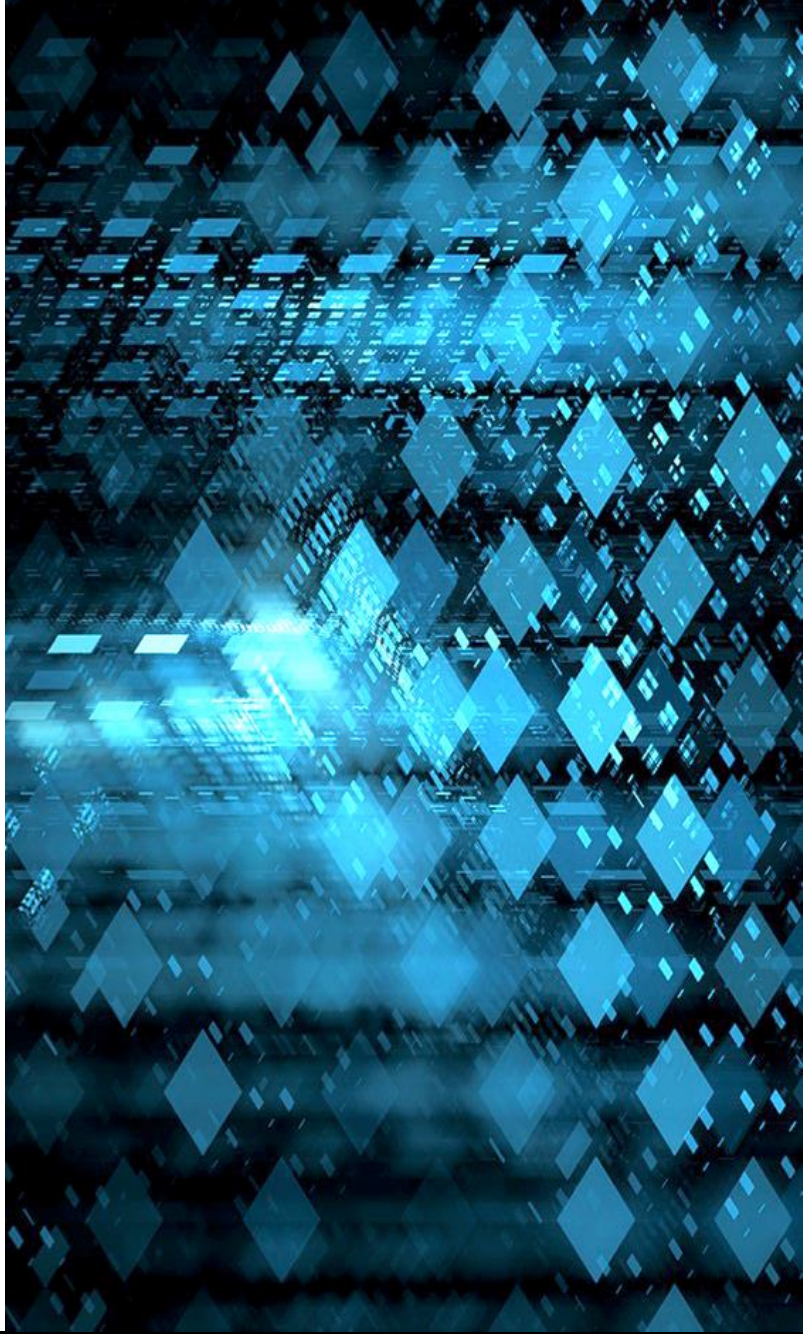
The Need for Operational and Cyber Resilience in Transportation Systems



January 14, 2016

Dr. Nader Mehravari, MBCP, MBCI

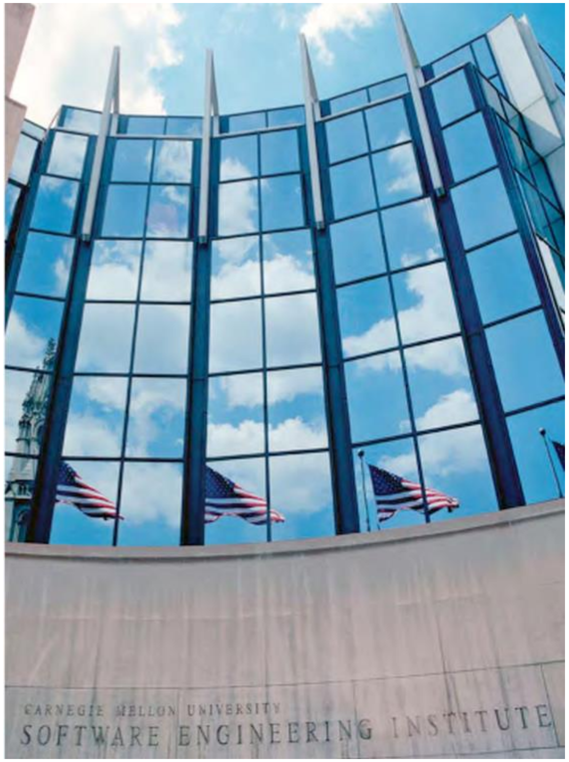
Cyber Risk and Resilience Management
Software Engineering Institute
Carnegie Mellon University
nmehravari@sei.cmu.edu
http://www.cert.org/resilience/

Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0003164

CERT | Software Engineering Institute | Carnegie Mellon



Carnegie
Mellon
University

Software Engineering Institute (SEI)

- Federally funded research and development center based at Carnegie Mellon University
- Basic and applied research in partnership with government and private organizations
- Helps organizations improve development, operation, and management of software-intensive and networked systems

CERT Division – *Anticipating and solving our nation’s cybersecurity challenges*

- Largest technical program at SEI
- Focused on internet security, secure systems, operational resilience, and coordinated response to security issues

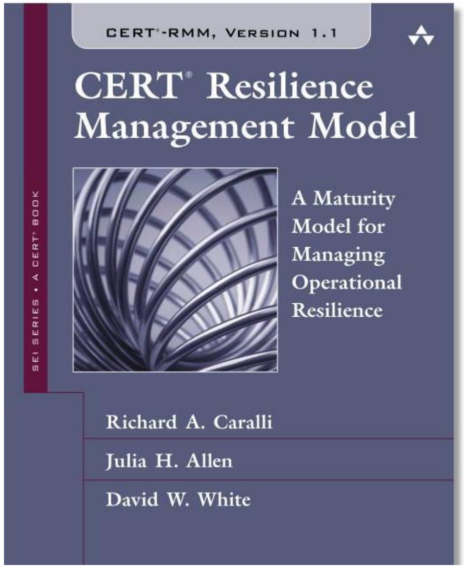
Cyber Risk & Resilience Management Team

Engaged in

- Applied research
- Education & training
- Putting into practice
- Enabling our federal, state, and commercial partners

In areas dealing with

- Resilience Management
- Operation Risk Management
- Cyber and Resilience Frameworks
- Integration of cybersecurity, business continuity, & disaster recovery



CERT®-RMM, Version 1.1

CERT® Resilience Management Model

A Maturity Model for Managing Operational Resilience

SEI Series • A CERT® Book

Richard A. Caralli

Julia H. Allen

David W. White

Contents

Operational Stress

Cyber-Induced Operational Stress on Transportation Sector

Prevention is Futile

Operational Resilience & Cyber Resilience

Techniques for Improving and Managing Cyber Resilience

Summary

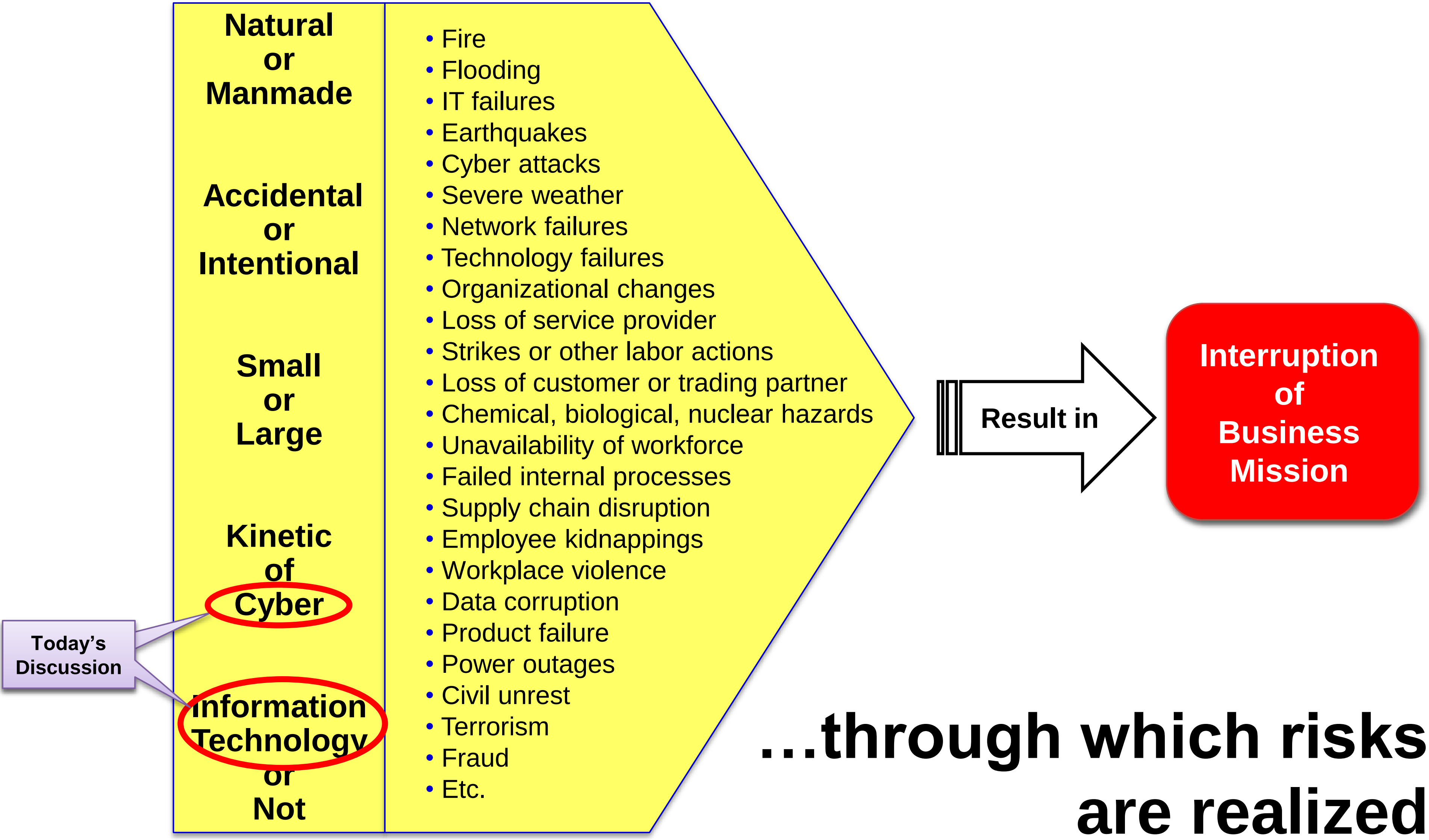
What do you see here?

A set of well looking evergreens.

Look Again!

A tree under **operational stress**

Operational Stress



Natural or Manmade

Accidental or Intentional

Small or Large

Kinetic of Cyber

Information Technology or Not

- Fire
- Flooding
- IT failures
- Earthquakes
- Cyber attacks
- Severe weather
- Network failures
- Technology failures
- Organizational changes
- Loss of service provider
- Strikes or other labor actions
- Loss of customer or trading partner
- Chemical, biological, nuclear hazards
- Unavailability of workforce
- Failed internal processes
- Supply chain disruption
- Employee kidnappings
- Workplace violence
- Data corruption
- Product failure
- Power outages
- Civil unrest
- Terrorism
- Fraud
- Etc.

