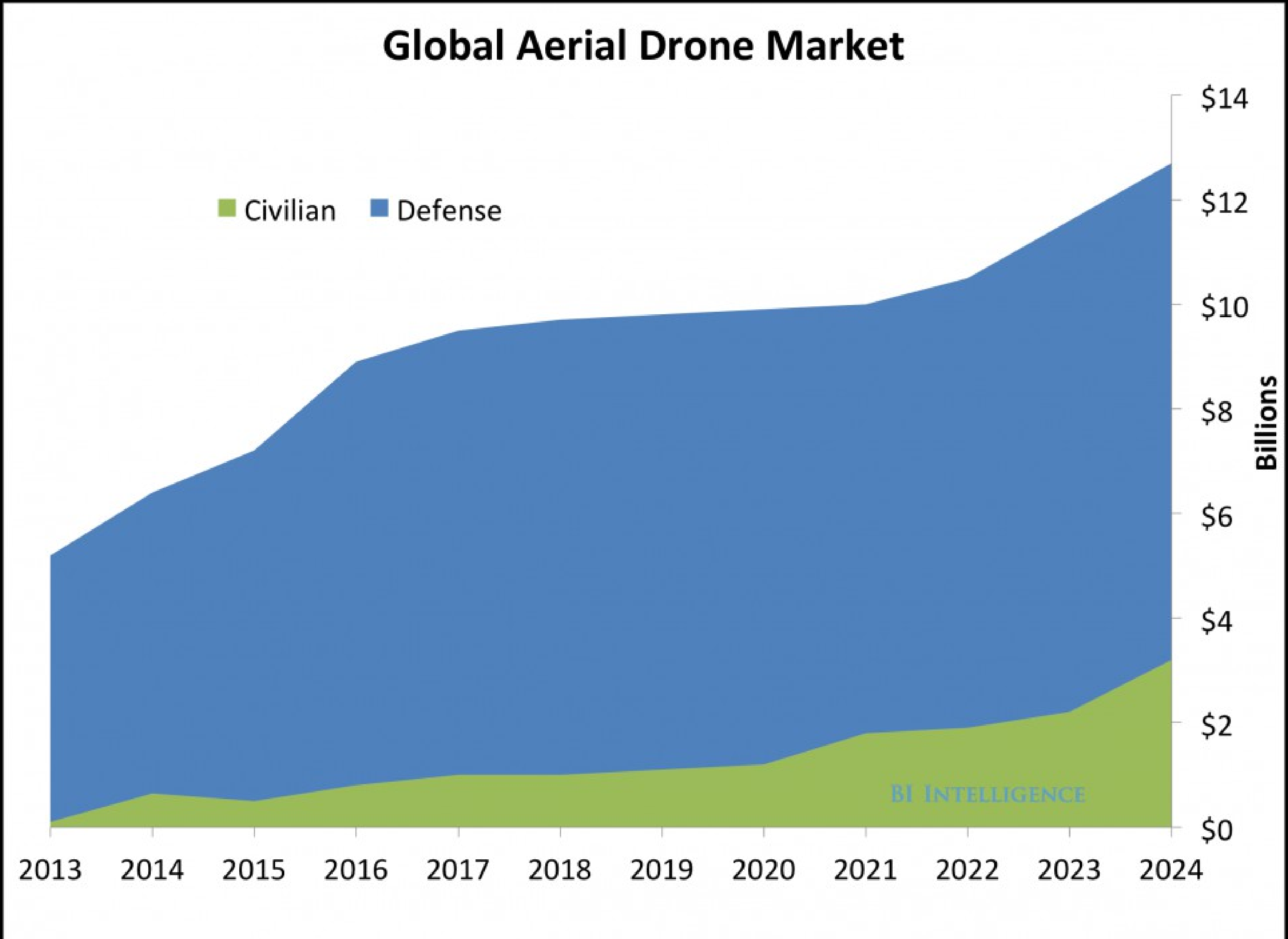
Trusted Software Repair for System Resiliency

