Deconfliction of ongoing investigations is difficult to accomplish (e.g., blue-on-blue).	• Develop a training curriculum that teaches law enforcement officers about which digital artifacts are most useful for deconfliction.
	Law enforcement agencies generally are unaware of the scope and breadth of crimes that are currently being facilitated with the dark web (e.g., narcotics, child exploitation, human trafficking, retail theft, murder for hire, credit card theft, identity theft, human organ theft, hacking equipment, and such destructive information as that contained in *The Anarchist's Cookbook*).	• Develop easy-to-consume guides that can be posted on a bulletin board that contain things to look for (e.g., symptoms).

Table 2—Continued

Tier	Problem or Opportunity	Associated Need
	It often is difficult for judges, defense attorneys, and juries to understand digital evidence that is extremely technical in nature.	• Develop high-quality, easy-to-understand, expert-endorsed videos (that are available to the public) that can be shown in a courtroom to explain the technical details in a way that can be easily understood by individuals without a technical background.
	The collection of evidence for dark web–related cases might require additional care and handling and additional training for investigators.	• Assess the content of existing trainings to look for gaps and recommend modifications or the creation of additional training.
2	Because of the encryption and data-cleaning protocols that are standard on the dark web, it is critical to ensure that investigators attempt to capture the contents of a live machine's RAM.	• Ensure that investigators are aware of the additional evidentiary value of the contents of a machine's RAM (especially for dark web cases).
	The number of officers with technical skills is insufficient.	• Explore and highlight best practices for the direct hire of individuals with highly valued technical skills.

Another large group of the highest-priority needs identified by the participants fell into the organizational cooperation and information-sharing category (see Table 3). This makes sense because of the cross-jurisdictional nature of most crimes that rely on the dark web. Panelists reported that significant value was likely to result from strengthening the structures used to share operational information and lessons learned and from developing new structures. For the most part, the top-tier problems and opportunities were related to information sharing and the second-tier needs were related to systems of coordination and deconfliction. In this category, most of the needs fell into Tier 1 or Tier 2, with only two of the problems landing in the lowest tier. Interestingly, the issues that fell into the lowest category had to do with encryption, likely indicating that pan-

Table 3. Needs Identified Related to Organizational Cooperation and Information Sharing

Tier	Problem or Opportunity	Associated Need
1	A large number of deaths related to opioid overdoses can be linked to dark web transactions (and distribution methods).	• Quickly collect and disseminate the lessons that have been learned by task forces that have worked these cases and disseminate them to other task forces that have not yet been pursuing dark net cases (e.g., case presentation video).
	Existing, successful, and cooperative models for cross-jurisdiction, cross-agency investigations that have the potential to make a significant impact are not well known.	• Explore the potential costs, risks, and benefits of extending a HIDTA model to a larger number of jurisdictions for addressing potential problems.
	Cross-jurisdictional relationships and cooperation are essential to being effective when conducting investigations.	• Identify and highlight existing best practices (e.g., case studies) that are designed to improve cross-jurisdictional relationships (e.g., information-sharing meetings).
	External funding (e.g., Organized Crime Drug Enforcement Task Force), when available quickly, has the potential to greatly improve the effectiveness of existing task forces.	• Conduct research into the potential positive impacts of increasing the pace of the funding process.
	Information collected at the patrol level often does not get added to intelligence databases, where it could be more useful.	• Conduct research on the benefits that result from collecting and sharing field-level (e.g., patrol) information in a way that is useful to law enforcement intelligence.
2	It is technically difficult to extract digital evidence from devices; interpreting such evidence is much easier (many more investigators can accomplish that).	• Identify and highlight the effect of digital evidence backlogs on national problems, such as drug overdose cases (similar to what was done for DNA and rape kits).
	A large number of deaths related to opioid overdoses can be linked to dark web transactions (and distribution methods).	• Encourage U.S. Department of Justice leadership to ask existing task forces with drug-focused funding (e.g., DEA, FBI, HIDTA) to focus a portion of their resources on dark web transactions.