Result in

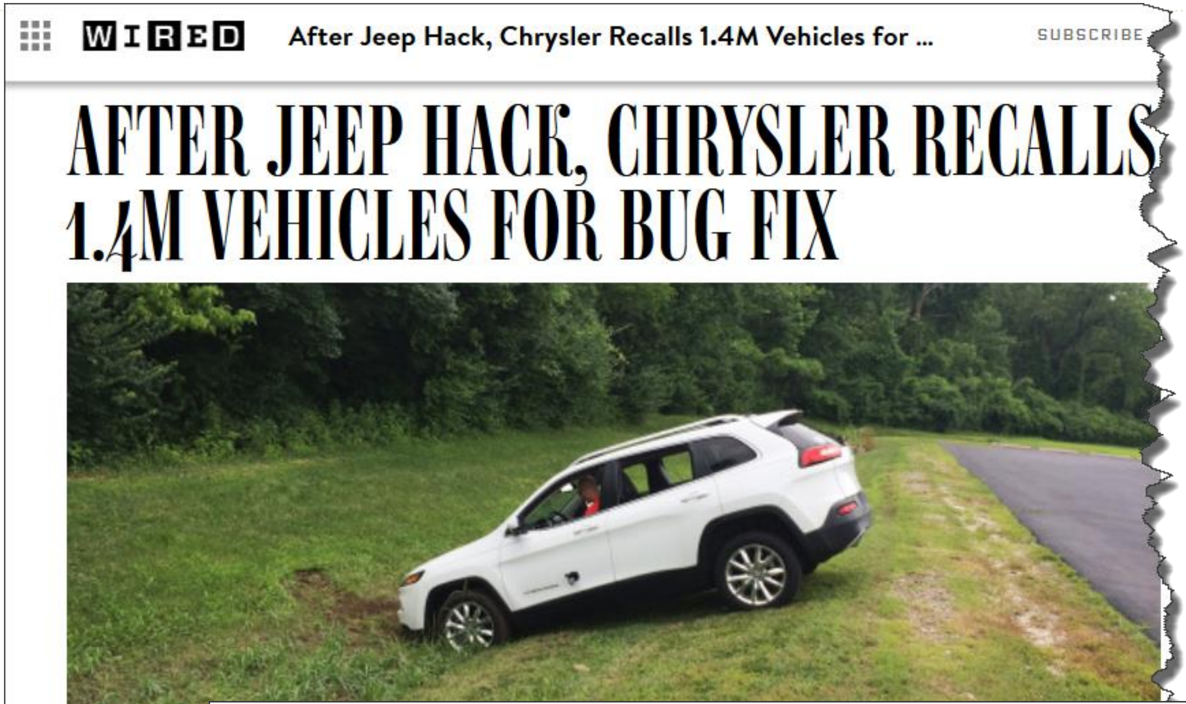
Interruption of Business Mission

Today's Discussion

…through which risks are realized

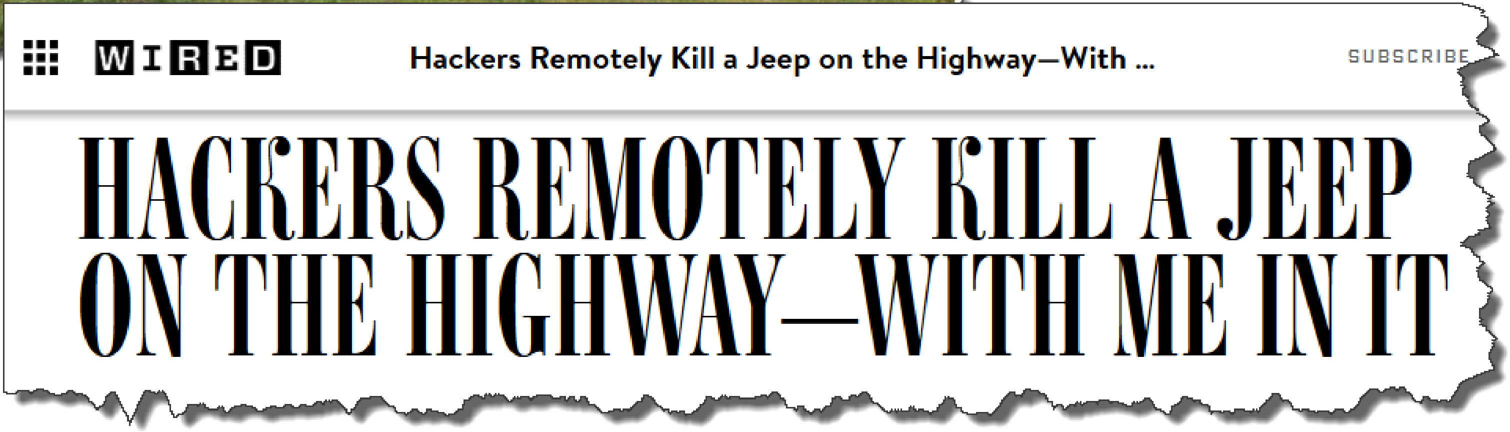
Examples of Cyber-Induced Operational Stress on Transportation Sector

July 2015



WIRED After Jeep Hack, Chrysler Recalls 1.4M Vehicles for ... SUBSCRIBE

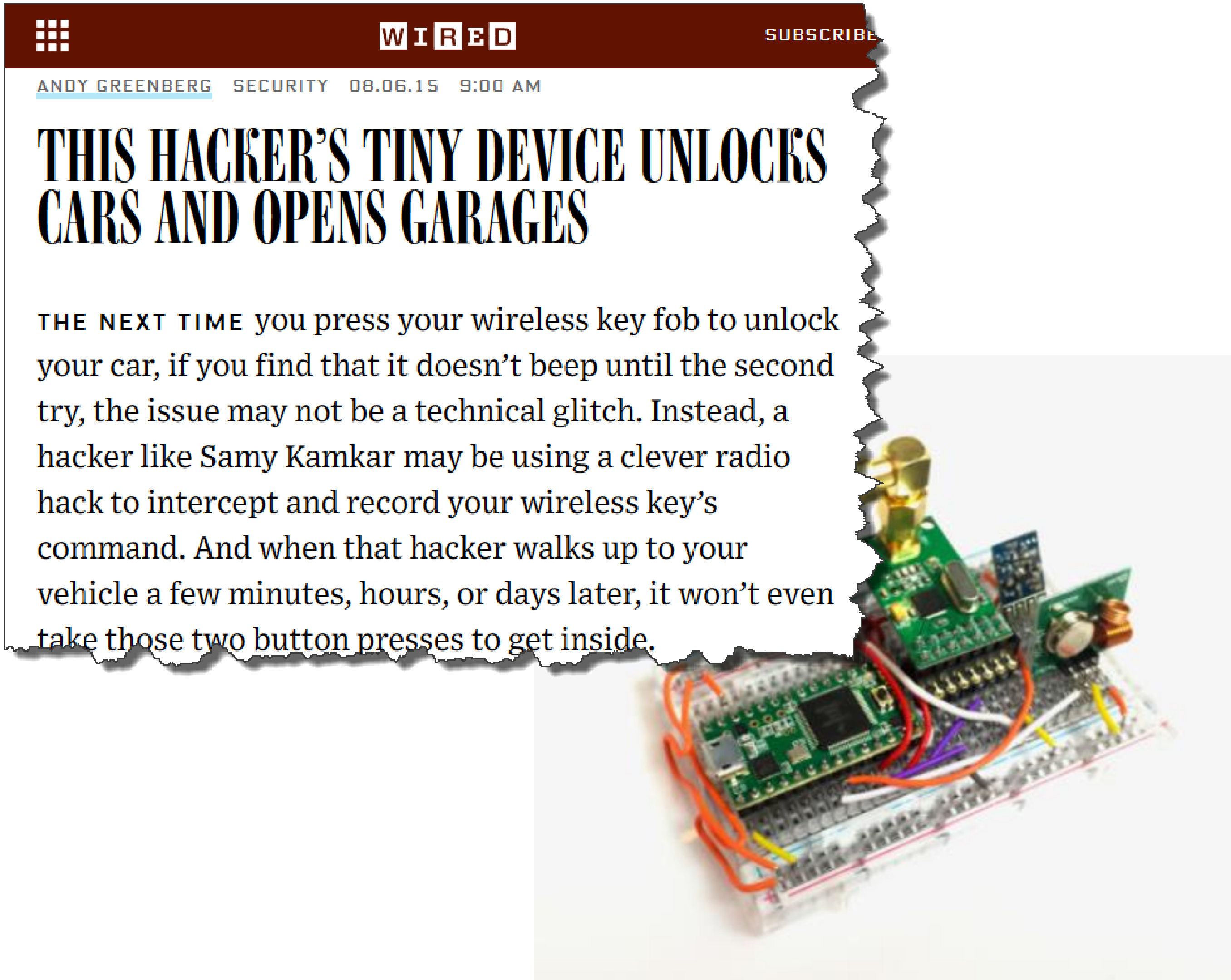
AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX



WIRED Hackers Remotely Kill a Jeep on the Highway—With ... SUBSCRIBE

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

August 2015

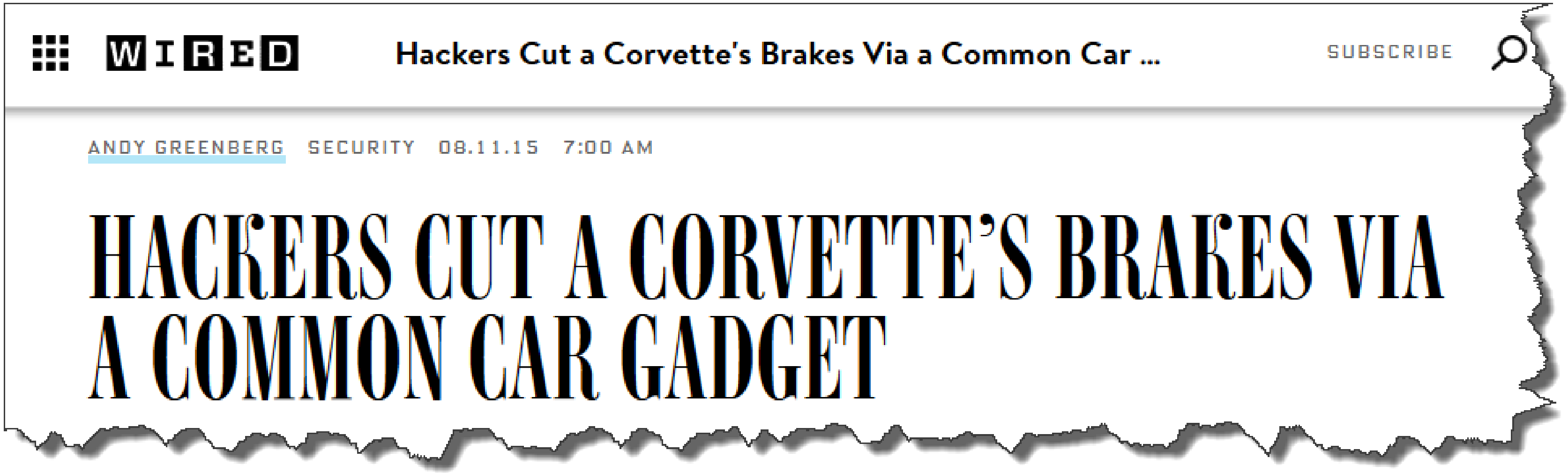


ANDY GREENBERG SECURITY 08.06.15 9:00 AM

THIS HACKER'S TINY DEVICE UNLOCKS CARS AND OPENS GARAGES

THE NEXT TIME you press your wireless key fob to unlock your car, if you find that it doesn't beep until the second try, the issue may not be a technical glitch. Instead, a hacker like Samy Kamkar may be using a clever radio hack to intercept and record your wireless key's command. And when that hacker walks up to your vehicle a few minutes, hours, or days later, it won't even take those two button presses to get inside.

August 2015



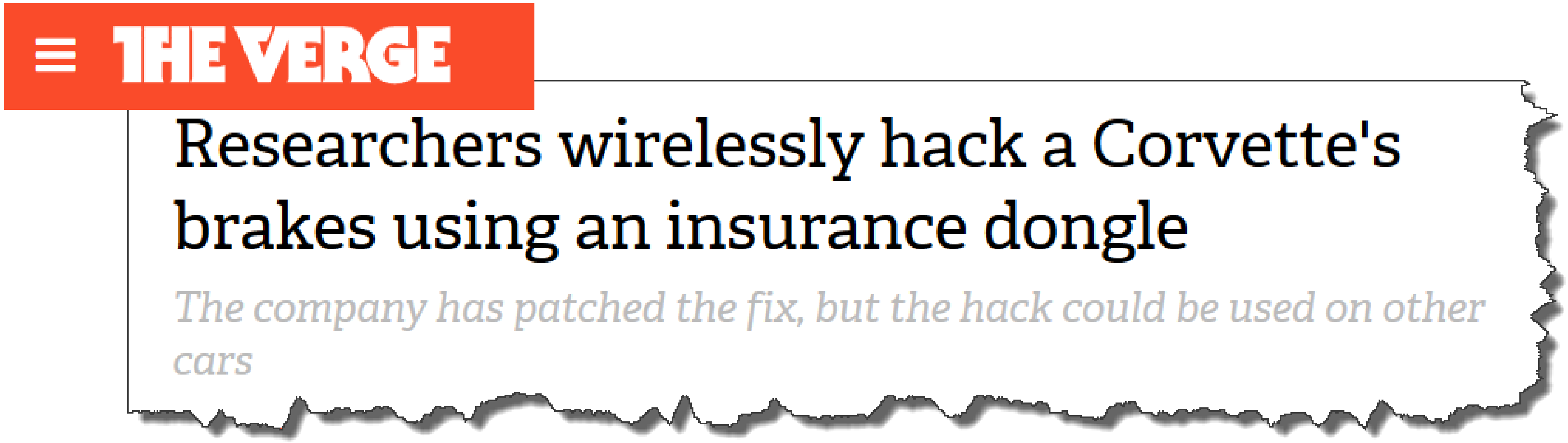
WIRED

Hackers Cut a Corvette's Brakes Via a Common Car ...

