Assessment

(U) Terrorist Use of Improvised Incendiary Devices and Attack Methods

IA-0186-10

Office of Intelligence and Analysis
ASSESSMENT

(U) Terrorist Use of Improvised Incendiary Devices and Attack Methods

16 March 2010

(U) Prepared by the DHS/I&A Domestic Threat Analysis Division, Infrastructure Threat Analysis Branch. This product is one in a series of intelligence assessments published by the DHS/Domestic Threat Analysis Division as part of the efforts of the DHS/Homeland Infrastructure Threat and Risk Analysis Center to facilitate a greater understanding of the emerging threats to the United States. This information is provided to support the activities of the Department and to assist federal, state, and local government counterterrorism and law enforcement officials in effectively deterring, preventing, preempting, or responding to terrorist attacks against the United States. Coordinated with the DHS/Office for Bombing Prevention, DHS/TSA Office of Intelligence, and the FBI/WMD Directorate. The Interagency Threat Assessment and Coordination Group reviewed this product from the perspective of our nonfederal partners.

(U) Scope

(U//FOUO) This assessment describes terrorists' use of improvised incendiary devices and the impact this attack method may have on U.S. critical infrastructure. It does not address terrorist intentions to use incendiary devices to attack specific U.S. critical infrastructure.

(U) Key Findings

(U//FOUO) Improvised incendiary devices (IIDs) typically are less expensive to make than improvised explosive devices but still are capable of creating mass casualties and causing widespread fear and panic.

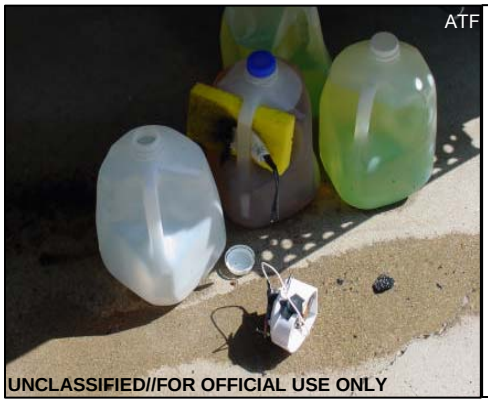
(U//FOUO) Improvised incendiary devices (IIDs) can be constructed easily from everyday materials available at hardware and grocery stores.

(U//FOUO) IIDs can be used against many types of infrastructure targets; violent extremists have used them successfully in attacks in the United States and overseas.

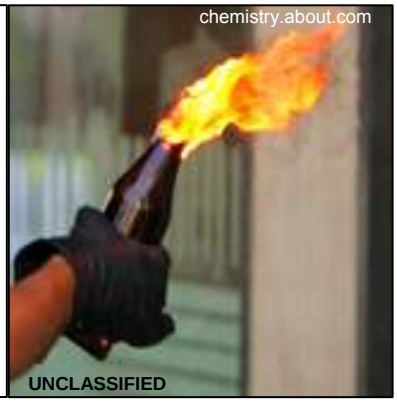
(U//FOUO) The DHS/Office of Intelligence and Analysis (I&A) has no credible or specific intelligence indicating current terrorist attack planning featuring use of IIDs against infrastructure in the United States. The ease with which IIDs can be constructed and used, however, makes it difficult to detect and prevent such attacks.

(U) Improvised Incendiary Devices Can Be Constructed from Common Materials

(U//FOUO) An IID consists of an ignition source, a flammable or combustible fuel —including kerosene, cigarette and charcoal lighter fluid, motor fuels, such as gasoline or diesel, and reactive chemicals—and some type of container, such as propane cylinders, plastic pipes, bottles, and cans. IIDs range in sophistication from very simple and easily-constructed Molotov cocktails—which are made by filling a glass bottle with fuel and lighting a rag placed in the top—to more complicated timed devices consisting of a sodium and acid mixture.



(U) Figure 1: Typical IID components.



(U) Figures 2 and 3: Unlighted and lighted Molotov cocktails.

(U//FOUO) Advantages of Improvised Incendiary Devices

- (U//FOUO) The materials needed to construct an IID can be obtained easily from many retail stores. Even with heightened public awareness, the purchase of components and fuels is not likely in most cases to arouse suspicion.
- (U//FOUO) Incendiary devices require little training to prepare and use. Flammable materials generally are not as volatile as explosives and require less skill and expertise in handling.
- (U//FOUO) Properly used and strategically placed, IIDs can cause damage over a widespread area as the fuel may rapidly create and sustain a fire that is difficult for first responders to contain.
- (U//FOUO) For terrorists seeking to preserve anonymity, IIDs improve prospects for destroying evidence, while those seeking publicity can benefit from the media coverage that a fire will attract.

(U) U.S. Infrastructure Vulnerable to Improvised Incendiary Device Attack

(U//FOUO) The accessibility of many types of infrastructure, such as government facilities, national monuments, various transportation and energy assets, and commercial facilities, make them susceptible to IID attacks. Passenger trains, ferries, and other public conveyances are among the more attractive targets for terrorists because they often have large numbers of people enclosed in concentrated areas that are difficult to evacuate rapidly.

(U) Previous Use of Improvised Incendiary Devices in the United States

(U//FOUO) Violent extremists have used IIDs against government facilities and vehicles, commercial facilities, and railroad lines. Their most frequent targets have been healthcare, educational and research facilities, and scientists and research personnel.