Table 3—Continued

Tier	Problem or Opportunity	Associated Need
	The rate of change with respect to tactics and techniques for successful evidence collection is constantly changing.	• Develop an information system to continuously collect and disseminate successes with respect to evidence collection and preservation.
	Local law enforcement agencies are perfectly positioned to understand the baseline of what is normal in their jurisdictions.	• Local law enforcement needs better ways to check whether anomalous activity is connected to a larger network of activity that might already be under investigation.
	Deconfliction of ongoing investigations is difficult to accomplish (e.g., blue-on-blue).	• Work with owners and managers of existing deconfliction systems to ensure that they handle digital artifacts appropriately (e.g., Bitcoin addresses, email addresses).
	When small agencies run across digital artifacts, they often turn to state labs to run an analysis. Those results could be relevant to an ongoing task force investigation, but that connection is not happening very efficiently.	• An NCIC is needed for deconfliction and criminal intelligence.
	The international nature of transactions on the dark web adds complications because laws and rules differ greatly.	• Conduct outreach and marketing targeted at state and local investigators to help them understand what options are available to them for requesting overseas information.
3	It can be difficult to gain access to potential evidence that is encrypted.	• Explore the viability of public-private partnerships that can be leveraged to improve access to potential evidence that is commercially encrypted by default (e.g., off-the-shelf encryption on operating systems such as Windows, MacOS, Linux, iOS, and Android). • Explore the viability of cooperative information-sharing techniques (e.g., multisignature authentication) for unencrypting potential evidence.

elists felt that there was a low likelihood of success on endeavors related to bypassing or cracking encryption protocols.

In Table 4, we list the set of problems and opportunities that fit into the more traditional notion of research and development. Many of these needs are centered on the development of standards for existing tools or conducting research into developing new tools or systems that would automate or simplify some of the more tedious and time-consuming aspects of an investigator's job. Most of these needs fell into Tier 2, with one need—developing standards for forensic tools—landing in the top category.

The final category of problems and opportunities is for those needs that did not fit neatly into one of the previous three categories (see Table 5). Two of these were in the first-priority tier. The first concerns conducting research into modernizing the laws surrounding law enforcement's ability to search mail and packages. The second concerns conducting research into the impacts of one class of crime—online or offline—on crime in other domains, such as transnational, federal, or local crime, with an eye toward informing law enforcement leadership about the impacts of focusing resources on certain types of difficult-to-solve local crimes, especially if those crimes have larger (i.e., federal or transnational) linkages.

Table 4. Needs Identified Related to Tool Development

Tier	Problem or Opportunity	Associated Need
1	Because of the encryption and other anonymity measures built into dark web software, it is important to ensure that the tools, processes, and procedures used to capture evidence remain the best available (e.g., forensic network information, computer screenshots).	• Encourage standards development bodies (e.g., National Institute of Standards and Technology Forensic Tool Testing group) to assess the newest procedures and develop standards for these newer processes.
2	The investigative puzzle is getting more difficult to assemble with the types of evidence found in dark web investigations.	• Identify (or develop) automated investigatory tools that are helpful for organizing the pieces of the investigation.
	Potential criminal marketplace servers increasingly are hardened against traditional investigative techniques, thus increasing the cost to conduct the investigation.	• Conduct research into the types of hardening that are being used and identify the most-appropriate responses for law enforcement.
	Handwritten codes or other small digital artifacts (e.g., Bitcoin wallet IDs, PGP keys, dark web addresses) often are the key to finding a larger cache of evidence that is hidden away in a computer or on the dark web.	• Develop a Google-like searchable repository that law enforcement can use to look up digital artifacts and obtain additional information on them.
	It can be difficult to obtain evidentiary history for dark web–related cases.	• Ensure that investigators are aware of the commercial services that are mirroring the content of public and dark web sites that can be used for evidentiary purposes.
	More peer-to-peer communication is occurring among suspects (i.e., they are not relying on intervening servers to communicate).	• Conduct research and development on potential investigative solutions, including identifying potential exploits and developing new tools.
3	It is very difficult to get agencies that are using different software systems to decide to cooperate and share information or use a common platform.	• Ensure that existing standards and coordination bodies are aware of the unique requirements for dark web investigations.

