University of BRISTOL

CyBOK

Cyber-Physical Systems Security

bristol.ac.uk

University of BRISTOL

CyBOK

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.

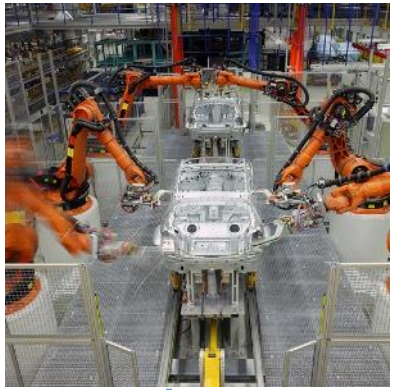
bristol.ac.uk

Modernization of our Physical Infrastructures

CyBOK

Industrial Control Systems

Manufacturing Automation



Building Automation

Smart Grid

Operations Center

Intelligent Transportation Systems

WirelessHART, ISA 100.11a, 6LoWPAN, ROLL, 802.15.4, …

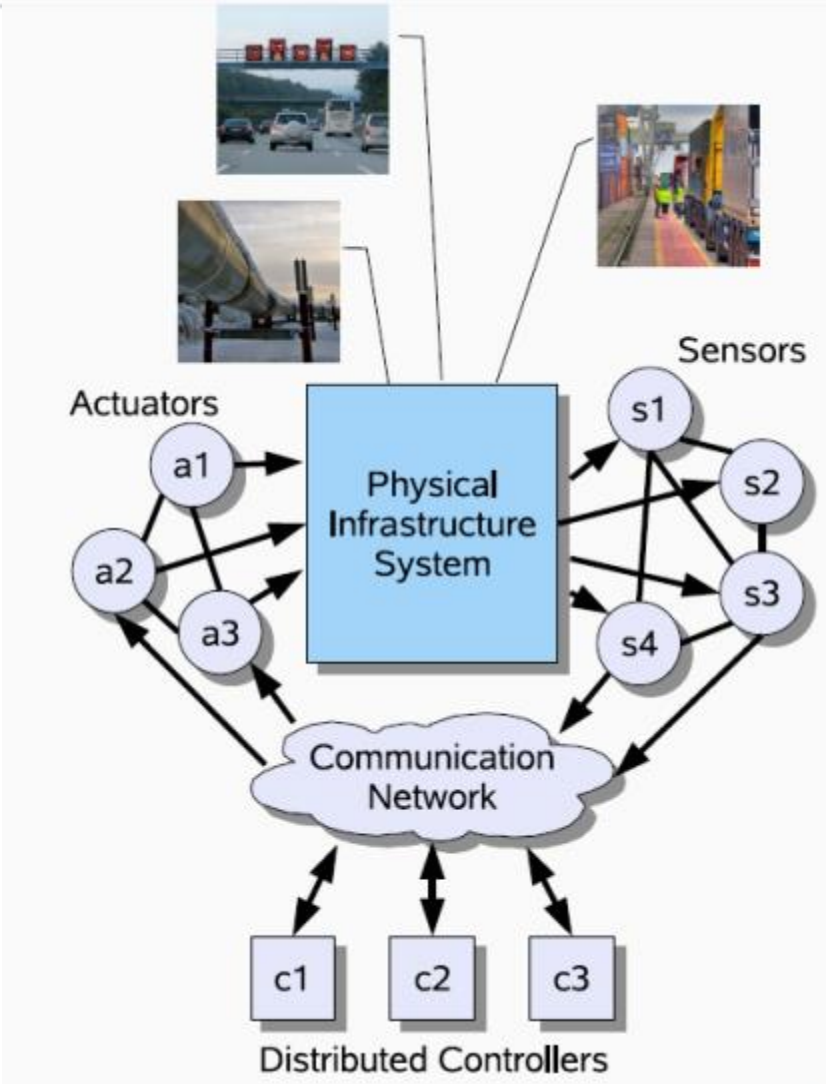
Smart Homes, Autonomous Vehicles, Agriculture