SUBSCRIBE

ANDY GREENBERG SECURITY 08.11.15 7:00 AM

HACKERS CUT A CORVETTE'S BRAKES VIA A COMMON CAR GADGET

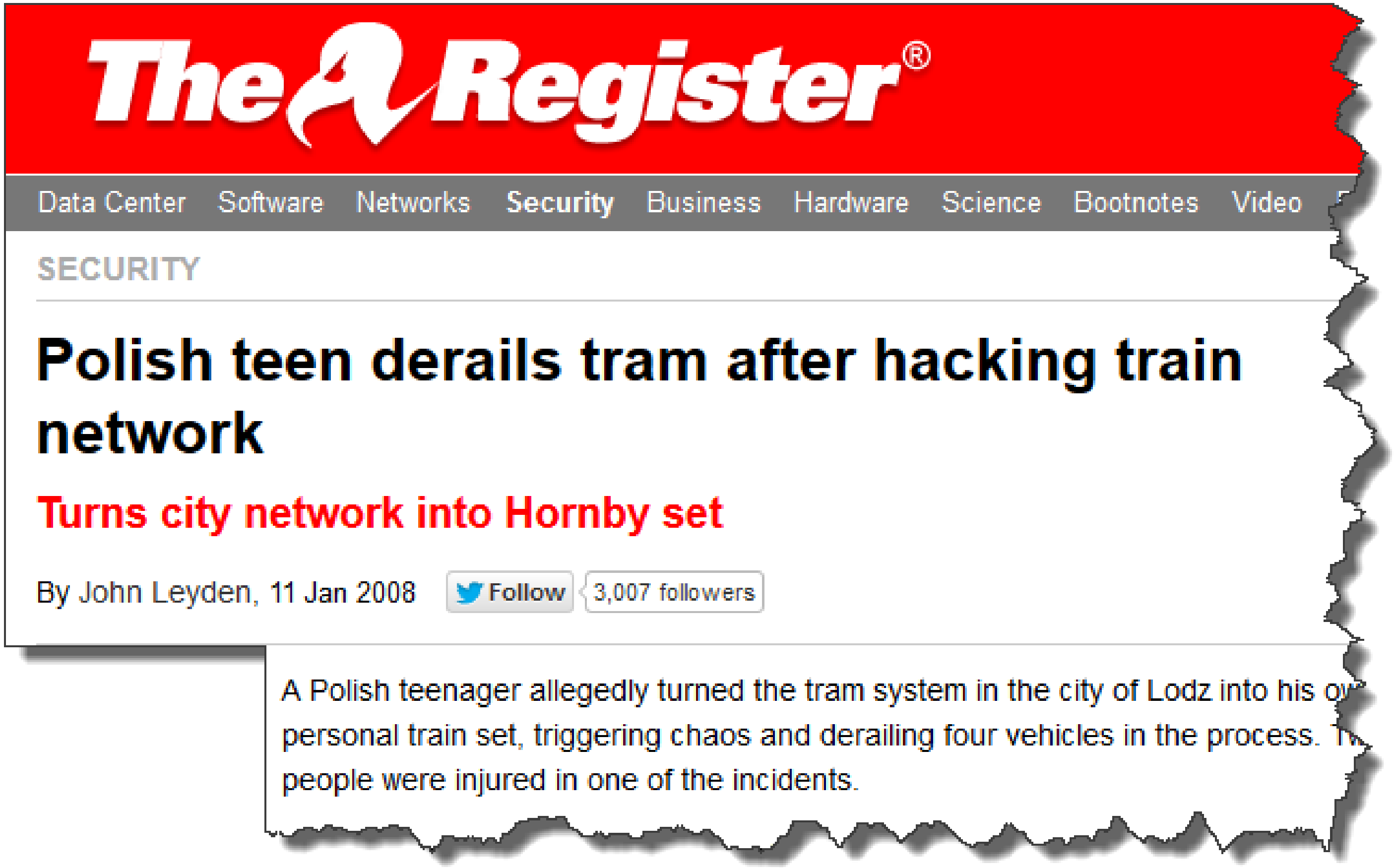


THE VERGE

Researchers wirelessly hack a Corvette's brakes using an insurance dongle

The company has patched the fix, but the hack could be used on other cars

January 2008



The Register®

Data Center Software Networks **Security** Business Hardware Science Bootnotes Video

SECURITY

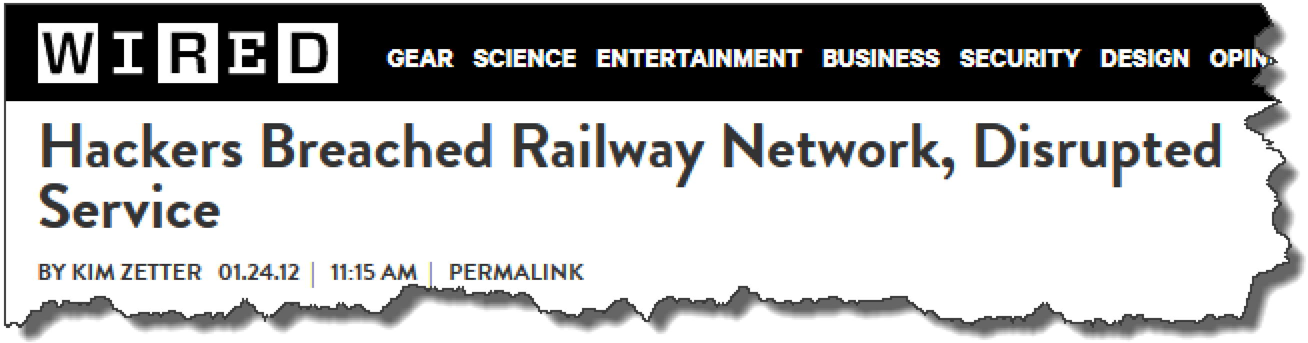
Polish teen derails tram after hacking train network

Turns city network into Hornby set

By John Leyden, 11 Jan 2008 Follow 3,007 followers

A Polish teenager allegedly turned the tram system in the city of Lodz into his ov personal train set, triggering chaos and derailing four vehicles in the process. Tw people were injured in one of the incidents.

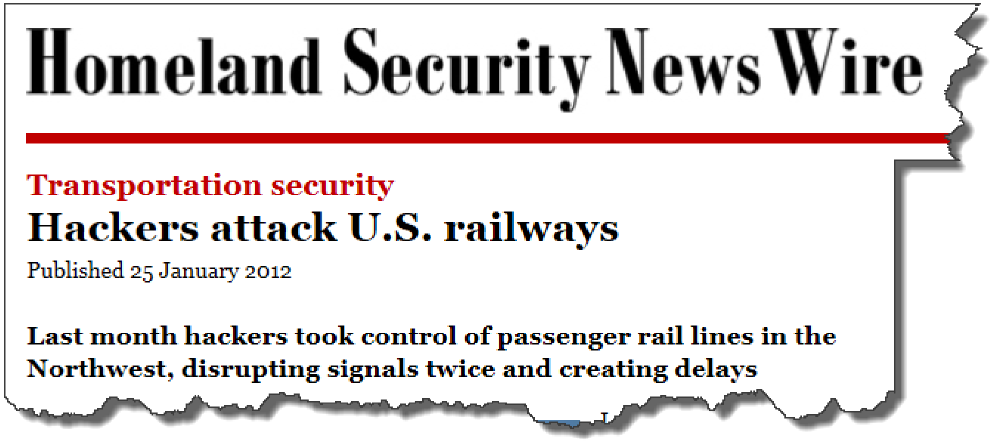
January 2012



WIRED

Hackers Breached Railway Network, Disrupted Service

BY KIM ZETTER 01.24.12 | 11:15 AM | PERMALINK



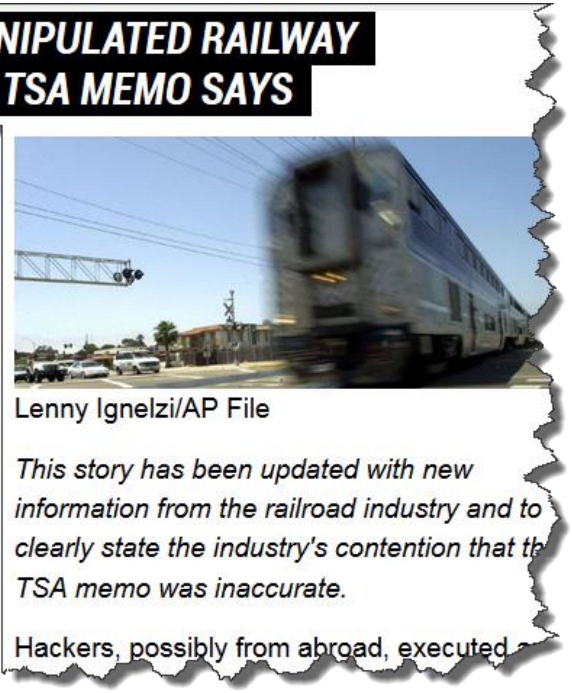
Homeland Security News Wire

Transportation security

Hackers attack U.S. railways

Published 25 January 2012

Last month hackers took control of passenger rail lines in the Northwest, disrupting signals twice and creating delays



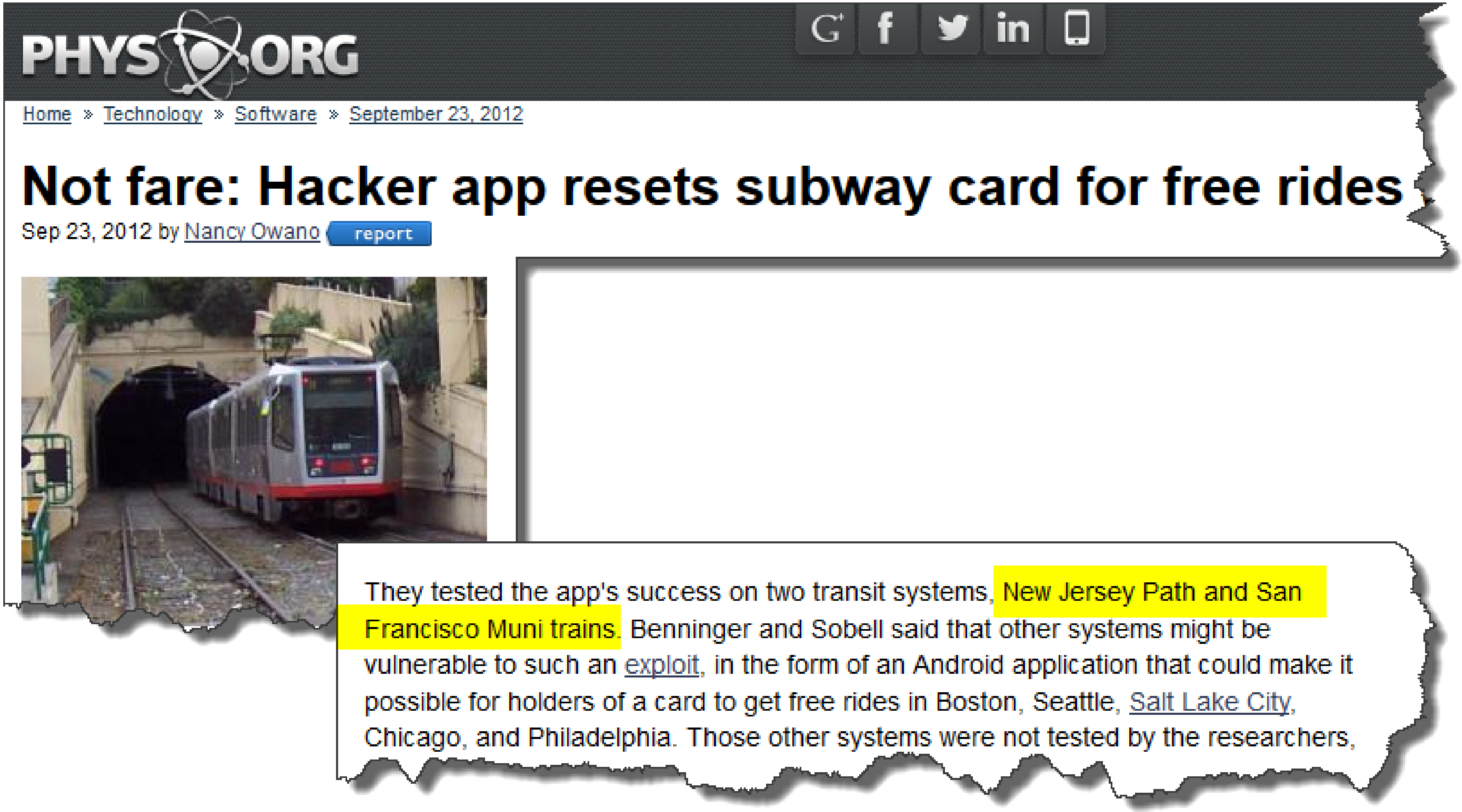
HACKERS MANIPULATED RAILWAY COMPUTERS, TSA MEMO SAYS

Lenny Ignelzi/AP File

This story has been updated with new information from the railroad industry and to clearly state the industry's contention that th TSA memo was inaccurate.

