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

RESEARCH —— Published Oct 29, 2019

A s more activities of daily life move online, criminals and criminal activity have followed. With the advent of the dark web, criminals can conduct their activities in ways that are difficult for law enforcement to discover, monitor, and investigate. The dark web provides anonymity and encryption, which significantly complicates the process of identifying suspects and collecting evidence. 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. Workshop participants identified 46 potential solutions, or needs, which include improving training for law enforcement officers, sharing information across jurisdictions, and investigating the gaps and shortcomings in current laws related to searching packages.

Key Findings

Improving training and information sharing will likely have the greatest impact

- Increased 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 lack of knowledge about what the dark web is and how criminals leverage it

- Investigating officers often overlook physical artifacts that are indicative of dark web activities when collecting evidence during a criminal investigation. These artifacts might include notes that identify 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 prove that a crime has been committed.

Recommendations

- Invest in training at all levels, from the most-junior to the most-senior officers.

- Invest in improving information sharing across agencies, both within the United States and internationally.

- Examine the benefits of investing further 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., electronic crime) that has the potential to affect the health and welfare of populations both near and far.

Topics

Cybercrime

Data Privacy

Delphi Method

The Internet

Law Enforcement

Document Details

Objective Analysis.
Effective Solutions.

RAND 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.