Image Source:
conosco.com

Cyber-Physical Systems

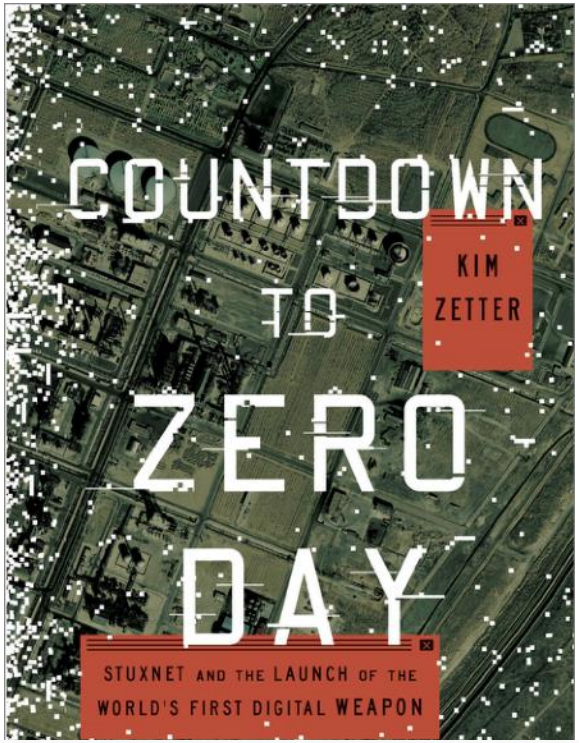
- Control
- Computation
- Communication

- Interdisciplinary Research!



Security Problems

CyBOK



Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure

December 14, 2017 | by Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer

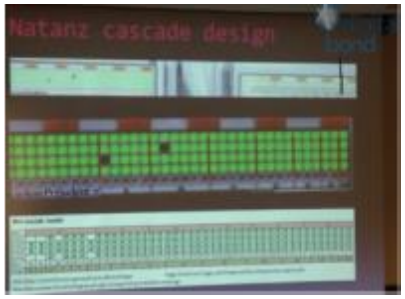
Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout

Malware which speaks the language of industrial machines is a danger to all of our critical services.

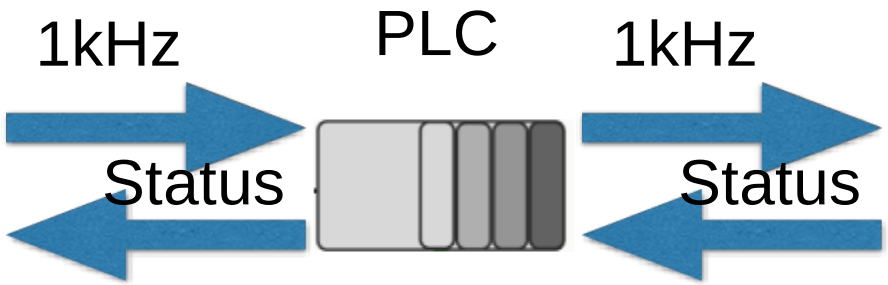
By Charlie Osborne for Zero Day | April 30, 2018 -- 11:08 GMT (04:08 PDT) | Topic: Security