Hackers, possibly from abroad, executed a

September 2012



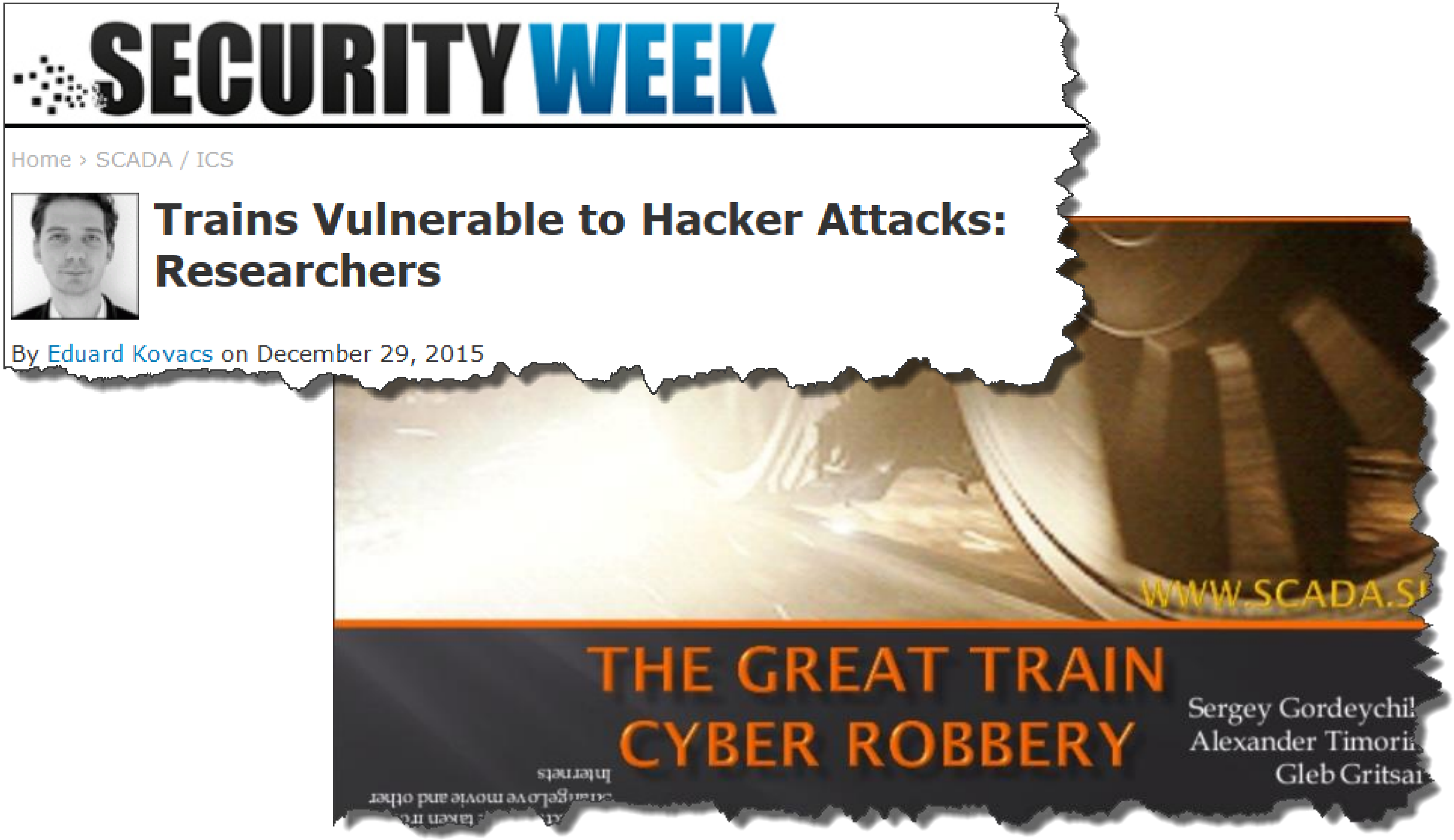
Home » Technology » Software » September 23, 2012

Not fare: Hacker app resets subway card for free rides

Sep 23, 2012 by Nancy Owano report

They tested the app's success on two transit systems, New Jersey Path and San Francisco Muni trains. Benninger and Sobell said that other systems might be vulnerable to such an exploit, in the form of an Android application that could make it possible for holders of a card to get free rides in Boston, Seattle, Salt Lake City, Chicago, and Philadelphia. Those other systems were not tested by the researchers,

December 2015



SECURITYWEEK

Home › SCADA / ICS

Trains Vulnerable to Hacker Attacks: Researchers

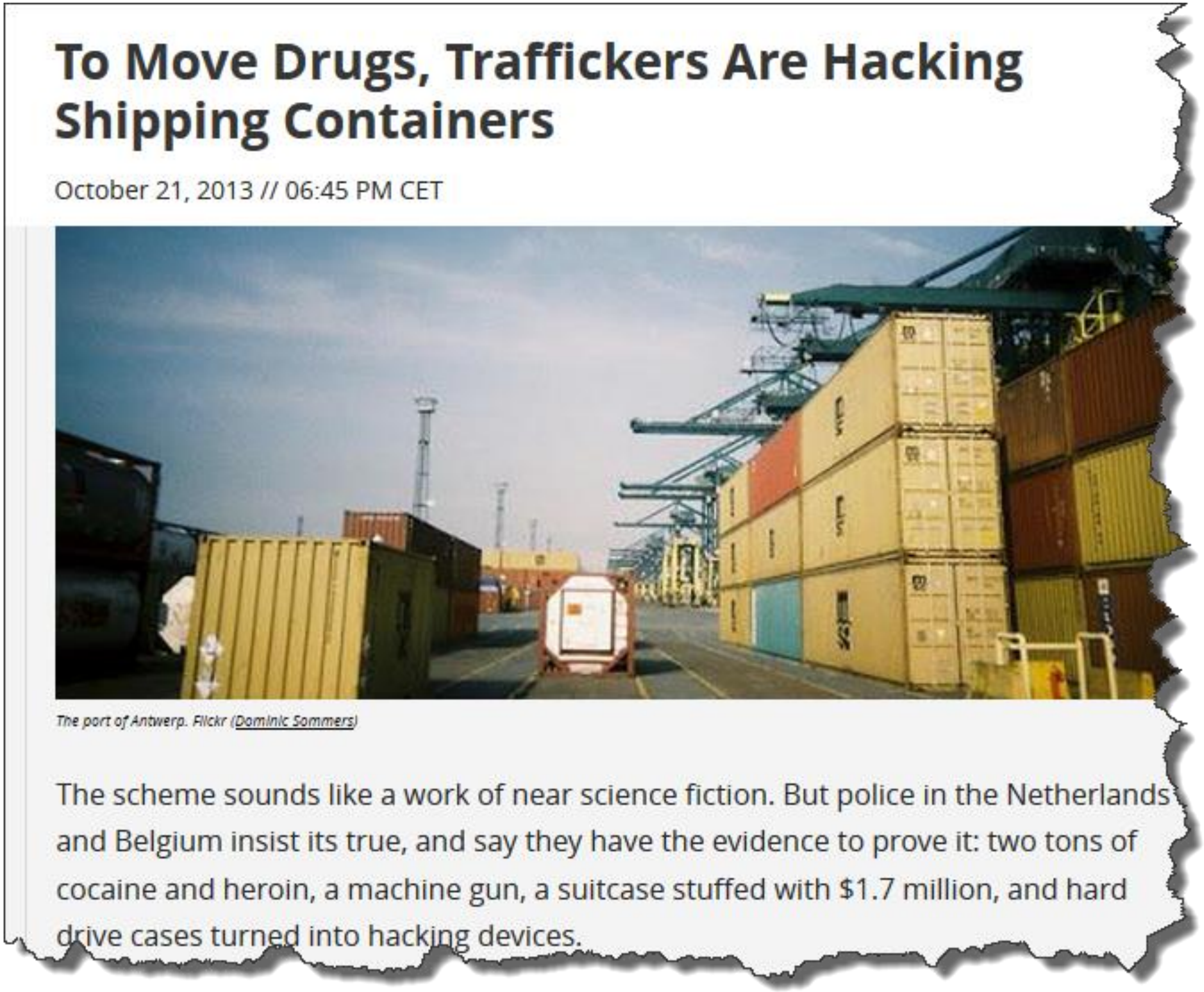
By Eduard Kovacs on December 29, 2015

WWW.SCADA.S

THE GREAT TRAIN CYBER ROBBERY

Sergey Gordeychi
Alexander Timori
Gleb Gritsa

October 2013



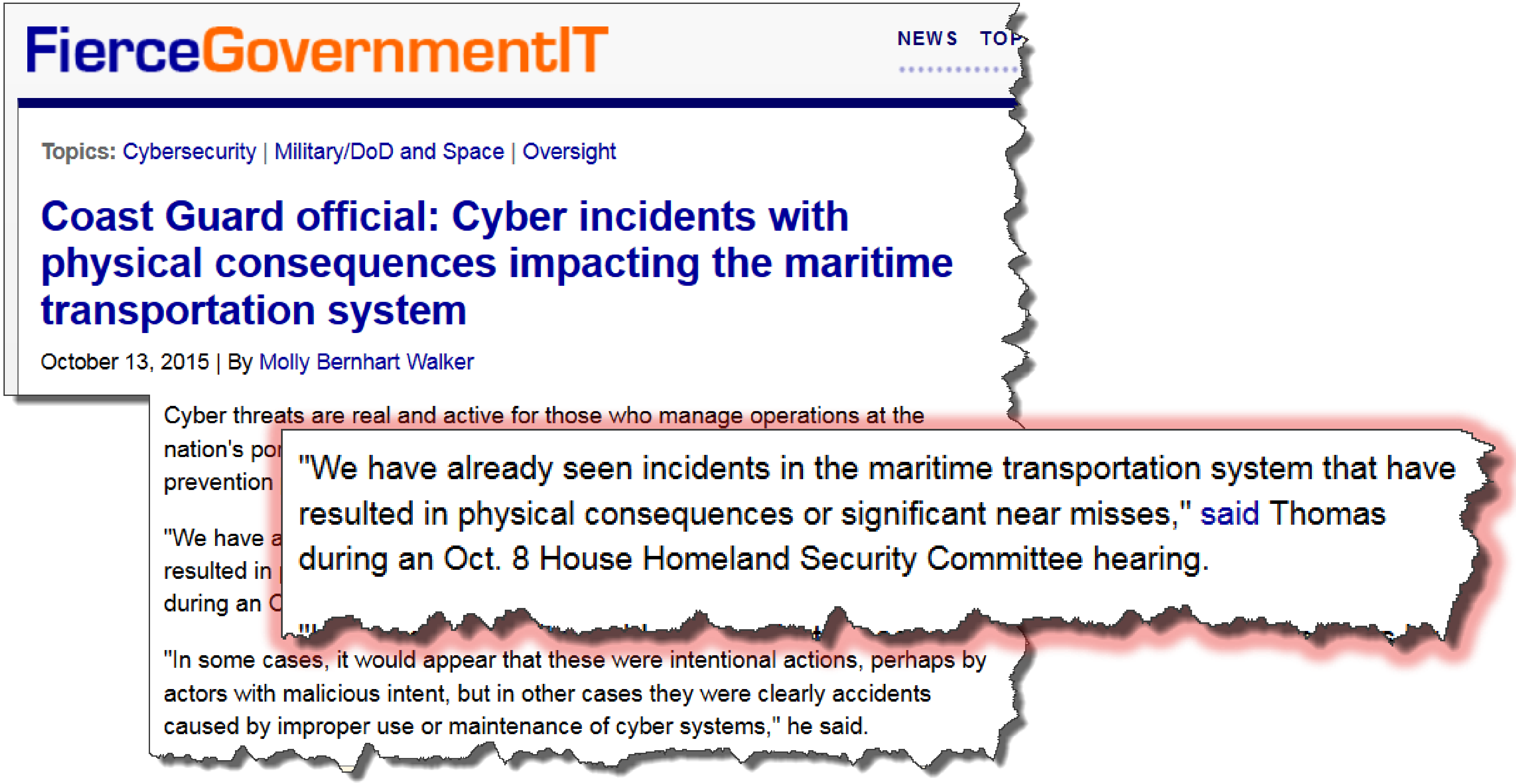
To Move Drugs, Traffickers Are Hacking Shipping Containers

October 21, 2013 // 06:45 PM CET

The port of Antwerp. Flickr (Dominic Sommers)

The scheme sounds like a work of near science fiction. But police in the Netherlands and Belgium insist its true, and say they have the evidence to prove it: two tons of cocaine and heroin, a machine gun, a suitcase stuffed with $1.7 million, and hard drive cases turned into hacking devices.