Tethered Flight Repair *Demonstration*

Joint Demonstration

- University of Virginia team
  - Carnegie Mellon University – Claire Le Goues
  - University of California, Los Angeles – Miryung Kim
  - University of New Mexico – Stephanie Forrest
  - University of Virginia – Westley Weimer
    - Kevin Angstadt, Jonathan Dorn, Kevin Leach
- Raytheon BBN team
  - Shane Clark, Partha Pal, Aaron Paulos



Sources: Teal Group, BI Intelligence Estimates, Michael Toscano

UAV deployment is projected to increase substantially

Systems Must Be Resilient to Attacks and new Environments

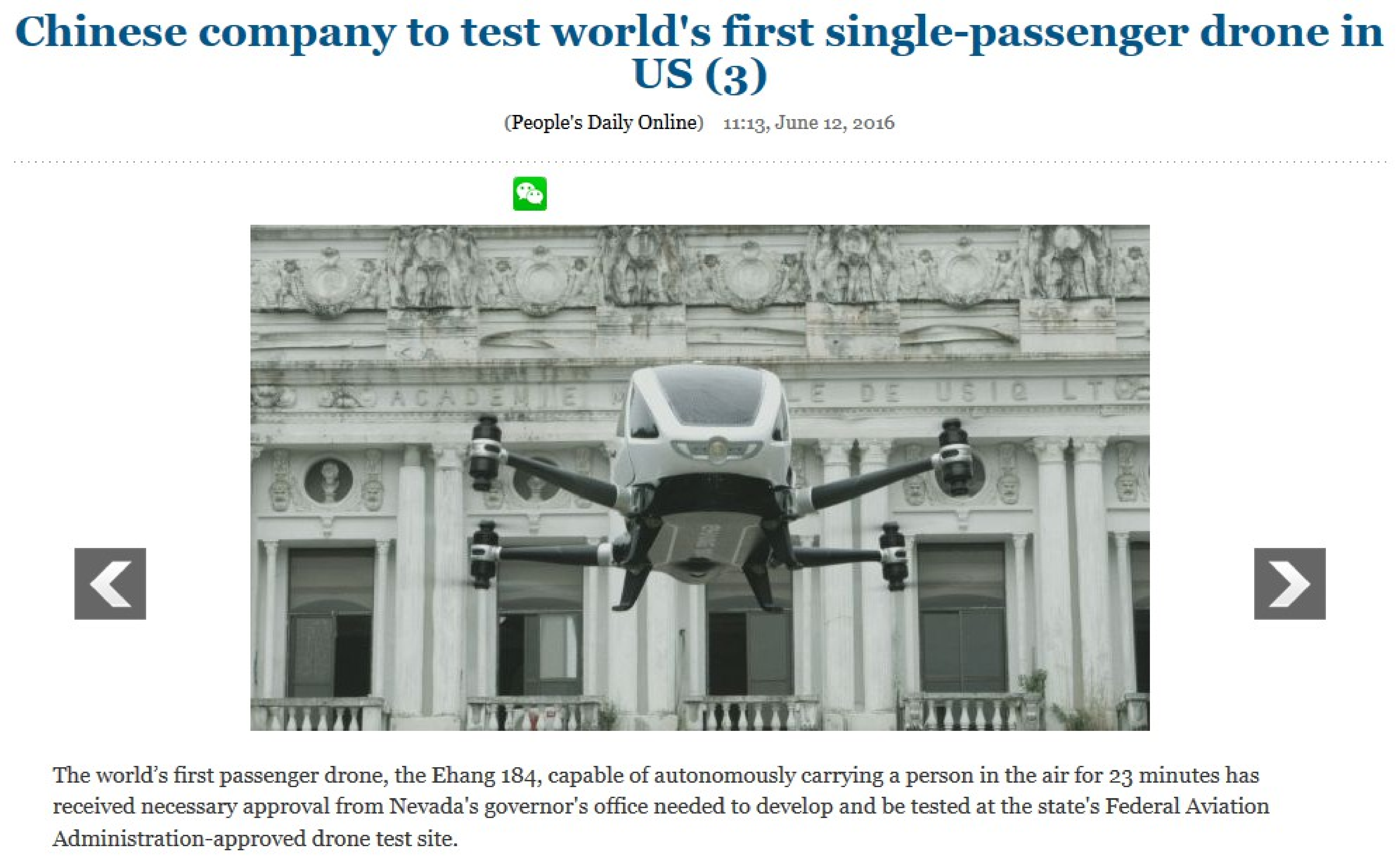
2014 Triathlete injured by UAV
"someone hacked or 'channel-hopped' the drone, taking over the controls"