Control Systems

HMI

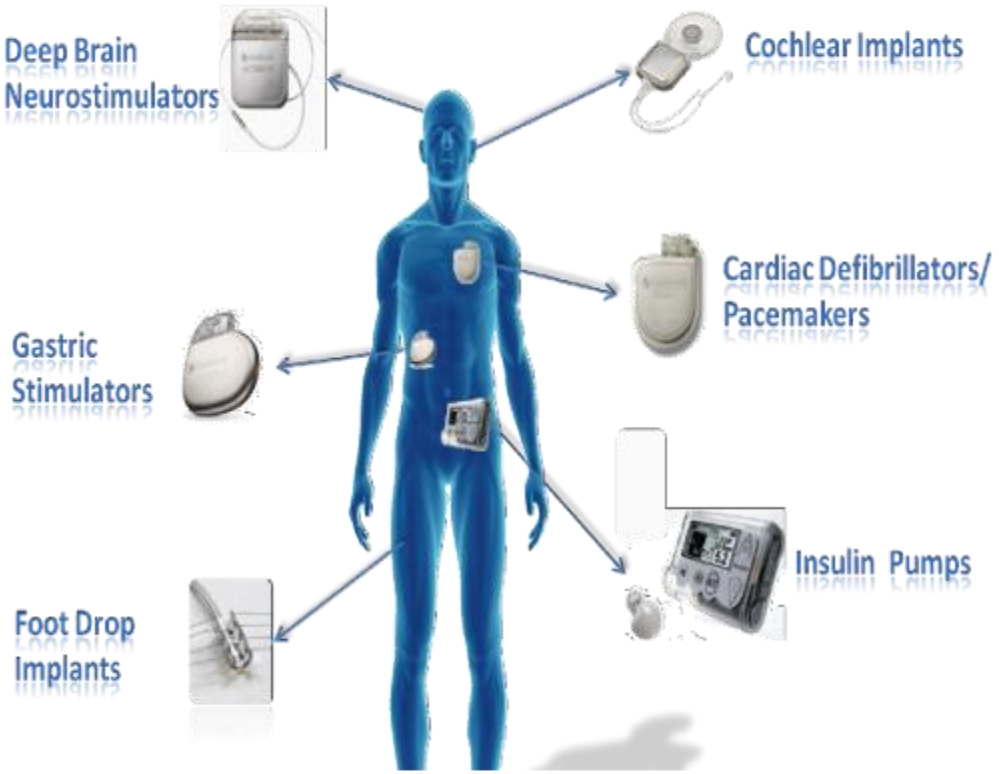


Control Room



Centrifuges

Medical Devices



Air Traffic Communications (ADS-B)

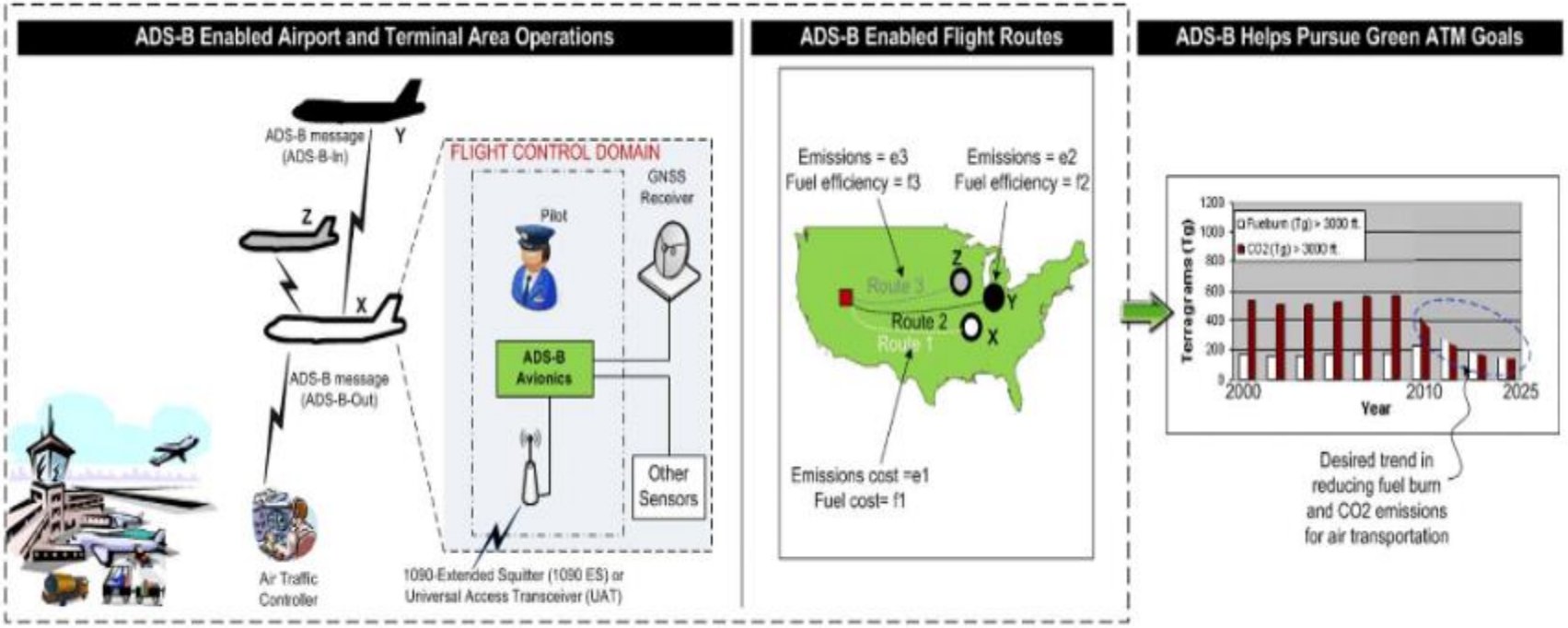
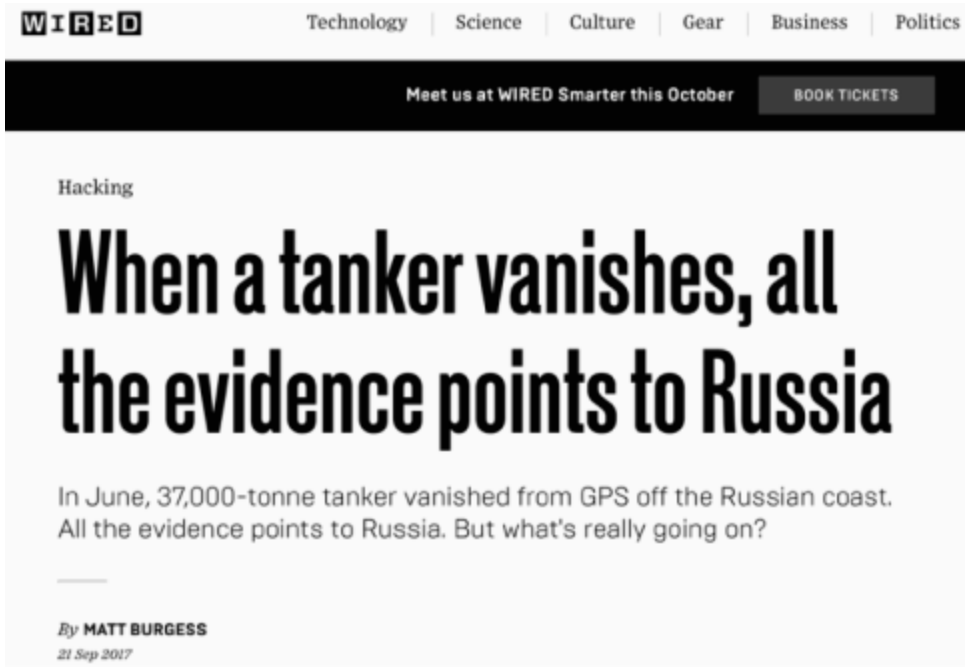