Table 5. Needs Identified Related to Other Problems and Opportunities

Tier	Problem or Opportunity	Associated Need
1	The laws governing package carriers' ability to conduct searches on suspicious packages are very old.	• Conduct research into the gaps and shortcomings of current laws related to searching packages.
	Modern crimes that have a network or internet component require a broader mindset of cooperation among federal, state, and local law enforcement entities than was required to be successful historically.	• Conduct research that is designed to help law enforcement leadership better understand how local crimes are tied to larger problems.
2	The use of cryptocurrencies for criminal activity significantly complicates investigations.	• Explore the costs, risks, and benefits of spending additional resources monitoring currency exchange companies that are not currently in compliance.
	How the dark web and its perception of perfect anonymity is affecting the demographics of offenders is unknown.	• Conduct research into the effects of new technologies on individual willingness to engage in criminal transactions.
	Dark web initiatives often will require additional financial resources.	• The scope and depth of the problem needs to be communicated clearly to policymakers, especially those who allocate budgets.
	The international nature of transactions on the dark web adds complications because laws and rules differ greatly.	• Work with MLAT program managers to encourage better service, including international dialog and round-the-clock communication and service. • Develop protocols for coordination and harmonization issues that are not covered by MLAT.
	There are differing standards for collecting and retaining information, depending on the information's purpose (e.g., national security, law enforcement, commercial).	• Conduct research to assess the privacy and operational impacts of retention lengths for different types of investigations and different types of data.

Table 5—Continued

Tier	Problem or Opportunity	Associated Need
3	Investigative methods are migrating into the public domain, which allows criminals to adapt their methods.	• Develop best practices to monitor the law enforcement tactics and identifying information that is leaking into the public domain via social media, etc.
	It is difficult to investigate crimes without running afoul of citizens' privacy expectations.	• Conduct research into the level of privacy that citizens are willing to give away to buy more security.
	It is becoming more common for investigators and arresting officers to be captured on video (sometimes with such identifiers as license plates and business cards), and that information quickly disseminates among criminal information networks.	• Develop best practices to monitor the law enforcement tactics and identifying information that is leaking into the public domain via social media, etc.

CONCLUSIONS

As global communications and commerce become increasingly interconnected, it is less challenging for criminals to conduct illicit activities across local, state, or international lines. Modern information technologies that obscure identities and the content of communications serve legitimate purposes for ensuring individual privacy, helping activists in repressive regimes, and facilitating the needs of U.S. agents working covertly. However, these same tools help criminals hide the evidence of their criminal activities and increase the level of difficulty for the typical investigator. As these new communication technologies place additional demands on investigators in terms of the levels of expertise and effort required to accomplish their missions, they could use additional resources and tools to efficiently accomplish the missions that they have sworn to pursue while remaining in compliance with both the spirit and the letter of U.S. laws and the U.S. Constitution. To support this mission, the members of the Priority Criminal Justice Needs Initiative dark web panel identified and prioritized several problems and opportunities that they felt would make a significant impact on the problems that law enforcement agencies face on a daily basis. Additionally, this work can assist in developing an actionable research and development agenda that will enhance law enforcement's ability to understand and investigate illicit activity on the dark web. At a high level, the recommendations that emerged from the workshop participants top challenges and needs are to

- invest in training at all levels, from the most-junior to the most-senior officer. The junior levels need to know what to look for and the senior levels need to ensure that appropriate levels of training are included in the training curriculum
- invest in efforts aimed at improving information sharing across agencies, both within the United States and across international borders
- examine the benefits of further investing in established cross-organization structures that are designed to facilitate cooperation and information sharing
- encourage standards organizations to develop new testing standards for forensic tools that are employed to collect evidence on computers that have been running dark web software
- conduct research into modernizing laws associated with inspecting packages transmitted via the U.S. mail and similar services
- conduct research into the increasingly interconnected nature of crime and criminals to ensure that law enforcement is able to focus on both the highly visible tip of the iceberg (i.e., traditional crime) and the less visible—but extremely important—portion of the iceberg (i.e., cybercrime) that has the potential to affect the health and welfare of populations both near and far.

Taken together, the high-priority needs identified across the areas explored during the workshop represent an agenda to better prepare law enforcement at all levels to address the challenge posed by cybercrime, both now and into the future.

TECHNICAL APPENDIX

In this appendix, we present additional detail on the panel process, needs identification, and prioritization carried out to develop the research agenda presented in the main report. The text in this section is based on that of other Priority Crimi-

nal Justice Needs Initiative reports (see RAND Corporation, undated b).