October 2015



FierceGovernmentIT

NEWS TOP

Topics: Cybersecurity | Military/DoD and Space | Oversight

Coast Guard official: Cyber incidents with physical consequences impacting the maritime transportation system

October 13, 2015 | By Molly Bernhart Walker

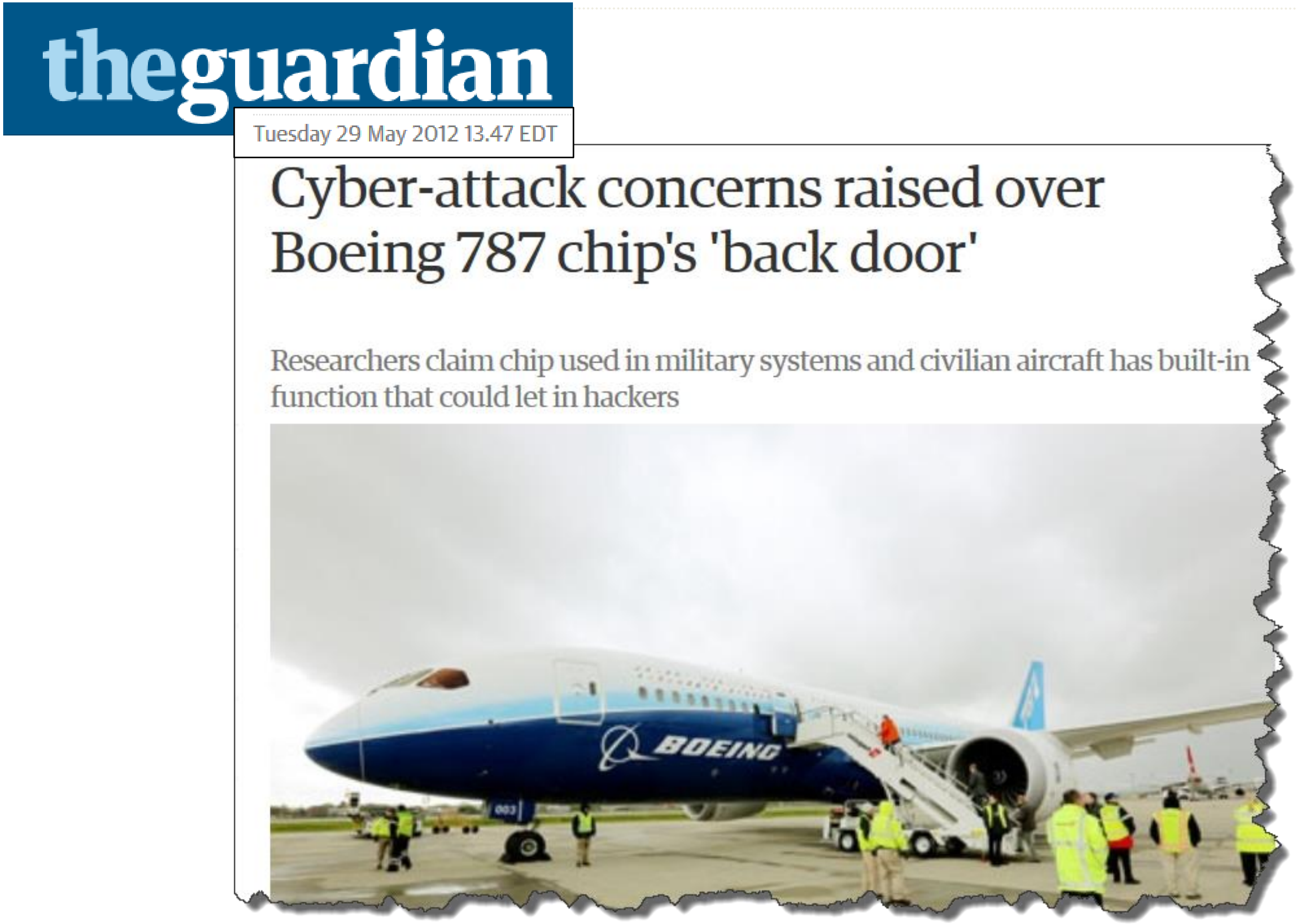
Cyber threats are real and active for those who manage operations at the
nation's por
prevention

"We have a
resulted in
during an C

"We have already seen incidents in the maritime transportation system that have resulted in physical consequences or significant near misses," said Thomas during an Oct. 8 House Homeland Security Committee hearing.

"In some cases, it would appear that these were intentional actions, perhaps by actors with malicious intent, but in other cases they were clearly accidents caused by improper use or maintenance of cyber systems," he said.

May 2012



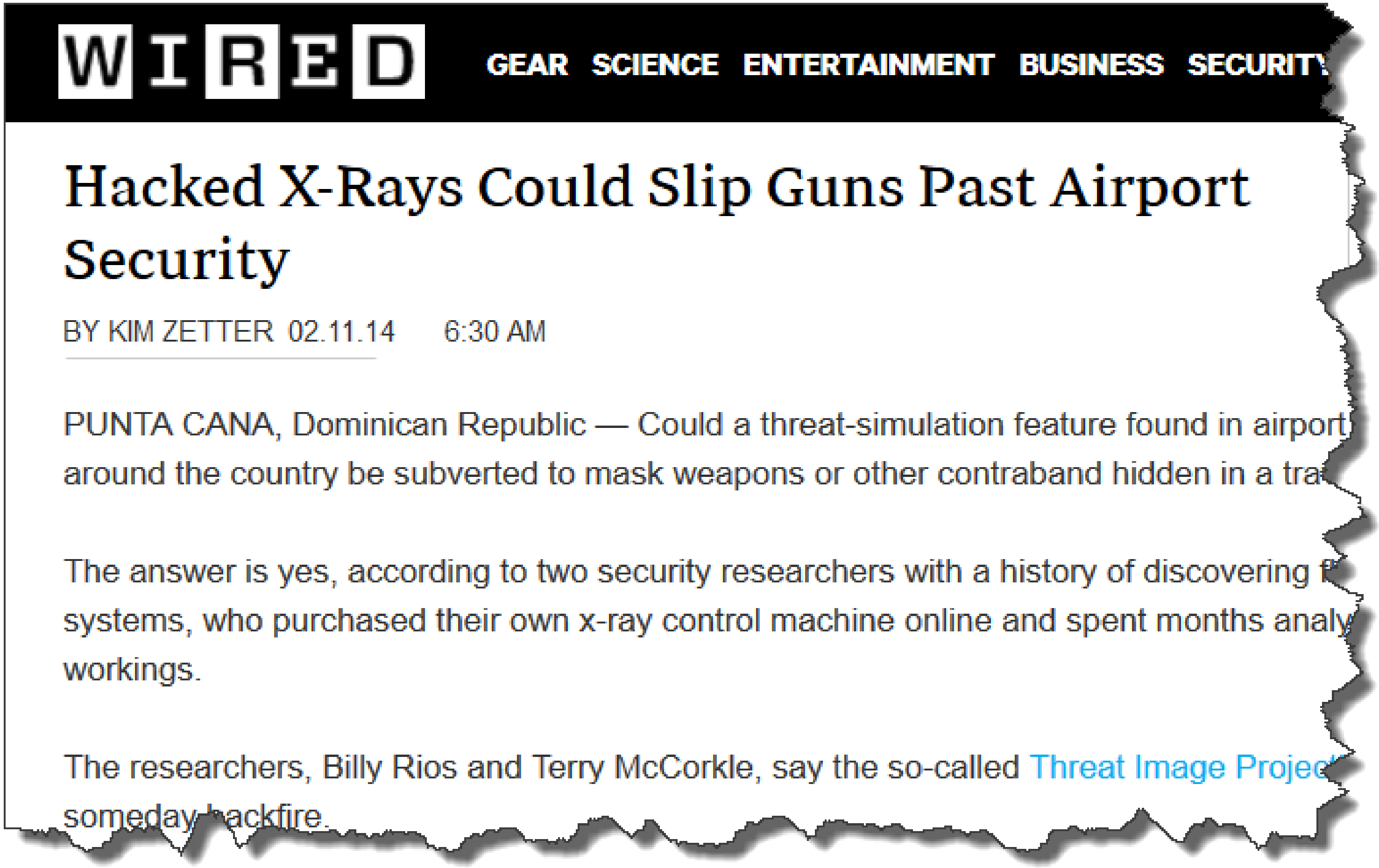
theguardian

Tuesday 29 May 2012 13.47 EDT

Cyber-attack concerns raised over Boeing 787 chip's 'back door'

Researchers claim chip used in military systems and civilian aircraft has built-in function that could let in hackers

February 2014



Hacked X-Rays Could Slip Guns Past Airport Security

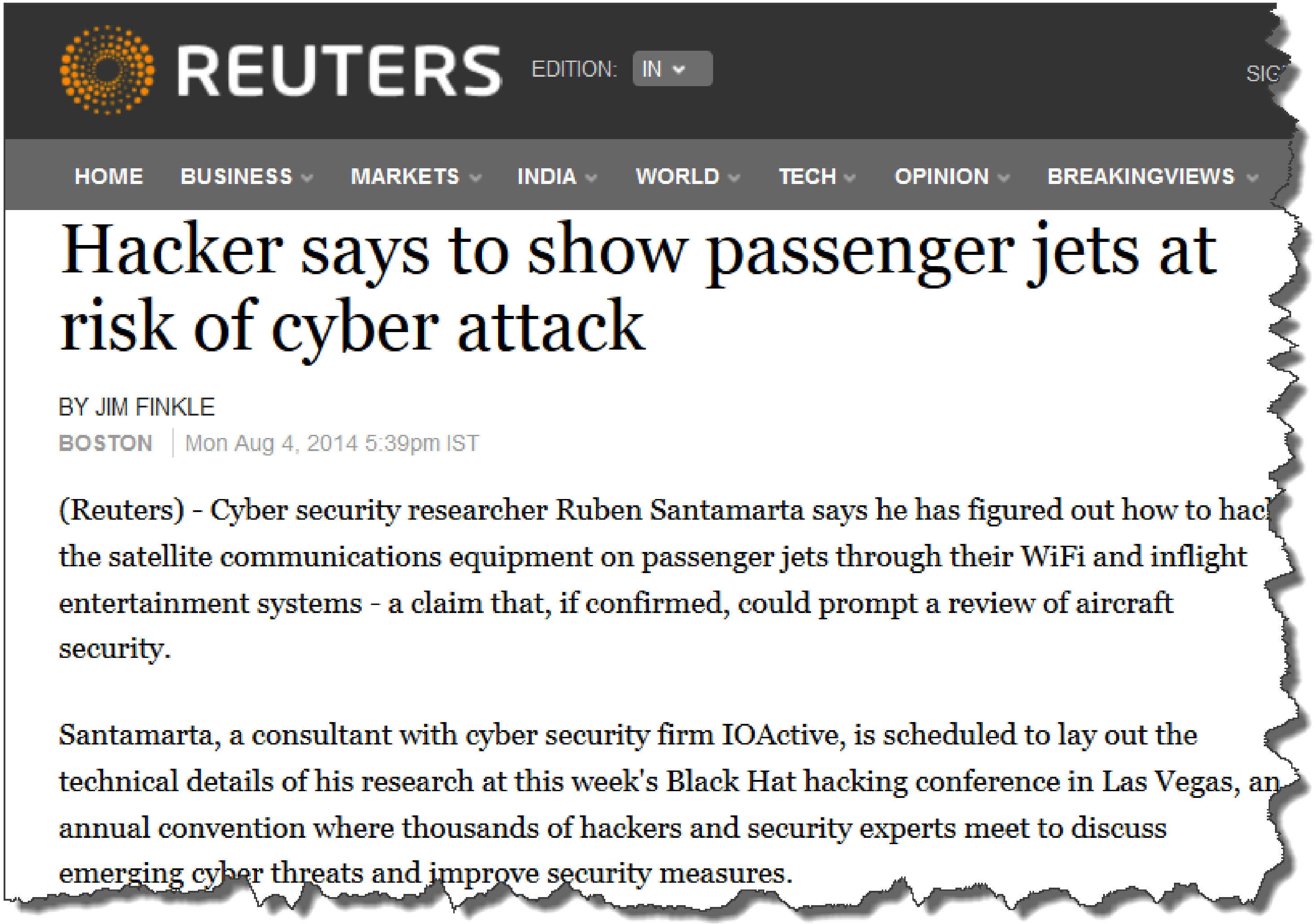
BY KIM ZETTER 02.11.14 6:30 AM

PUNTA CANA, Dominican Republic — Could a threat-simulation feature found in airport around the country be subverted to mask weapons or other contraband hidden in a tra

The answer is yes, according to two security researchers with a history of discovering f systems, who purchased their own x-ray control machine online and spent months analy workings.