Enrique Iglesias's fingers sliced by UAV during concert (2015)
"Iglesias reached out to the flying device as it photographed the audience"

Resiliency is not always present …

Google Self-Driving Car pulled off the road for traffic violation (November 2015)

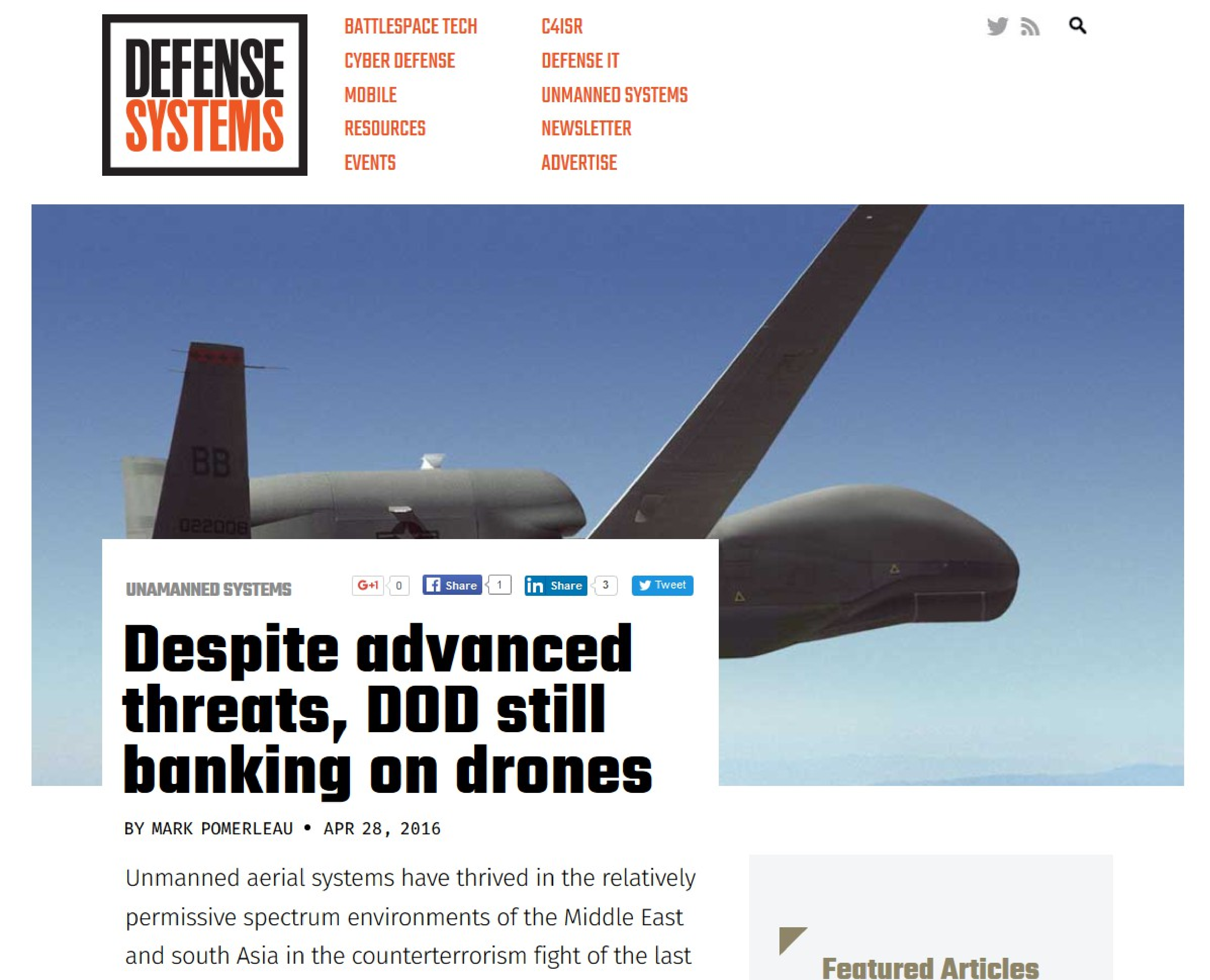
More than 400 large U.S. military drones have crashed in major accidents around the world since 2001, a record of calamity […], according to a year-long Washington Post investigation.