Pre-Workshop Activities

RAND and PERF researchers recruited the panel members by extending invitations to knowledgeable individuals identified through existing professional and social networks (e.g., LinkedIn) and by reviewing literature published on the topic. At the time of the invitation, panelists were provided with a brief description of the workshop's focus areas. The workshop agenda is presented in Table A.1.

To prepare for the workshop, panelists were provided with read-ahead materials and were given an opportunity to identify the issues and topics that they felt would be important to discuss during the workshop. Prior to the workshop, four attendees responded with feedback regarding the topics they deemed worthy of further discussion. A summary of the read-ahead document and the feedback we received is included in the main report. The pre-workshop questionnaire was delivered as an online survey and is presented in the next section.

Pre-Workshop Questionnaire

Thank you for your assistance in focusing our agenda and topics for the workshop by taking part in this questionnaire. We would like your input on the relative importance of topics mentioned in the read-ahead document, input on specific challenges or opportunities in any of the areas mentioned, and feedback and suggestions on topics that deserve greater attention or that were missed altogether. You are free to skip any of the questions in the questionnaire.

1. What are the **top three challenges** or issues facing law enforcement today when conducting criminal investigations with a dark web component?

   For each of the questions below, consider the following processes:
   - crime identification
   - evidence identification
   - evidence preservation
   - evidence access and collection
   - evidence quality, provenance, and presentation.

2. What are the most significant ***legal*** problems or challenges in this area related to law enforcement effectiveness?

3. What are the most significant ***technical*** problems or challenges in this area related to law enforcement effectiveness?

4. What are the most significant challenges related to preserving the civil rights of noncriminals using the dark web?

5. What opportunities do you see in this area (e.g., applying new technologies, changing law enforcement strategies or practices, other innovations) that would improve law enforcement performance or efficiency?

6. Are there any issues, problems, or opportunities that you see that are related to conducting criminal investigations with a dark web component that do not easily fit into the categories defined in this questionnaire? Is there anything else that was not discussed above that should be covered in this workshop?

Prioritization of Needs

During the workshop, participants collectively reviewed the list of challenges and issues that they provided prior to the workshop. While conducting this review, they suggested additional potential areas worthy of research or investment. Workshop

Table A.1. Workshop Agenda

Day 1	
8:30	Welcome and Introductions
9:30	Initial Discussion of Problems
9:45	Case Study Presentation
10:30	Discussion of Problems and Needs
11:30	Lunch
1:00	Case Study Presentation
2:00	Discussion of Problems and Needs

Day 2	
8:30	Needs Discussions
10:30	Review and Final Brainstorming
11:30	Working Lunch
12:00	Prioritize Needs
1:30	Wrap-Up and Next Steps
2:00	End of Workshop

participants also considered whether there were areas that were not included in the existing list and suggested new ones.

To develop and prioritize a list of technology and policy areas that are likely to benefit from research and development investment, we followed a process that has been used in previous research (see, for example, Jackson et al., 2016, and references therein). The panelists discussed and refined opportunities and problems in each category and also identified potential needs and solutions that could address each problem or opportunity. Once the group had compiled and refined its list of issues and needs, they were converted into a web-based Delphi instrument using the Confirmit service.

Delphi Round 1

Using the Delphi instrument, each panelist was asked to individually score each issue and its associated need using a 1–9 scale for the following dimensions: (1) importance or payoff and (2) probability of success. For the importance or payoff dimension, participants were instructed that 1 was a low score and 9 was a high score. Participants were further told to score that importance or payoff dimension with a 1 if the need or solution would have little or no impact on the problem and with a 9 if the need or solution would reduce the impact of the problem by 20 to 30 percent (or more).

When the first Delphi round was completed, the panel members' responses and comments were anonymously collected and summarized. This summary contained a "kernel density" distribution figure and a collection of the members' comments for each issue and need. This summary was used to facilitate discussion among the panelists for the needs that had the most disagreement, either in the areas of payoff or probability of success. The purpose of the discussion was to encourage the panelists to discuss their differences and to attempt to move toward consensus. During this discussion, panelists were asked to return to the Delphi tool to provide a second round of responses while keeping the group's collective response and any discussion in mind.

In Figure A.1, we show an example of one of the questions presented to the group prior to their second-round answers (in the figure, "issue" is the challenge or opportunity).