The researchers, Billy Rios and Terry McCorkle, say the so-called Threat Image Project someday backfire.

August 2014



Hacker says to show passenger jets at risk of cyber attack

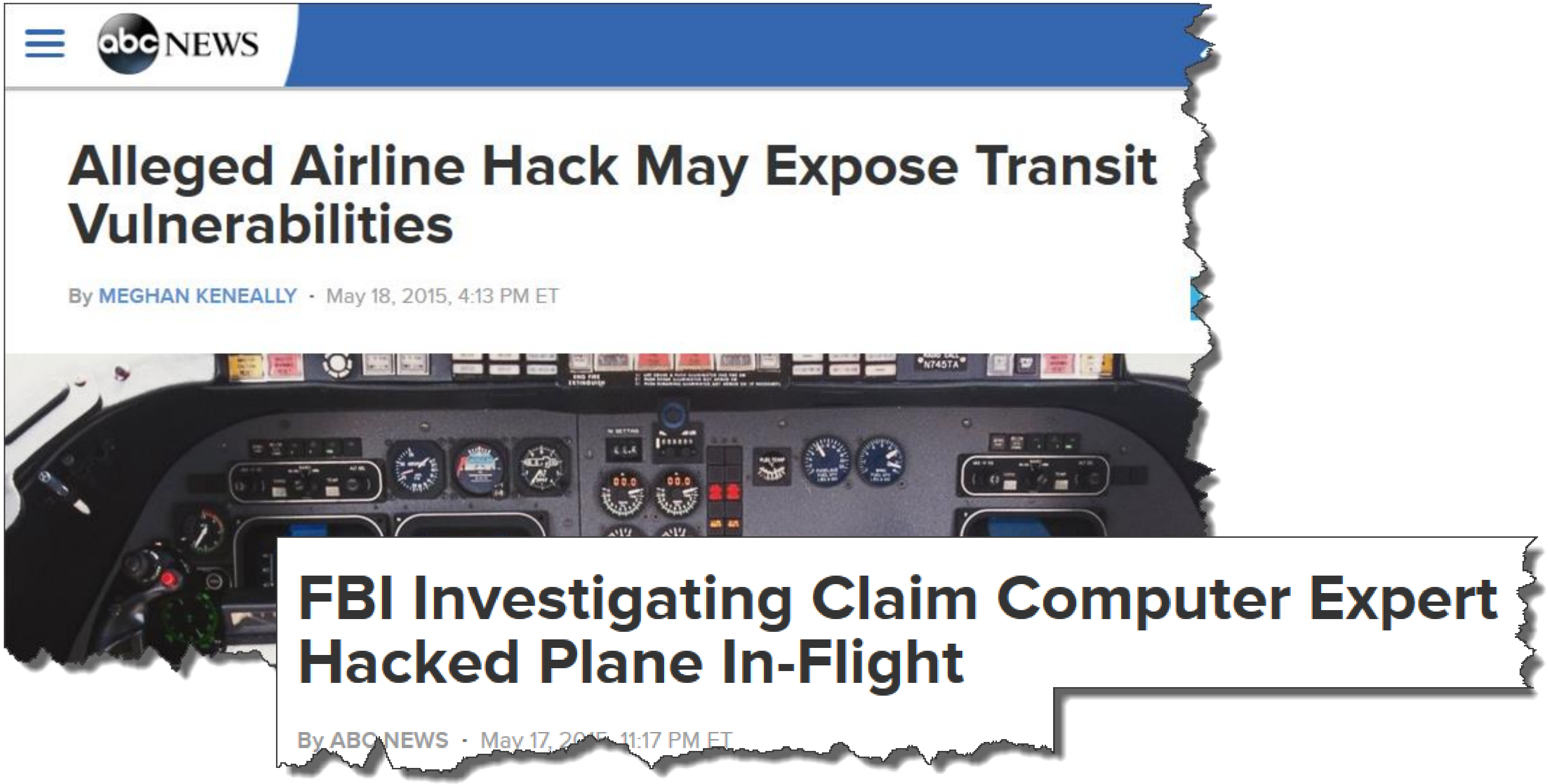
BY JIM FINKLE

BOSTON | Mon Aug 4, 2014 5:39pm IST

(Reuters) - Cyber security researcher Ruben Santamarta says he has figured out how to hac the satellite communications equipment on passenger jets through their WiFi and inflight entertainment systems - a claim that, if confirmed, could prompt a review of aircraft security.

Santamarta, a consultant with cyber security firm IOActive, is scheduled to lay out the technical details of his research at this week's Black Hat hacking conference in Las Vegas, an annual convention where thousands of hackers and security experts meet to discuss emerging cyber threats and improve security measures.

May 2015



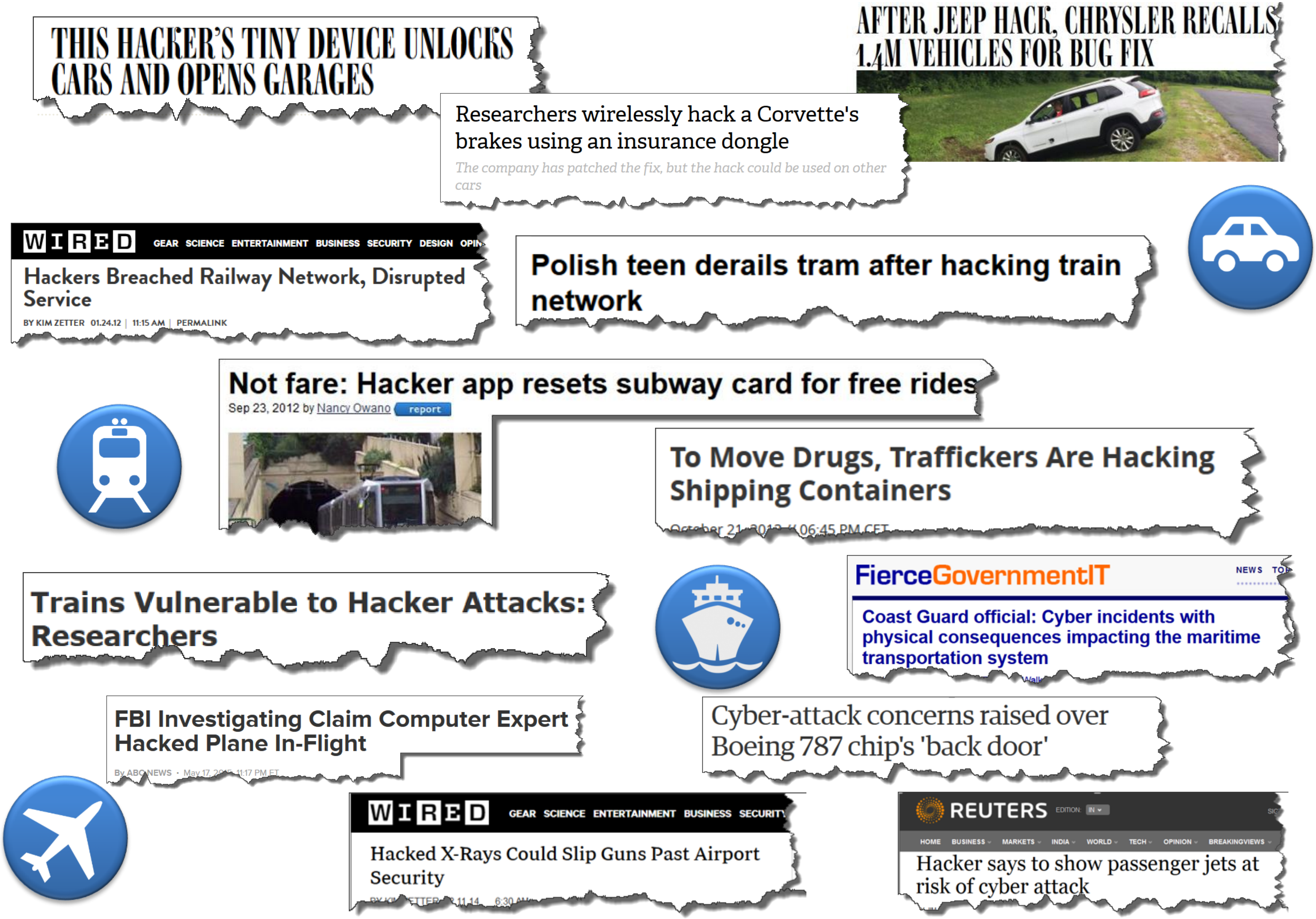
abc NEWS

Alleged Airline Hack May Expose Transit Vulnerabilities

By MEGHAN KENEALLY · May 18, 2015, 4:13 PM ET

FBI Investigating Claim Computer Expert Hacked Plane In-Flight

By ABC NEWS · May 17, 2015, 11:17 PM ET



THIS HACKER'S TINY DEVICE UNLOCKS CARS AND OPENS GARAGES

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

Researchers wirelessly hack a Corvette's brakes using an insurance dongle

The company has patched the fix, but the hack could be used on other cars

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPIN

Hackers Breached Railway Network, Disrupted Service

BY KIM ZETTER 01.24.12 | 11:15 AM | PERMALINK

Polish teen derails tram after hacking train network

Not fare: Hacker app resets subway card for free rides

Sep 23, 2012 by Nancy Owano report

To Move Drugs, Traffickers Are Hacking Shipping Containers

October 21, 2013 | 06:45 PM CET

Trains Vulnerable to Hacker Attacks: Researchers

FierceGovernmentIT NEWS TOP

Coast Guard official: Cyber incidents with physical consequences impacting the maritime transportation system

FBI Investigating Claim Computer Expert Hacked Plane In-Flight

By ABC NEWS · May 17, 2015 1:17 PM ET

Cyber-attack concerns raised over Boeing 787 chip's 'back door'

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY

Hacked X-Rays Could Slip Guns Past Airport Security

BY KIM ZETTER 12.11.14 6:30 AM

REUTERS EDITION: IN

HOME BUSINESS MARKETS INDIA WORLD TECH OPINION BREAKINGVIEWS

Hacker says to show passenger jets at risk of cyber attack

Discussion is Applicable to All Subsectors

Freight Rail

Maritime

Passenger Rail

Postal & Shipping

Aviation

Highway Infrastructure

Motor Carrier

Pipeline

Mas Transit

Discussion is Applicable to…

Transportation Subsectors	Primary Units of Transportation	Modes of Transportation
Aviation	People & Goods	Air
Highway Infrastructure & Motor Carrier	People & Goods	Ground
Maritime Transportation Systems	People & Goods	Sea
Mass Transit & Passenger Rail	People	Ground
Pipeline Systems	Oil & Gas	Ground
Freight Rail	Goods	Ground
Postal & Shipping	Mailpieces & Goods	Air, Ground, Sea

Prevention is Futile

Cyber Intrusions are a Fact of Life

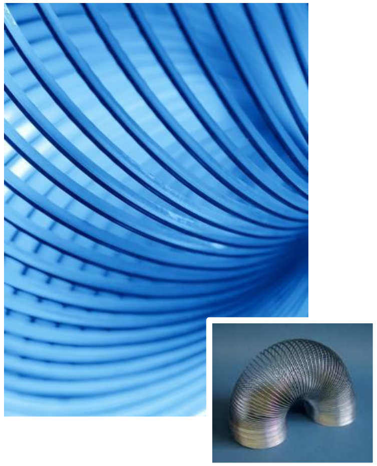
]HackingTeam[
UCLA Health System
SONY PICTURES
ASHLEY MADISON®
Life is short. Have an affair.®
UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
UBER
PlayStation.Network
TARGET
THE HOME DEPOT
UNITED STATES POSTAL SERVICE
JPMORGAN CHASE & CO.
DEPARTMENT OF STATE UNITED STATES OF AMERICA
Forbes
EVERNOTE
UNITED STATES CENTRAL COMMAND
Anthem.
ebay
Toys R us

Traditional Information Security Function

Protect / Shield / Defend / Prevent

- Is necessary
- Is not Sufficient
- Fails too frequently

Operational and Cyber Resilience



An Operationally Resilient Entity?