(U) Improvised Incendiary Device Attacks Abroad

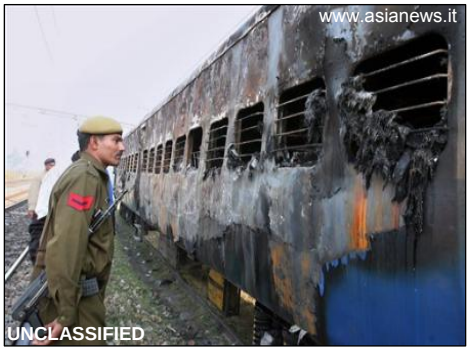
(U) Terrorists using IIDs achieved their most notable success in a February 2007 attack by Kashmiri operatives who placed six suitcase IIDs in three cars of the “Friendship Express” passenger train traveling from India to Pakistan. Four of the six IIDs ignited, causing fires in two passenger cars that killed 68 people and injured 13. Other incidents, like those in the United States, have achieved mixed results.

- (U) In May 2008, an ethnic Uighur woman aboard a domestic flight bound for Beijing, China attempted to ignite a flammable liquid in a beverage can. She aroused suspicions when she exited the lavatory to pick up a second can after the first failed to ignite and produced a smell of gasoline.

— (U) In June 2007, two men drove a burning jeep with several gasoline-filled containers into the main terminal building at the Glasgow, Scotland airport, causing structural damage to the front of the building but no casualties.

— (U) In July 2006, two men plotted to attack two trains in Germany using suitcases filled with butane and gasoline, but the devices failed to ignite. German prosecutors claimed, however, that the trains would have become "balls of fire" had the IIDs functioned as planned.

(U) Figure 5: Burning vehicle driven into Glasgow Airport terminal.



(U) Figure 6: Indian passenger rail car destroyed by IIDs.

(U) Protective Measures

(U) IIDs pose complex security challenges for all critical infrastructure sectors. The principal objectives for implementing protective measures against an IID are to complicate attack planning and surveillance, protect potential targets, and mitigate the risk of attack. To reduce vulnerabilities to an attack using IIDs, the DHS/Office for Bombing Prevention recommends these protective measures:

— (U) Establish a public awareness and vigilance campaign that reinforces public awareness of threats posed by IIDs.

— (U) Ensure that a simple and consistent mechanism is in place to report suspicious activities.

— (U) Maintain a visible police and security presence, such as access control and perimeter security at various locations within at-risk venues, especially at entrance sites and choke points.

— (U) Institute random security procedures to complicate attack planning, including screening of baggage, packages, and parcels that enter facilities that may be potential targets.

— (U) Ensure that security personnel review surveillance detection and countersurveillance procedures to establish awareness of possible attack planning.

— (U) Identify potential locations that could be used as staging or assembly sites for IIDs.

— (U) Inform service industry and hotel employees to be alert to indicators of attack planning activities, such as maps, photographs, and communications equipment.

— (U) Establish and rehearse evacuation protocols for IID attacks (for example, fire drills and code words) and identify and predesignate primary and secondary evacuation routes and assembly areas for building or site occupants.

(U) Outlook

(U//FOUO) Law enforcement officials and homeland security personnel need to be aware that IIDs can be constructed easily and used against a variety of targets with little or no prior detection. IIDs provide an alternative to explosives or other, more easily detectable weapons such as handguns and improvised explosive devices (IEDs), and require additional vigilance by security personnel and longer screening times.

(U) Reporting Notice:

(U) DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the nearest state and local fusion center and to the local FBI Joint Terrorism Task Force. The nearest state and local fusion centers' contact information can be found online at http://www.dhs.gov/files/resources/editorial_0306.shtm. The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm and the DHS National Operations Center (NOC) can be reached by telephone at (202) 282-9685 or by e-mail at NOC.Fusion@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at (202) 282-9201 or by e-mail at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) Detailed information on improvised incendiary devices is provided for law enforcement by the Department of Homeland Security at TRIPwire.dhs.gov or TRIPwire Community Gateway (http://cs.hsin.gov) if you are a member of the private sector. If you need access to either system, please contact help@tripwire.dhs.net. For further information on TRIPwire and bombing prevention contact the DHS/Office for Bombing Prevention at obp@dhs.gov.

(U) DHS/I&A would like to invite you to participate in a brief customer feedback survey regarding this product. Your feedback is extremely important to our efforts to improve the quality and impact of our products on your mission. Please click below to access the form, then follow a few simple steps to complete and submit your response. Thank you.

Survey

(U) Tracked by: HSEC-03-00000-ST-2009

Office of Intelligence and Analysis

I&A Customer Survey

Product Title:

Product Classification: Select One Type of Partner: Select One

1. How did you use this product in support of your mission?

- ☐ Integrated into one of our finished information or intelligence products
- ☐ Shared contents with federal or DHS component partners
  - If so, which partners
- ☐ Shared contents with state and local partners
  - If so, which partners
- ☐ Shared contents with private sector partners
  - If so, which partners
- ☐ Other (please specify)

2. Please rank this product's relevance to your mission.

Critical: ○ Very important: ○ Somewhat important: ○ Not important: ○ N/A: ○

Comment:

3. How could our product or service be improved to increase its value to your mission?

Comment:

4. If this product was supplied in response to a specific request - please rate your satisfaction with each of the following services provided by I&A:

	Very Satisfied	*Somewhat Satisfied*	*Somewhat Dissatisfied*	*Very Dissatisfied*	*N/A*
(a) Timeliness of Product or Support	○	○	○	○	◉
(b) Communication During Processing of Your Request	○	○	○	○	◉
(c) Responsiveness to Your Questions	○	○	○	○	◉

** To help us understand more about your organization so we can better tailor future products, please provide:*

Your Organization:

Your Name/Position:

Your contact # or email:

Submit to IA.feedback@hq.dhs.gov - **Submit Request**