Fig. 4. *Illustration of ADS-B modes and benefits for future ATM systems.*

- Source: Sampigethaya et al.

Autonomous Vehicles

CyBOK



WIRED Technology | Science | Culture | Gear | Business | Politics

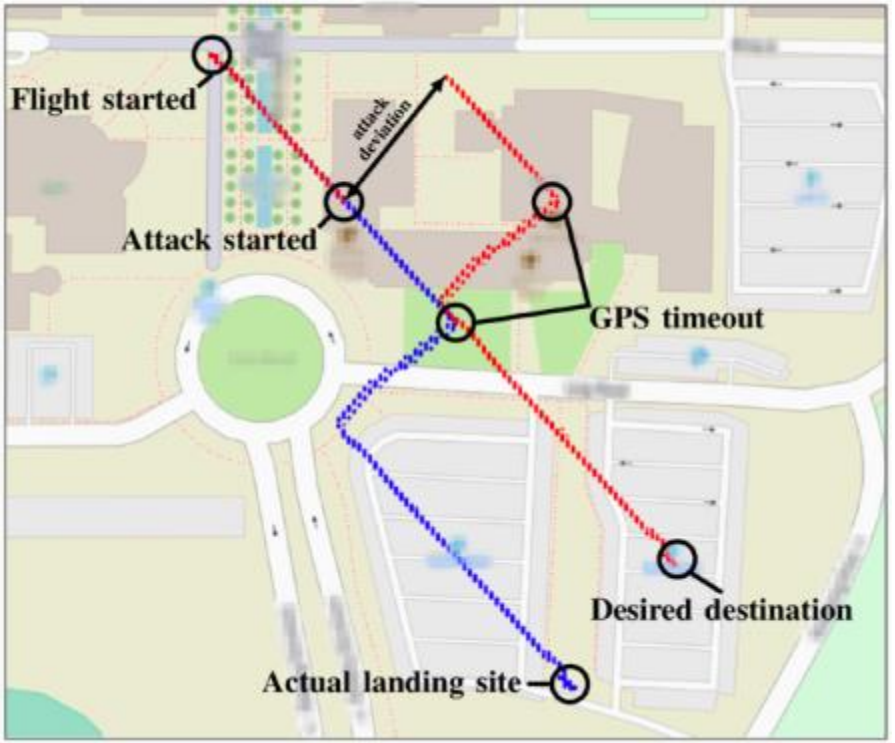
Meet us at WIRED Smarter this October BOOK TICKETS

Hacking

When a tanker vanishes, all the evidence points to Russia

In June, 37,000-tonne tanker vanished from GPS off the Russian coast. All the evidence points to Russia. But what's really going on?