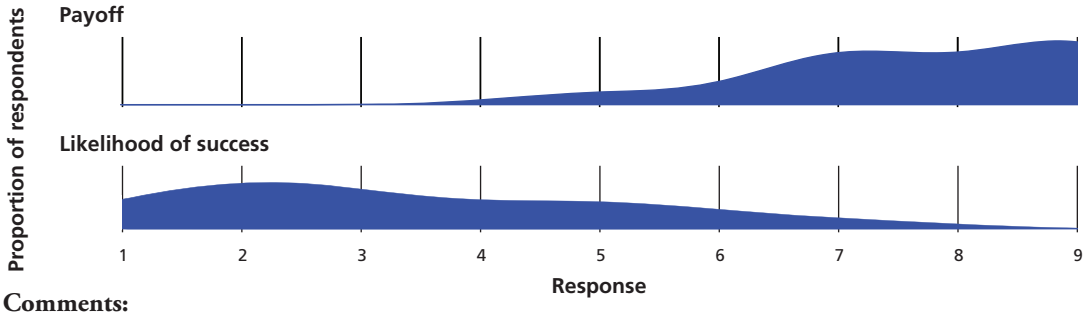
Delphi Round 2

Once the round 2 responses were collected, they were ranked by calculating an expected value using the method outlined in Jackson et al., 2016. Specifically, for each question, the payoff and the likelihood of success scores were multiplied together, and the median of that product was the expected value. The resulting expected value scores were then clustered using a hierarchical clustering algorithm. The algorithm we selected was the "ward.D" spherical algorithm from the "stats" library in the R statistical package, version 3.4.1. We chose this algorithm to minimize within-cluster variance when determining the breaks between tiers. The choice of three tiers is arbitrary but was done in part to remain consistent across the set of technology workshops we have conducted for NIJ. Also, the choice of three tiers represents a manageable system for policymakers. Specifically, the top tier is made up of the priorities that should be the primary policymaking focus, the middle tier should be examined

Figure A.1. Example Post–Round 1 Delphi Summary Question

Issue: It can be difficult to gain access to potential evidence that is encrypted.

Need: Explore the viability of public-private partnerships that can be leveraged to improve access to potential evidence that is commercially encrypted by default (e.g., off-the-shelf encryption on such operating systems as Windows, MacOS, Linux, iOS, and Android).

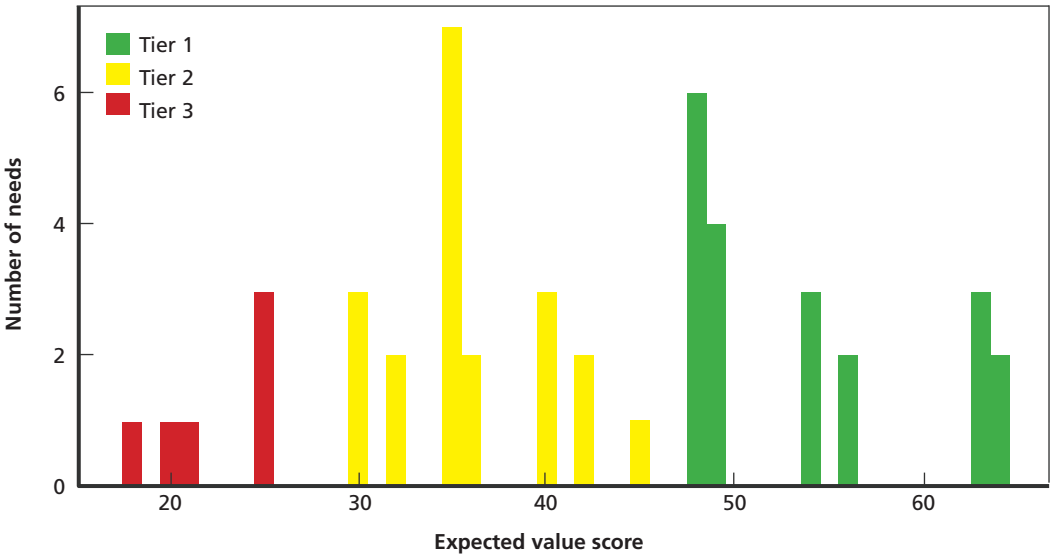


Comments:

There is a risk of undermining public trust, as in San Bernardino case.

closely, and the final tier is probably not worth much attention in the near term. Figure A.2 shows the distribution of the needs by their expected value scores. The height of a bar indicates the number of needs that had that score, and the color of the bar indicates the tier that the need was ultimately assigned to by the clustering algorithm.