Chinese company to test world's first single-passenger drone in US (3)

(People's Daily Online) 11:13, June 12, 2016

The world's first passenger drone, the Ehang 184, capable of autonomously carrying a person in the air for 23 minutes has received necessary approval from Nevada's governor's office needed to develop and be tested at the state's Federal Aviation Administration-approved drone test site.



UNAMANNED SYSTEMS

Despite advanced threats, DOD still banking on drones

BY MARK POMERLEAU • APR 28, 2016

Unmanned aerial systems have thrived in the relatively permissive spectrum environments of the Middle East and south Asia in the counterterrorism fight of the last

Featured Articles

Can we provide UAV systems with resiliency while admitting operator trust during deployment?

Terminology

Dependability

A measure of how consistently the UAV platform successfully completes its assigned mission.

Trustworthy

A UAV is trustworthy if the human operators believe it to be dependable.

Ex: DARPA High-Assurance Cyber Military Systems (HACMS)

Resilient

Capable of recovering from or avoiding human, platform or environmental factors that adversely affect the mission.

Ex: GenProg, Fault Tolerance Techniques

Desired Capability (joint UVA-BBN)

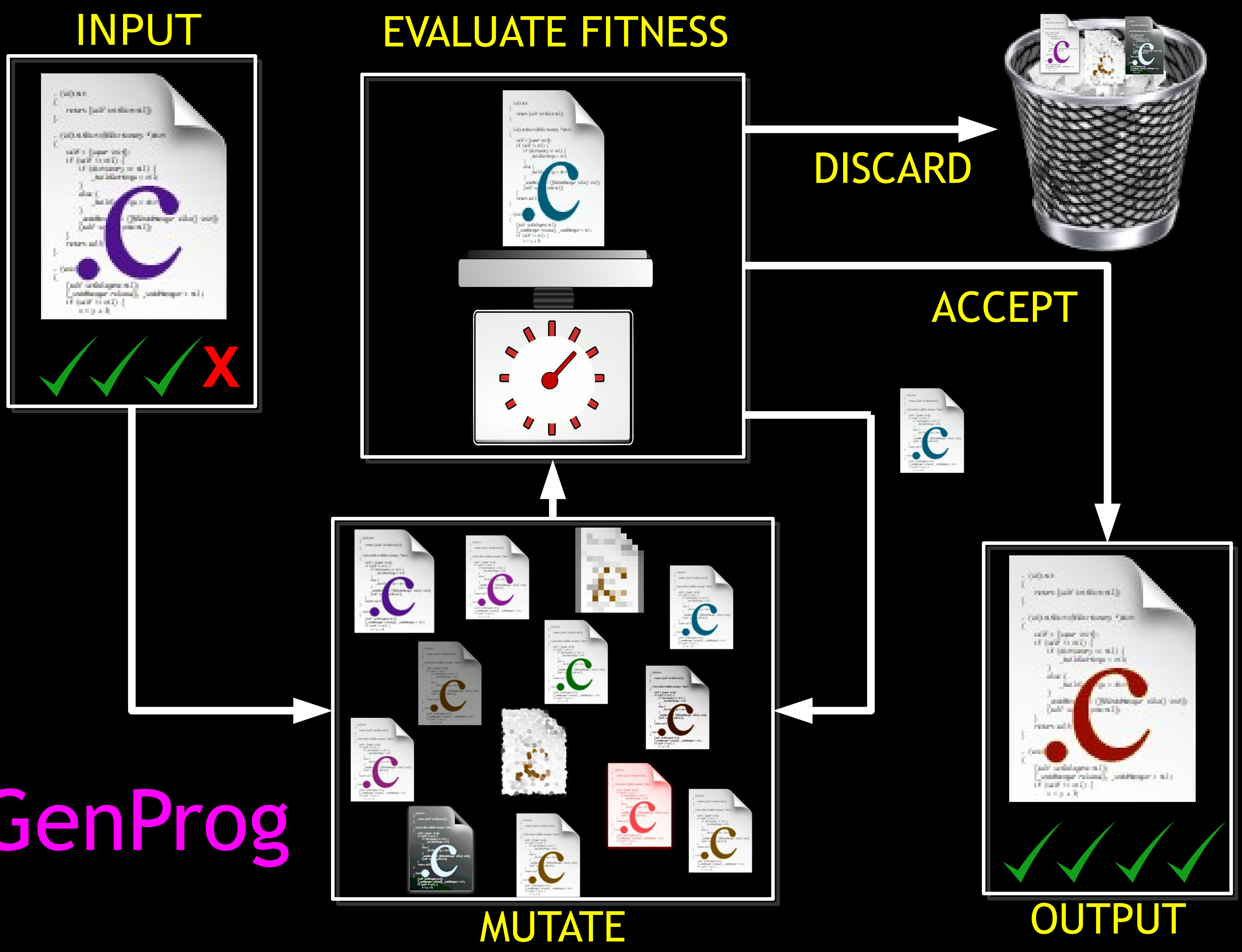
- Monitor a UAV mission
- Detect anomalies
- Devise repairs to software or data
- Deploy those repairs
- Complete and monitor the mission
- Provide evidence to support operator trust in the post-repair system