By **MATT BURGESS**
21 Sep 2017



A decade ago it was hard to convince researchers this was a problem

CyBOK

Only one verified attack to control systems: 2000 attack on waste water control system

The Register®
Biting the hand that feeds IT

DATA CENTER SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Software

Hacker jailed for revenge sewage attacks

Job rejection caused a bit of a stink

31 Oct 2001 at 15:55, Tony Smith

An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

Event: More than 750,000 gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds

Impact: Loss of marine life, public health jeopardized, $200,000 in cleanup and monitoring costs

Specifics: SCADA system had 300 nodes (142 pumping stations) governing sewage and drinking water

- Used OPC ActiveX controls, DNP3, and ModBus protocols
- Used packet radio communications to RTUs
- Used commercially available radios and stolen SCADA software to make laptop appear as a pumping station
- Caused as many as 46 different incidents over a 3-month period (Feb 9 to April 23)

Why is CPS Security Different?

CyBOK

Security of Control Systems?

Nothing new!
Use normal IT security tools!

Not my job!
It's the IT security guy's job!

Security

Control

If attacker has partial control of system, it can drive it to unsafe states.

Not my job!
It's the control engineers job!

Nothing new!
Safety and fault tolerance will save the day!

Attacks != Failures

Security in CPS

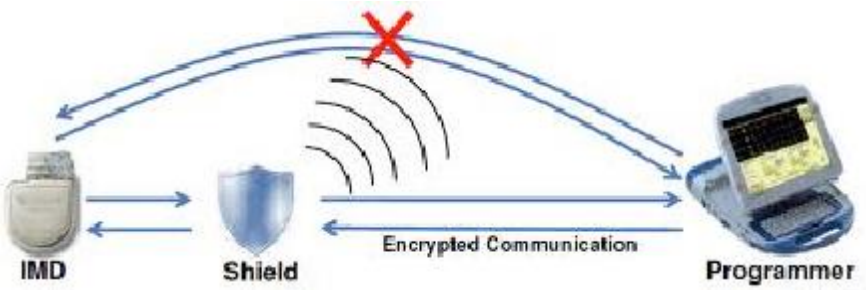
CyBOK

- Security is not only about keeping attackers out
- It is also about
  - Understanding risks
  - Mitigating
  - Detecting
  - Responding