Figure A.2. Distribution of the Clustered Needs Following Round 2



References

Afilipoaie, Alois, and Patrick Shortis, "From Dealer to Doorstep–How Drugs Are Sold on the Dark Net," Wales, United Kingdom: Swansea University, Global Drug Policy Observatory Situation Analysis, June 2015. As of September 1, 2019: https://www.swansea.ac.uk/media/Dealer%20to%20Doorstep%20FINAL%20SA.pdf

Aldridge, Judith, and David Décary-Hétu, "Hidden Wholesale: The Drug Diffusing Capacity of Online Drug Cryptomarkets," *International Journal of Drug Policy*, Vol. 35, September 2016, pp. 7–15.

American Civil Liberties Union, Electronic Frontier Foundation, and the National Association of Criminal Defense Lawyers, *Challenging Government Hacking in Criminal Cases*, New York, March 2017. As of January 31, 2019: https://www.aclu.org/report/challenging-government-hacking-criminal-cases

Argonne National Laboratories, "DarkNet Terminology: Definitions of the DarkNet, the Dark Web, and the Deep Web," webpage, undated. As of September 1, 2019: https://coar.risc.anl.gov/coar-attends-department-of-homeland-security-hosted-darknet-summit/

Buxton, Julia, and Tim Bingham, "The Rise and Challenge of Dark Net Drug Markets," Wales, United Kingdom: Swansea University, Global Drug Policy Observatory, Policy Brief 7, January 2015. As of August 10, 2018: https://www.swansea.ac.uk/media/The%20Rise%20and%20Challenge%20of%20Dark%20Net%20Drug%20Markets.pdf

Ciancaglini, Vincenzo, Marco Balduzzi, Robert McArdle, and Martin Rösler, *Below the Surface: Exploring the Deep Web*, Tokyo, Japan: Trend Micro, 2015. As of September 1, 2019: https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf

DEA—*See* U.S. Drug Enforcement Administration.

Europol, "Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation," press release, July 20, 2017. As of August 9, 2018: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

FBI—*See* Federal Bureau of Investigation.

Federal Bureau of Investigation, "About the Uniform Crime Reporting Program," webpage, undated a. As of August 10, 2018: https://www.bjs.gov/ucrdata/abouttheucr.cfm

Federal Bureau of Investigation, *National Crime Information Center (NCIC)*, webpage, undated b. As of August 10, 2018: https://www.fbi.gov/services/cjis/ncic

Federal Bureau of Investigation Internet Crime Complaint Center, *2016 Internet Crime Report*, Washington, D.C., 2016. As of August 9, 2018: https://pdf.ic3.gov/2016_IC3Report.pdf

Finklea, Kristin, *Dark Web*, Washington, D.C.: Congressional Research Service, R44101, March 10, 2017. As of August 10, 2018: https://fas.org/sgp/crs/misc/R44101.pdf

Goodison, Sean E., Robert C. Davis, and Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, Santa Monica, Calif.: RAND Corporation, RR-890-NIJ, 2015. As of August 10, 2018: https://www.rand.org/pubs/research_reports/RR890.html

Greenberg, Andy, "Crackdowns Haven't Stopped the Dark Web's $100M Yearly Drug Sales," *Wired*, August 12, 2015. As of August 9, 2018: https://www.wired.com/2015/08/crackdowns-havent-stopped-dark-webs-100m-yearly-drug-sales/

Jackson, Brian A., Duren Banks, John S. Hollywood, Dulani Woods, Amanda Royal, Patrick W. Woodson, and Nicole J. Johnson, *Fostering Innovation in the U.S. Court System: Identifying High-Priority Technology and Other Needs for Improving Court Operations and Outcomes*, Santa Monica, Calif.: RAND Corporation, RR-1255-NIJ, 2016. As of August 10, 2018: https://www.rand.org/pubs/research_reports/RR1255.html

Kruithof, Kristy, Judith Aldridge, David Décary-Hétu, Megan Sim, Elma Dujso, and Stijn Hoorens, *Internet-Facilitated Drugs Trade: An Analysis of the Size, Scope and the Role of the Netherlands*, RAND Europe and WODC, Ministerie van Veiligheid en Justitie, RR-1607-WODC, 2016. As of August 9, 2018: https://www.rand.org/pubs/research_reports/RR1607.html

Levi, Michael, "Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues," *Crime, Law and Social Change*, Vol. 67, No. 1, February 2017, pp. 3–20.