Resiliency and Trust

- Resiliency
  - Anomaly Detection (BBN)
  - Automated Program Repair (UVA)
  - Repair Deployment (UVA and BBN)
- Trust
  - Continuous Assessment of Trust (BBN)
  - Dynamic Execution Signals (UVA)
  - Targeted Differential Testing (UVA)
  - Invariants and Proofs (UVA)

Automated Program Repair

- Any of a family of techniques that generate and validate or solve constraints to synthesize program patches or run-time changes
  - Typical Input: program (source or binary), notion of correctness (passing and failing tests)
- Program repair provides resiliency
  - Powerful enough to repair serious issues like Heartbleed, format string, buffer overruns, etc.
- Efficient (dollars per fix via cloud computing)



INPUT

✓✓✓X

EVALUATE FITNESS

DISCARD

ACCEPT

MUTATE

OUTPUT

✓✓✓✓

GenProg

Resiliency and Trust

- Resiliency
  - Anomaly Detection (BBN)
  - Automated Program Repair (UVA)
  - Repair Deployment (UVA and BBN)
- Trust
  - Continuous Assessment of Trust (BBN)
  - Dynamic Execution Signals (UVA)
  - Targeted Differential Testing (UVA)
  - Invariants and Proofs (UVA)

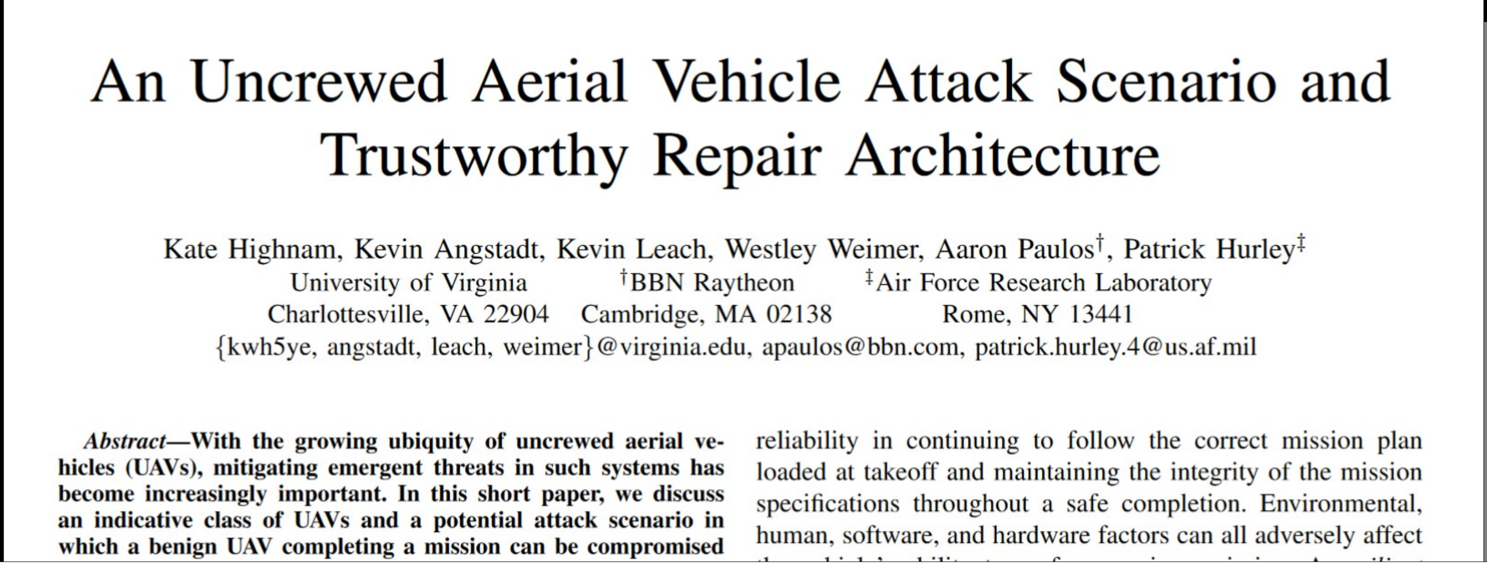
This Demo

30-month award
Start: March 1st, 2015
Now: ~17 months in

Demonstration Goals

- We will jointly demonstrate on
  - An indicative commercial UAV platform
  - An indicative mission
  - An indicative attack
- We will jointly demonstrate
  - In-flight attack detection
  - In-flight mission data repair
  - In-flight repair deployment
  - Complete and monitor post-repair mission