to adversaries that have partial access to your system

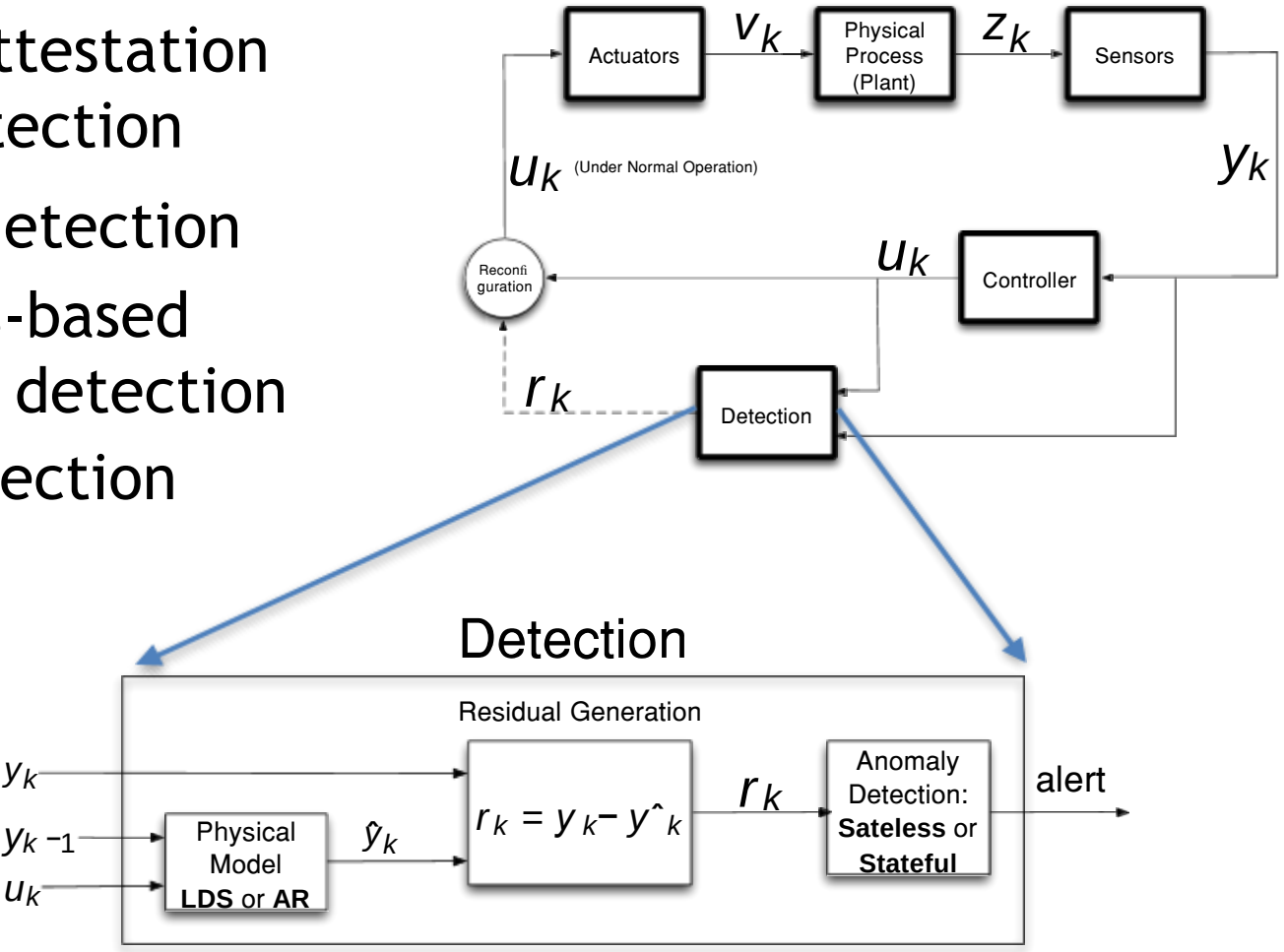
Preventing Attacks

- Securing Legacy Systems
  - Bump-in-the-wire
  - Wireless shields
  - Retrofitting security in legacy communications
- Lightweight security
- High-assurance systems
- Preventing **transduction attacks**