Martin, James, "Lost on the *Silk Road*: Online Drug Distribution and the 'Cryptomarket,'" *Criminology and Criminal Justice*, Vol. 14, No. 3, July 2014, pp. 351–367.

McCormick, Ty, "The Darknet: A Short History," *Foreign Policy*, December 9, 2013. As of August 9, 2018: http://foreignpolicy.com/2013/12/09/the-darknet-a-short-history

Moore, Daniel, and Thomas Rid, "Cryptopolitik and the Darknet," *Survival*, Vol. 58, No. 1, February-March 2016, pp. 7–38.

National Academies of Sciences, Engineering, and Medicine, *Modernizing Crime Statistics: Report 1: Defining and Classifying Crime*, Washington, D.C.: National Academies Press, 2016.

Peralta, Eyder, "N.H. Public Library Resumes Support of 'Tor' Internet Anonymizer," *National Public Radio*, September 16, 2015. As of August 9, 2018: https://www.npr.org/sections/thetwo-way/2015/09/16/440848324/n-h-public-library-resumes-its-support-of-tor-network

PERF—*See* Police Executive Research Forum.

Persi Paoli, Giacomo, Judith Aldridge, Nathan Ryan, and Richard Warnes, *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web*, Santa Monica, Calif.: RAND Corporation, RR-2091-PACCS, 2017. As of August 9, 2018: https://www.rand.org/pubs/research_reports/RR2091.html

Police Executive Research Forum, *New National Commitment Required: The Changing Nature of Crime and Criminal Investigations*, Washington, D.C., January 2018. As of August 9, 2018: http://www.policeforum.org/assets/ChangingNatureofCrime.pdf

"Police Ran 2nd Dark Web Marketplace as Sting to Spot Drug Deals," CBC News, July 21, 2017. As of August 9, 2018: http://www.cbc.ca/news/technology/darknet-hansa-market-1.4215567

RAND Corporation, "Delphi Method," webpage, undated a. As of October 5, 2017: https://www.rand.org/topics/delphi-method.html

RAND Corporation, "Priority Criminal Justice Needs Initiative," webpage, undated b. As of August 9, 2018: https://www.rand.org/jie/justice-policy/projects/priority-criminal-justice-needs.html

Shesgreen, Deirdre, "An Inside Look at the Hunt for Fentanyl, the Deadly Opioid Driving the Overdose Crisis," *USA Today*, September 22, 2017. As of August 10, 2018: https://www.usatoday.com/story/news/nation/2017/09/17/opioid-crisis-how-customs-officers-find-fentanyl-mail/662838001/

Soska, Kyle, and Nicolas Christin, "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem," 24th USENIX Security Symposium, Washington, D.C., August 12–14, 2015. As of August 9, 2018: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/soska

TrendLabs, *Cybercrime and the Deep Web: Forward-Looking Threat Research (FTR) Team*, Tokyo, Japan: Trend Micro, 2016. As of August 10, 2018: https://documents.trendmicro.com/assets/wp/wp-cybercrime-and-the-deep-web.pdf

U.S. Department of Justice, "Attorney General Sessions Announces New Tool to Fight Online Drug Trafficking," press release, January 29, 2018. As of August 9, 2018: https://www.justice.gov/opa/pr/attorney-general-sessions-announces-new-tool-fight-online-drug-trafficking

U.S. Drug Enforcement Administration, "DEA Programs: High Intensity Drug Trafficking Areas (HIDTAs)," webpage, undated. As of August 10, 2018: https://www.dea.gov/ops/hidta.shtml

U.S. House of Representatives, Clarifying Lawful Overseas Use of Data Act, Bill 4943, February 6, 2018. As of August 10, 2018: https://www.congress.gov/bill/115th-congress/house-bill/4943

U.S. Postal Service, "Postal Facts: One Day in the Life of the U.S. Postal Service," webpage, undated. As of August 10, 2018: https://about.usps.com/who-we-are/postal-facts/one-day-by-the-numbers.htm

Van Hout, Marie Claire, and Tim Bingham, "Responsible Vendors, Intelligent Consumers: Silk Road, the Online Revolution in Drug Trading, *International Journal of Drug Policy*, Vol. 25, No. 2, March 2014, pp. 183–189.

