Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 19 — Issue 34 | September 19, 2019

Robots find safer ways to map, search subterranean environments

It may seem more like a version of BattleBots or Robot Wars: teams build several robots to navigate underground environments in a timed competition, completing a set of graded tasks. But these teams are working with the Defense Advanced Research Projects Agency (DARPA) to find better ways to rapidly map, navigate and search underground environments sometimes seen in disaster response or combat operations.

DARPA's Subterranean, or "SubT," Challenge runs through 2021, with 11 teams testing robots and aerial drones – and even one mini blimp – in three different underground subdomains: a tunnel system, an urban underground and a cave network. Each subdomain can span miles, and some of them involve multiple levels, giving teams quite a challenge when building robots to navigate them.

Teams must attempt to remotely map the subdomain, identify artifacts (such as a fire extinguisher installed on the side of a cave wall) and report the greatest number of artifacts in the underground environment. Teams must build several robots to handle different tasks or terrain, but they must be able to communicate with each other and work together to manage obstacles with limited human input.

Pushing technology to its limits with innovation and good-natured competition will have an impact on future disaster response and military operations. These challenges expand capabilities of remote exploration in areas too dangerous to send people. The information learned from these challenges will steer future technological development.

Teams completed the tunnel challenge last month in two Pittsburgh coal mines dubbed the experimental tunnel and safety research tunnel. See all the DARPA SubT Challenge videos and follow future testing on the DARPAtv YouTube channel.

(Source: DARPA)

National Fire Academy admissions process goes online

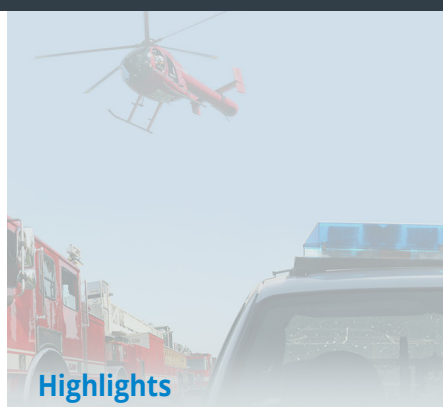
The application period for the National Fire Academy (NFA) second semester, which runs April 1-September 30, 2020, opens October 15, 2019. New this year, NFA will be accepting applications online.

Applying online gives you your best chance to successfully submit your application and have it accepted by the NFA. As with the paper applications, you will need to:

- Have a Federal Emergency Management Agency Student Identification number.
- Know the course requirements and have prerequisite documents electronically.
- Verify the name and email address of the person authorized to approve your application.

It is vital you have all this information ready as incomplete applications will be denied.

Watch the U.S. Fire Administration website on October 15 for the new online application system. All questions concerning the admissions process should be



Highlights

U.S. Fire Administration

The U.S. Fire Administration operates the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC).

For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: (301) 447-1325 and/or emr-isac@fema.dhs.gov.

Subscribe here

directed to the NFA Admissions Office Monday – Friday between 7 a.m. – 4:30 p.m. Eastern, at 800-238-3358, ext. 1035, or by email at netcadmissions@fema.dhs.gov.

(Source: USFA)

Public Health System Training for Disaster Recovery

The "Public Health System Training in Disaster Recovery" (PH STriDR) program from the National Center for Disaster Medicine and Public Health (NCDMPH) gives employees of local public health agencies a better understanding of the disaster recovery process and their part in it.

Available free online, PH STriDR focuses on individual and organizational contributions to disaster recovery. Its four 90-minute modules cover the following:

- Basic concepts in disaster recovery.
- Worker roles.
- Common personal, family and workplace issues.
- What a successful recovery in their agency and community might look like.

PH STriDR uses the train-the-trainer approach with each agency choosing the trainer. Materials include a Trainer guide; PowerPoint presentations with Trainer Notes; four Learner worksheets; and several supporting items for each sessions.

This training would benefit any public health agency interested in strengthening its role in community disaster recovery.

(Source: Uniformed Services University)

Webinar: Staffing 911 Centers in the Era of NG911

Ultimately, it is a community decision to pay for technologies and staffing to support Next Generation 911 (NG911). NG911 can provide different kinds of information to public safety agencies, but it also requires changes to 911 center staffing, hours, workload and training.

Prior to NG911 adoption, PSAPs need to measure staff workload and performance. Accurate data is crucial when determining how much additional staff time may be needed to handle work generated by new NG911 capabilities.

On Thursday, October 3, 2019 at 1 p.m. Eastern, Justice Clearinghouse is hosting "Staffing 911 Centers in the Era of NG911," a webinar to help 911 centers identify and answer these questions. Registration is required for this webinar.

This webinar addresses methods for quantifying call taker and dispatcher workload for police, fire and EMS. It will cover analysis methods for determining the amount of work that translates into numbers of full time call takers and dispatchers needed in a community.

By the end of the webinar, attendees should have clear guidance on how to establish an effective, ongoing data collection and analysis process that can measure staffing needs when NG911 technologies are being proposed in their communities.

See more Justice Clearinghouse webinars on its events calendar.

(Source: Justice Clearinghouse)

Cyber Threats

Mayor describes city's decision not to pay $5.3 million ransom

The mayor of New Bedford, Massachusetts, took the unusual step this week of holding a press conference to describe a recent ransomware attack and **explain why the city decided not to pay the $5.3 million ransom that was demanded**.

Since New Bedford first detected the ransomware attack on July 5, its management information systems department has completely rebuilt its server network, restored most software applications and replaced all of the computer workstations that were affected, the mayor said on Wednesday.

(Source: DataBreachToday)

How much cybercriminals pay for hacked information

The Dark Web is awash with both commoditized and creative black market goods and services targeted for cybercriminals of all kinds. Whether the bad guys are looking for ransomware-as-a-service to take systems hostage for profit, seeking personally identifiable information they can use to commit identity theft, or looking for hacking tools to collect that information themselves, **there's always someone in the black-market supply chain willing to provide a product for a price**.

Researchers recently released a report with detailed analysis on just exactly what those prices look like for many common black market products. Those findings, along with data from recent reports released by researchers at Deloitte and ESET within the last year, were compiled for this guide on just what crooks invest to fuel their online criminal enterprises.

(Source: DarkReading)

Emotet is back, why you should be concerned

After a lull over the summer, Emotet banking trojan is back in the news. In fact, according to the Multi-State Information Sharing and Analysis Center (MS-ISAC), Emotet was the top malware reported last month.

Emotet targets individuals, companies and government entities and steals banking login information and financial data. This allows attackers to steal money from banks using stolen banking credentials.

(Source: MalwareBytes)

Widespread security flaw in GPS trackers

Researchers have discovered serious security vulnerabilities in some 600,000 child and pet trackers for sale on Amazon.com and other large online merchants. **The devices expose data sent to the cloud, including the exact real-time GPS coordinates**. Twenty-nine models of trackers showed the vulnerabilities.

The vulnerabilities impacting these trackers can allow unauthorized parties to spoof user location, access the microphone, view personal user information, send SMS messages and install new firmware. The user accounts associated with the trackers use default passwords and the data transferred between the devices and online accounts is routed through the insecure hypertext transfer protocol (HTTP).

(Source: Avast)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.