A tree under operational stress…

…while achieving its “business” mission

Operational Resilience

The ***emergent*** property of an entity

- that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

The ability of an entity to

- Prevent disruptions from occurring;
- And when struck by a disruption, the ability to quickly respond to and recover from a disruption in the primary business processes.

Sample Techniques

for

Improving and Managing

Cyber Resilience

Organizational Aspects

How should **organizational structures, roles, and responsibilities** be adapted?

Example:

- “Traditional” vs. “Modern” information security functions

Modern Information Security Functions

Protect / Shield / Defend / Prevent

Monitor / Detect / Hunt

Respond/ Recover / Sustain

**Management,
Governance,
Compliance,
Education,
Risk Management.**

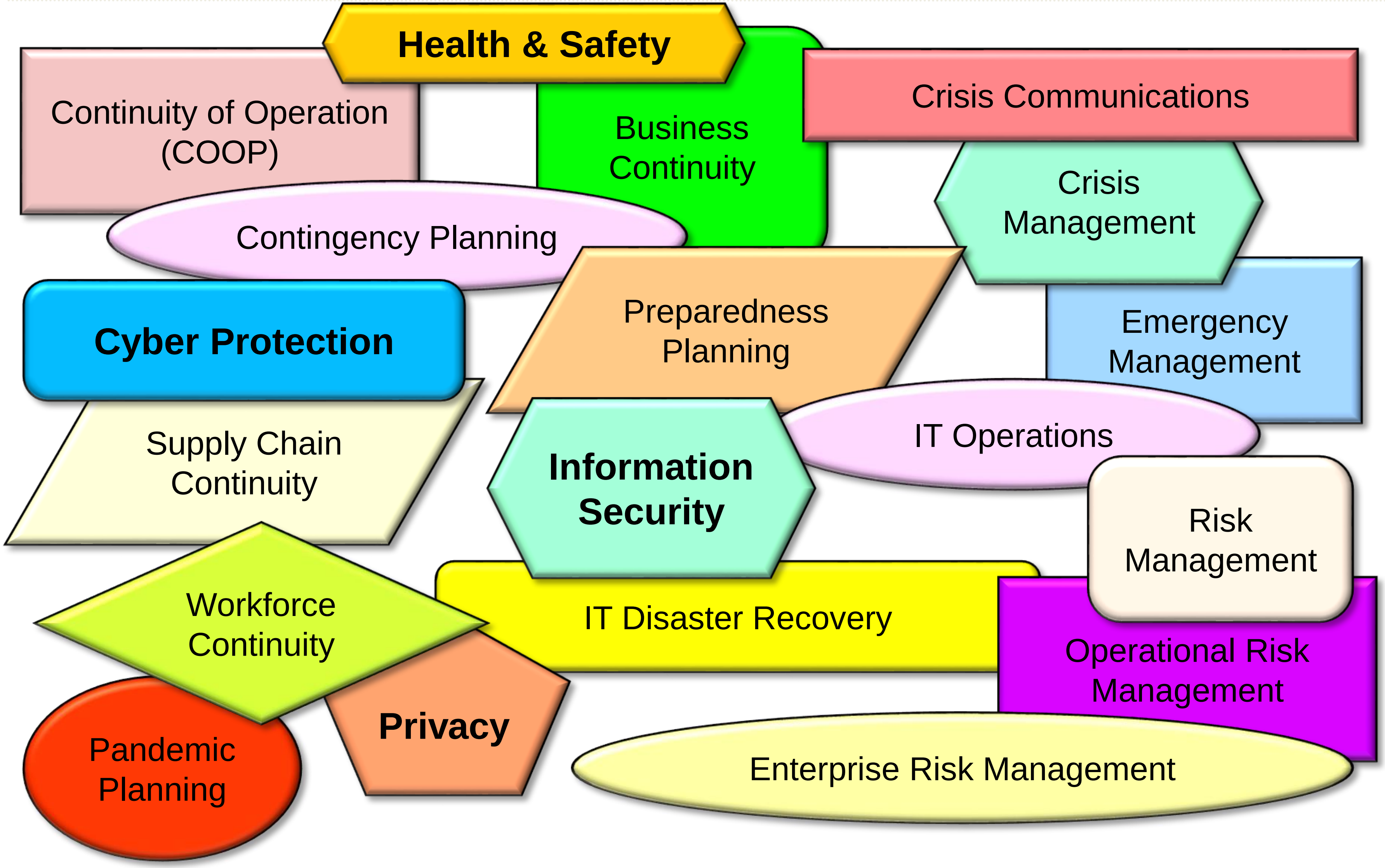
Operational Risk Aspects

How should organizations adapt their overall **operational risk management principles and practices**?

Example:

- Integration and convergence of operational risk management activities.

Today’s Operational Risk Management



Health & Safety

Continuity of Operation (COOP)

Business Continuity

Crisis Communications

Crisis Management

Contingency Planning

Cyber Protection

Preparedness Planning

Emergency Management

Supply Chain Continuity

Information Security

IT Operations

Risk Management

Workforce Continuity

IT Disaster Recovery

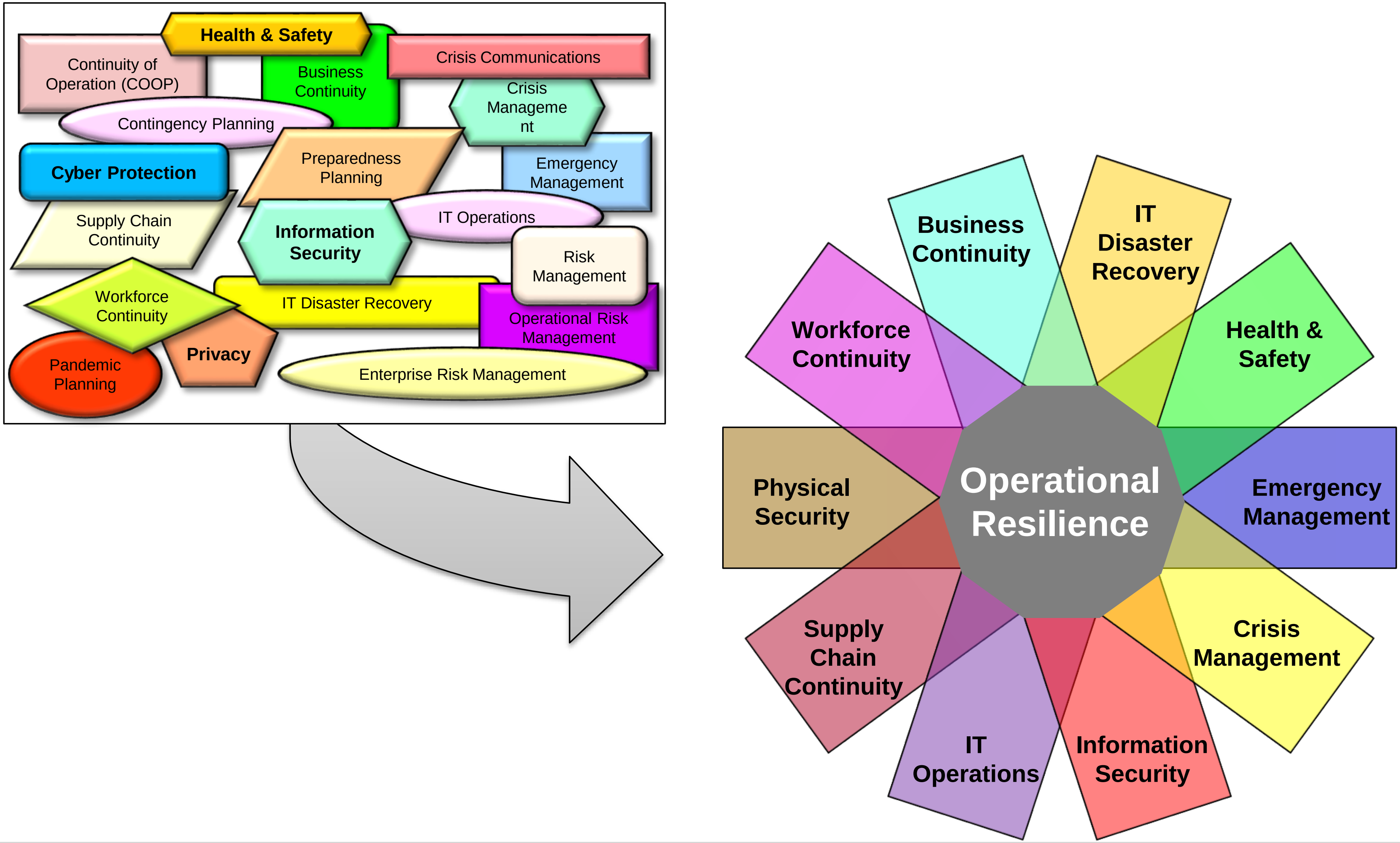
Operational Risk Management

Pandemic Planning

Privacy

Enterprise Risk Management

Desired Solution Approach



Tools and Techniques Aspects

What structured (i.e., not ad hoc) **frameworks** could guide and assist organizations?

Example:

- Resilience Management Model

What is Resilience Management Model?

Framework for managing and improving operational resilience

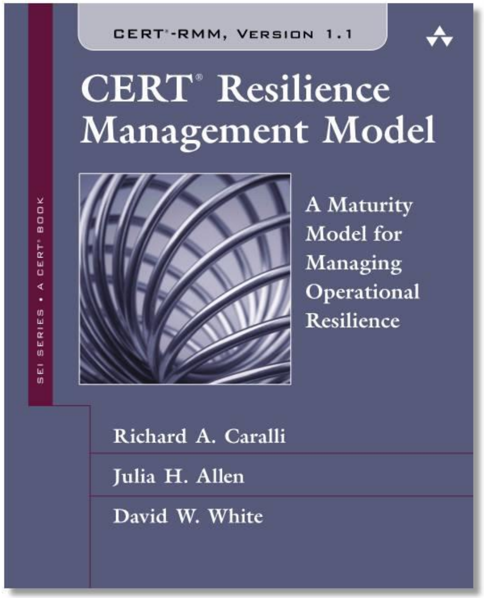
Guides implementation, mgmt, and sustainment of operational risk management activities

Improves confidence in how an organization manages and responds to operational stress

Focuses on “What” not “How”

Applicable to a variety of organizations

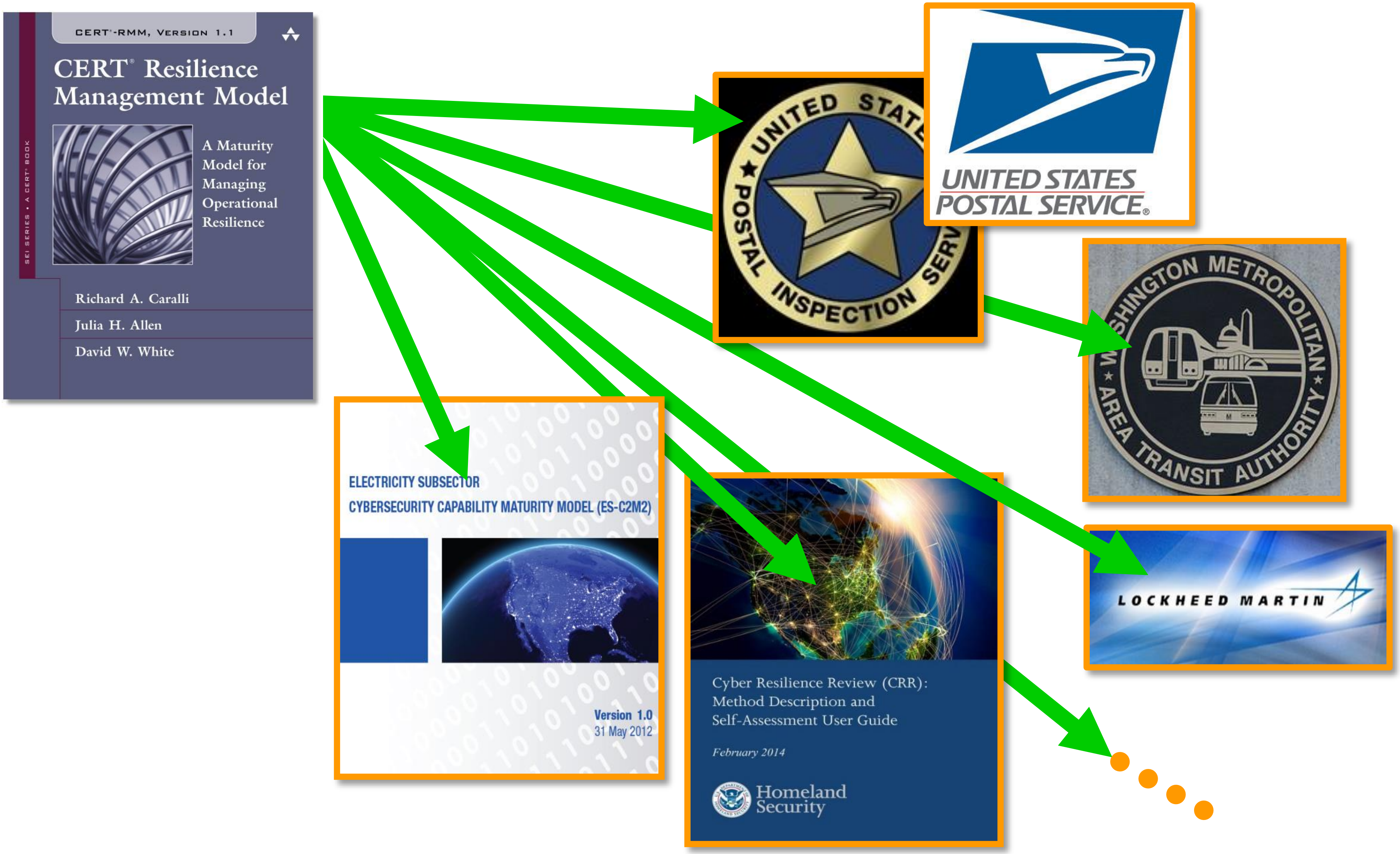
- small or large
- simple or complex
- public or private


CERT®-RMM, Version 1.1
CERT® Resilience Management Model
A Maturity Model for Managing Operational Resilience
SEI Series • A CERT® Book
Richard A. Caralli
Julia H. Allen
David W. White

“…an extensive super-set of the things an organization could do to be more resilient.”