Vermeer, Michael J. D., Dulani Woods, and Brian A. Jackson, *Identifying Law Enforcement Needs for Access to Digital Evidence in Remote Data Centers*, Santa Monica, Calif.: RAND Corporation, RR-2240-NIJ, 2018. As of August 10, 2018: https://www.rand.org/pubs/research_reports/RR2240.html

Wayback Machine, homepage, undated. As of August 10, 2018: https://web.archive.org

Acknowledgments

The authors would like to acknowledge the participation and assistance of the members of the dark web expert workshop, who are listed in the body of the report. This effort would not have been possible without their willingness to participate in the effort. The authors also would like to acknowledge the contributions of Steve Schuetz and Martin Novak of the National Institute of Justice. The authors also acknowledge the valuable contributions of the peer reviewers of the report, Daniel Gonzales of RAND, Julia Buxton of the Swansea University Global Drug Policy Observatory, and the anonymous reviewers from the U.S. Department of Justice.

The RAND Justice Policy Program

RAND Social and Economic Well-Being is a division of the RAND Corporation that seeks to actively improve the health and social and economic well-being of populations and communities throughout the world. This research was conducted in the Justice Policy Program within RAND Social and Economic Well-Being. The program focuses on such topics as access to justice, policing, corrections, drug policy, and court system reform, as well as other policy concerns pertaining to public safety and criminal and civil justice. For more information, email justicepolicy@rand.org.

About the Authors

Sean E. Goodison is a deputy director and senior research criminologist at the Police Executive Research Forum (PERF). His work focuses on quantitative research, research methodology, program evaluation, police use of technology, and national data collection efforts. He received his Ph.D. in criminology and criminal justice.

Dulani Woods is a data science practitioner adept at data acquisition, transformation, visualization, and analysis. His research typically focuses on justice and homeland security policy. He began his career as a Coast Guard Officer on afloat and ashore assignments in Miami, Florida; New London, Connecticut; and Baltimore, Maryland. He holds an M.S. in agricultural economics (applied economics).

Jeremy D. Barnum is a research associate at PERF. He specializes in geographic information science (GIS), spatial data analysis, policing, and crime prevention. Prior to joining PERF, he was a project manager for the Rutgers Center on Public Security. He holds a M.A. in criminal justice.

Adam R. Kemerer is a senior research assistant at PERF. He has contributed to work on police technology, the opioid epidemic, and law enforcement responses to sexual assault investigations. He has a bachelor's degree in economics and political science.

Brian A. Jackson is a senior physical scientist at the RAND Corporation. His research focuses on criminal justice, homeland security, and terrorism preparedness. His areas of examination have included safety management in large-scale emergency response operations, the equipment and technology needs of criminal justice agencies and emergency responders, and the design of preparedness exercises. He has a Ph.D. in bioinorganic chemistry.

About This Report

On behalf of the U.S. Department of Justice, National Institute of Justice (NIJ), the RAND Corporation, in partnership with the Police Executive Research Forum (PERF), RTI International, and the University of Denver, is carrying out a research effort to assess and prioritize technology and related needs across the criminal justice community. This initiative is a component of NIJ's National Law Enforcement and Corrections Technology Center (NLECTC) System and is intended to support innovation within the criminal justice enterprise. For more information about the NLECTC Priority Criminal Justice Technology Needs Initiative, see www.rand.org/jie/justice-policy/projects/priority-criminal-justice-needs.

This report is one product of that effort. It presents the results of an expert workshop focused on identifying and prioritizing ways to conduct criminal investigations involving evidence on the dark web. This report and the results it presents should be of interest to law enforcement agencies at the state and local level, research and operational criminal justice agencies at the federal level, private-sector technology providers, and policymakers active in the criminal justice field. Mentions of products or companies do not represent approval or endorsement by NIJ or the RAND Corporation.

NIJ | National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

This publication was made possible by Award Number 2013-MU-CX-K003, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.html. For more information on this publication, visit www.rand.org/t/rr2704.

© Copyright 2019 RAND Corporation

www.rand.org

RAND CORPORATION

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

RR-2704-NIJ