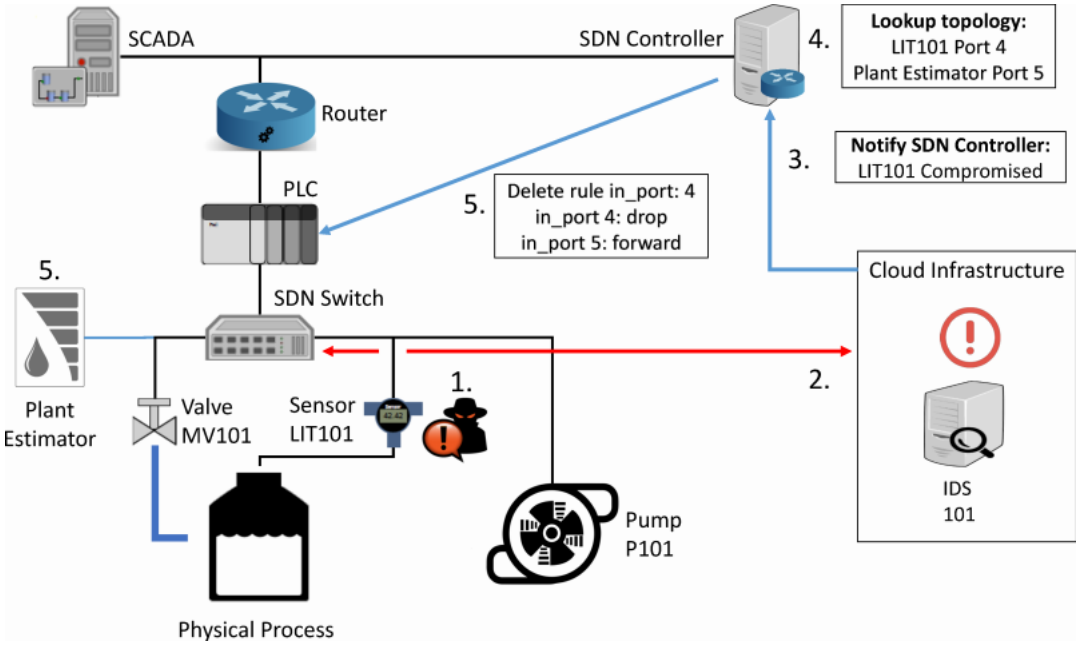
Detecting Attacks

- Remote attestation
- Misuse detection
- Anomaly detection
  - Physics-based attack detection
- Active detection



Mitigating Attacks

- Conservative control
- Security indices
- Resilient estimation
- Inertial resets
- Constraining actuation
- Virtual sensors
- Reactive response (game theory)
- Safe controls



University of BRISTOL

CyBOK

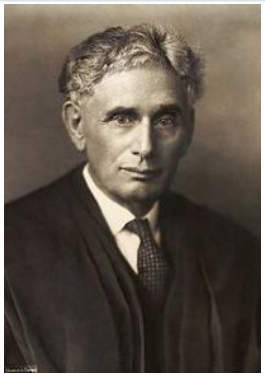
Privacy in CPS

bristol.ac.uk

Privacy and New Technologies

Warren and Brandeis

(1890)



- The right to be let alone (Thomas Cooley)
- There is a growing threat to this right
  - "recent inventions and business methods"
  - "instantaneous photographs"
- Cameras created a new privacy problem:
  - They allowed photography of unwilling or unknowing persons

Kevin Ashton Describes "the Internet of Things"

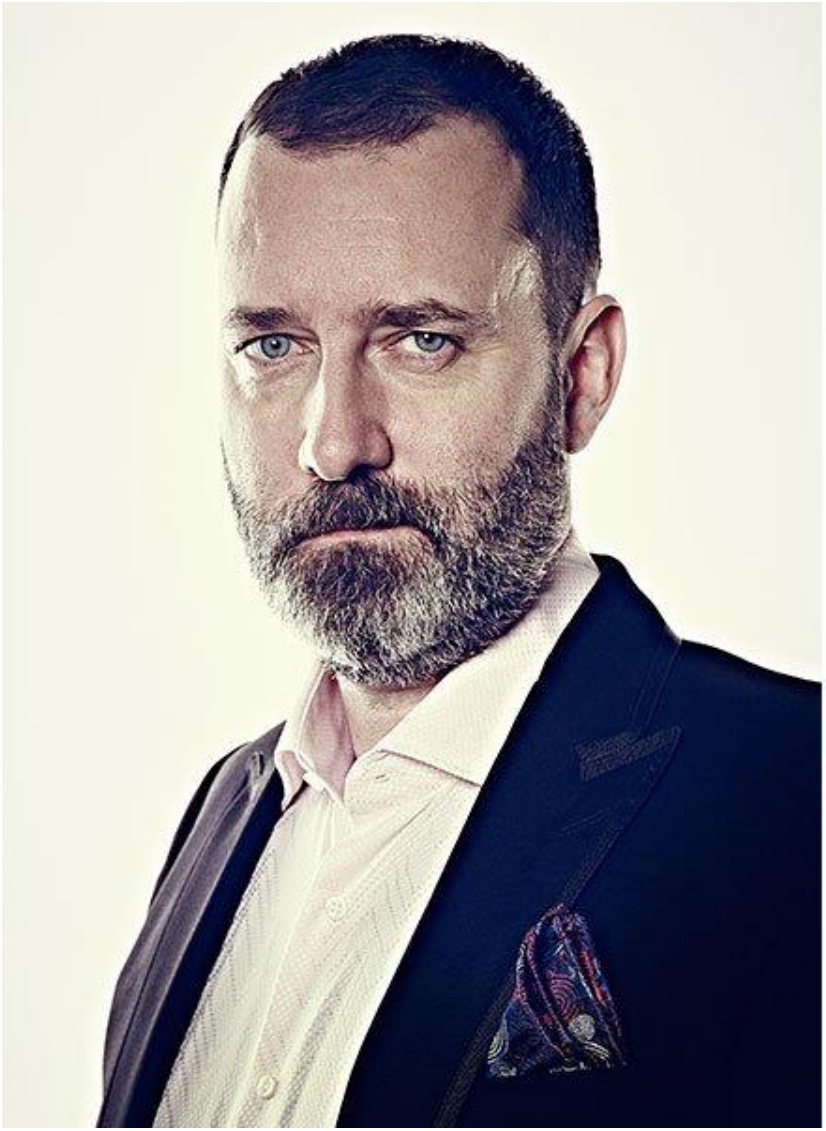
The innovator weighs in on what human life will be like a century from now