- CERT-RMM adopter

A Sampling of RMM Success Stories



CERT®-RMM, Version 1.1

CERT® Resilience Management Model

A Maturity Model for Managing Operational Resilience

Richard A. Caralli

Julia H. Allen

David W. White

SEI Series • A CERT® Book

ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Version 1.0

31 May 2012

Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide

February 2014

Homeland Security

UNITED STATES POSTAL INSPECTION SERV
UNITED STATES POSTAL SERVICE®
WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY
LOCKHEED MARTIN

In Closing

Sampling of ITS Emerging Capabilities

Convenience, Comfort, & Entertainment

- Keyless entry
- Remote engine start
- Mobile device integration
- Infotainment

Smart Transportation

- Vehicle-to-infrastructure communications
- Smart intersection
- Traffic light control
- Collision avoidance
- Traffic management.

Advanced Driver Assistant Systems (ADAS)

- Smart lighting control
- Adaptive cruise control
- Lane departure warning
- Parking assist

Autonomous Driving

Diagnostics & Maintainability

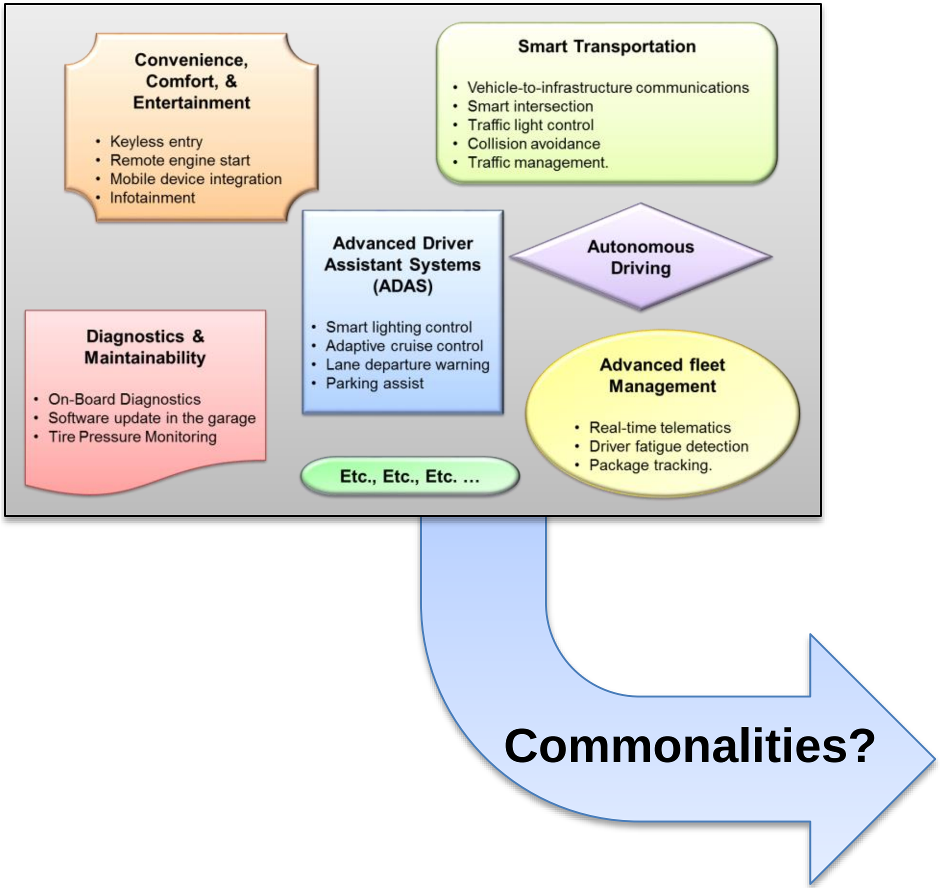
- On-Board Diagnostics
- Software update in the garage
- Tire Pressure Monitoring

Advanced fleet Management

- Real-time telematics
- Driver fatigue detection
- Package tracking.

Etc., Etc., Etc. …

Commonalities in Emerging Capabilities



Convenience, Comfort, & Entertainment

- Keyless entry
- Remote engine start
- Mobile device integration
- Infotainment

Smart Transportation

- Vehicle-to-infrastructure communications
- Smart intersection
- Traffic light control
- Collision avoidance
- Traffic management.

Advanced Driver Assistant Systems (ADAS)

- Smart lighting control
- Adaptive cruise control
- Lane departure warning
- Parking assist

Autonomous Driving

Diagnostics & Maintainability

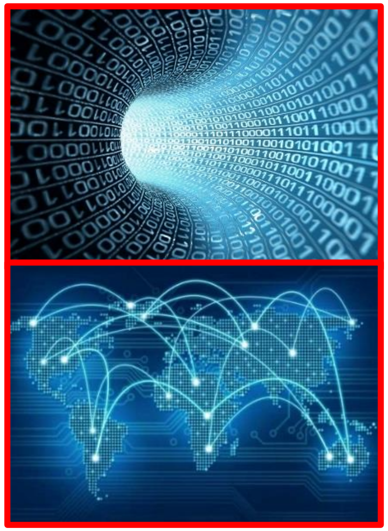
- On-Board Diagnostics
- Software update in the garage
- Tire Pressure Monitoring

Advanced fleet Management

- Real-time telematics
- Driver fatigue detection
- Package tracking.

Etc., Etc., Etc. …

Commonalities?

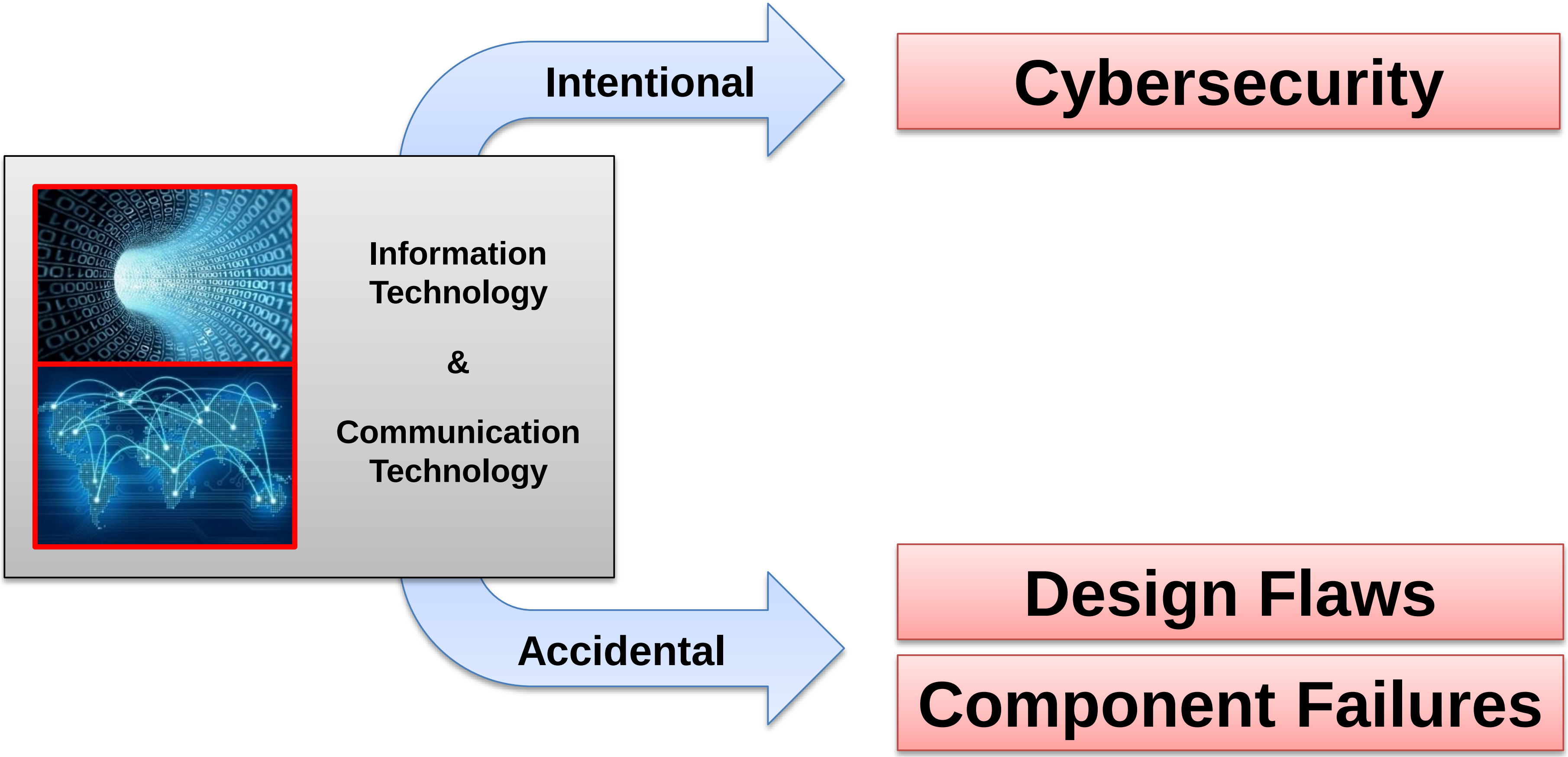


Information Technology

&

Communication Technology

Primary Risks to Common Elements



Information Technology

&

Communication Technology

Intentional

Cybersecurity

Accidental

Design Flaws

Component Failures

Cyber Risk Mitigation Challenge

Traditional IT cybersecurity contingencies are not feasible

- Failover over to a disaster recovery site
- Restoring from backup
- Failover to another vehicle
- Federal Motor Vehicle Safety Standards (FMVSS) timeframes precludes “Patch Tuesdays.”
- Can’t call a breach response team (AAA does not do that yet)

Successful management of cyber risk within ITS may require a (significant) shift in thinking and approach.

Promising and Proven Approach

Thank you for your attention.

References

1. J. H. Allen, R. H. Caralli, and D. W. White, CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience, Addison-Wesley Professional, 2010.

2. N. Mehravari, J. Allen, P. Curtis, and G. Crabb, “A Proven Method for Identifying Security Gaps in International Postal and Transportation Critical Infrastructure,” *93rd Annual Transportation Research Board Conference*, Washington, DC, January 13-18, 2014.

3. N. Mehravari, J. Allen, P. Curtis, and G. Crabb, “Improving the Security and Resilience of U.S. Postal Service Mail Products and Services,” *93rd Annual Transportation Research Board Conference*, Washington, DC, January 13-18, 2014.

4. N. Mehravari, "Cybersecurity Update,” a lecture as part of the Business Continuity and Crisis Management Summer School, Massachusetts Institute of Technology, July 2015.

5. N. Mehravari, “Cyber and Operational Resilience Management,” half-day tutorial, planned for *2015 IEEE Military Communications Conference (MILCOM’15),* Tampa, FL, October 26-28, 2015.

6. N, Mehravari, “Principles and Practice of Operational Resilience,” half-day tutorial, *IEEE Systems Conference*, Vancouver, BC, April 12-16, 2015.

7. N. Mehravari, “Information Resilience in Today's High-Risk Economy,” *Software Engineering Institute Blog*, November 17, 2014.