Direct Academic Publications

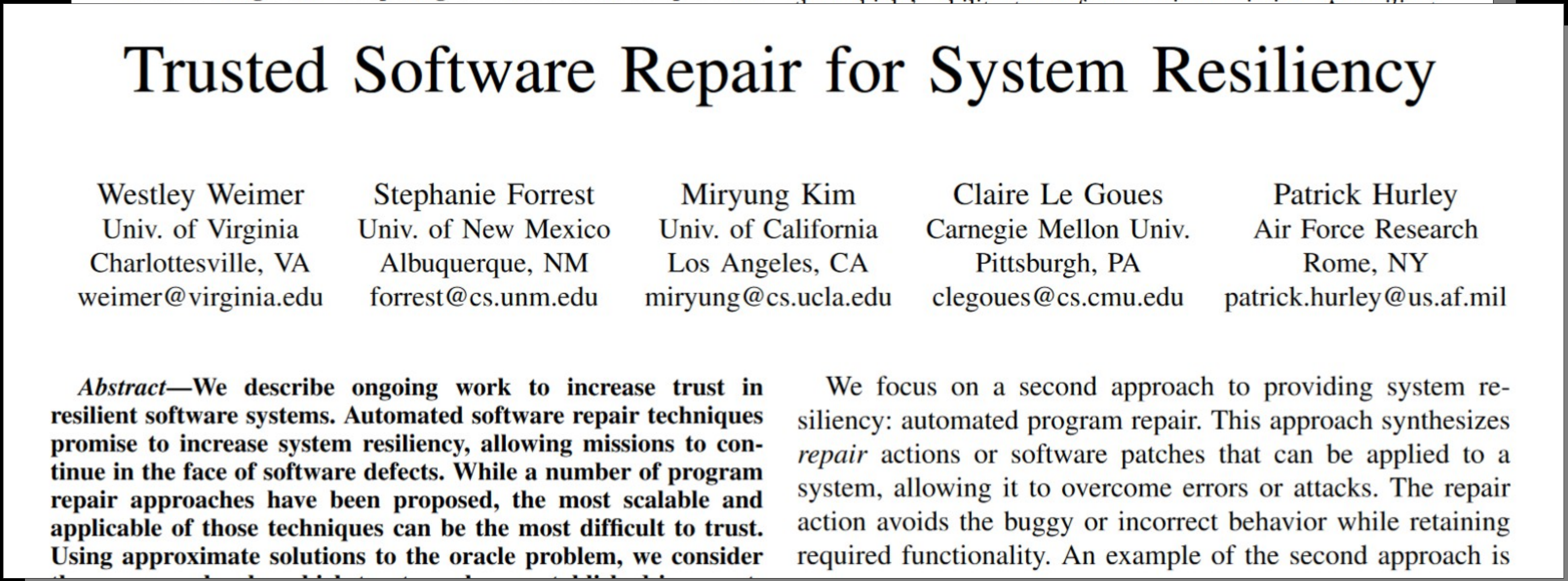


An Uncrewed Aerial Vehicle Attack Scenario and Trustworthy Repair Architecture

Kate Highnam, Kevin Angstadt, Kevin Leach, Westley Weimer, Aaron Paulos[†], Patrick Hurley[‡]
University of Virginia [†]BBN Raytheon [‡]Air Force Research Laboratory
Charlottesville, VA 22904 Cambridge, MA 02138 Rome, NY 13441
{kwh5ye, angstadt, leach, weimer}@virginia.edu, apaulos@bbn.com, patrick.hurley.4@us.af.mil

***Abstract*—With the growing ubiquity of uncrewed aerial vehicles (UAVs), mitigating emergent threats in such systems has become increasingly important. In this short paper, we discuss an indicative class of UAVs and a potential attack scenario in which a benign UAV completing a mission can be compromised**

reliability in continuing to follow the correct mission plan loaded at takeoff and maintaining the integrity of the mission specifications throughout a safe completion. Environmental, human, software, and hardware factors can all adversely affect



Trusted Software Repair for System Resiliency

Westley Weimer
Univ. of Virginia
Charlottesville, VA
weimer@virginia.edu

Stephanie Forrest
Univ. of New Mexico
Albuquerque, NM
forrest@cs.unm.edu

Miryung Kim
Univ. of California
Los Angeles, CA
miryung@cs.ucla.edu

Claire Le Goues
Carnegie Mellon Univ.
Pittsburgh, PA
clegoues@cs.cmu.edu

Patrick Hurley
Air Force Research
Rome, NY
patrick.hurley@us.af.mil

***Abstract*—We describe ongoing work to increase trust in resilient software systems. Automated software repair techniques promise to increase system resiliency, allowing missions to continue in the face of software defects. While a number of program repair approaches have been proposed, the most scalable and applicable of those techniques can be the most difficult to trust. Using approximate solutions to the oracle problem, we consider**

We focus on a second approach to providing system resiliency: automated program repair. This approach synthesizes *repair* actions or software patches that can be applied to a system, allowing it to overcome errors or attacks. The repair action avoids the buggy or incorrect behavior while retaining required functionality. An example of the second approach is

Schedule

- Today (rain permitting …)
  - Jonathan Dorn – Demonstration Details (Repair)
  - BBN Team – Demonstration Details (Detect, Trust)
  - Live Tethered Flight Demonstrations
    - Milton Airfield
    - Normal mission, undefeated attack, defeated attack
    - Optional: variant attack, flight software repair
  - Reconvene, Dinner
- Tomorrow
  - Presentations: Trust and Evidence