By Arik Gabbai

SMITHSONIAN MAGAZINE | SUBSCRIBE

JANUARY 2015

- 20th Century: computers were brains without senses—-they only knew what we told them.
- More info in the world than what people can type on keyboard
- 21st century: computers sense things, e.g., GPS we take for granted in our phones



Kevin Ashton (British entrepreneur) coined the term IoT in 1999.

Vehicular Privacy

CyBOK

Ford Exec: 'We Know Everyone Who Breaks The Law' Thanks To Our GPS In Your Car

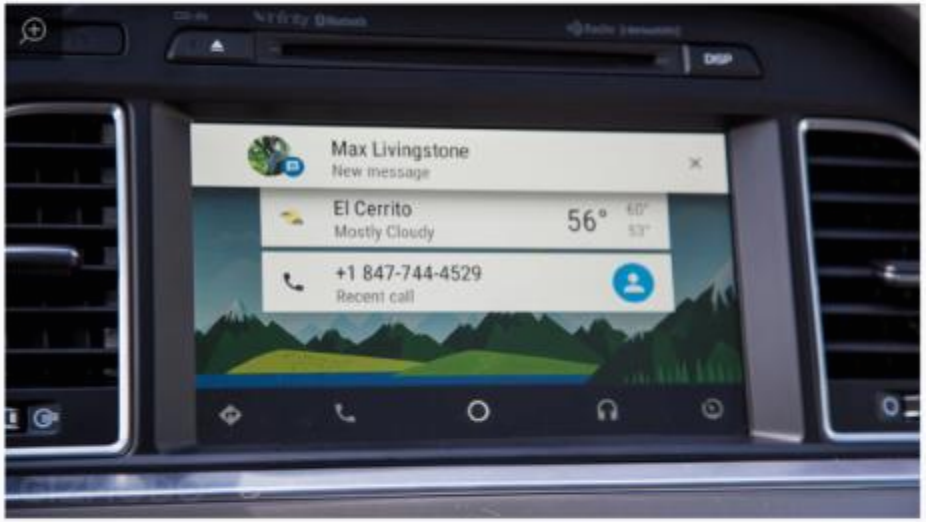
Jim Edwards Jan. 8, 2014, 8:16 PM

GIZMODO

Google Swears Android Auto Isn't Spying On You (That Much)

Adam Clark Estes
Filed to: VROOM VROOM 10/07/15 2:40pm

13,831 12

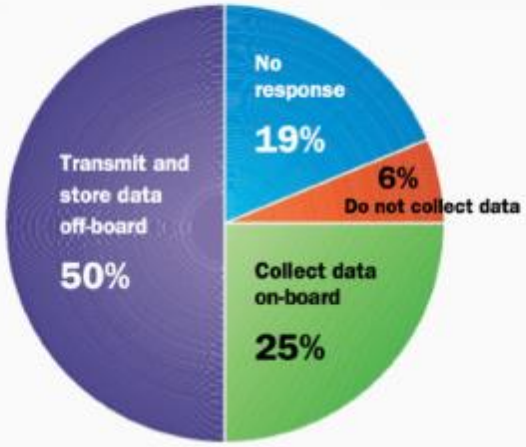


The era of car computers is upon us, and it's a little scary from a privacy perspective. Look no further than the recent controversy of how much data Google is collecting about drivers using Android Auto. We know this much: Google is probably collecting more data than you realize.

Tracking & Hacking:

Security & Privacy Gaps Put American Drivers at Risk

PERCENTAGE OF AUTOMOBILE MANUFACTURERS THAT COLLECT AND TRANSMIT DRIVING HISTORY DATA



naked security by SOPHOS

Award-winning computer security news

"Cheaper car insurance" dongle could lead to a privacy wreck

Drones and Privacy

CyBOK

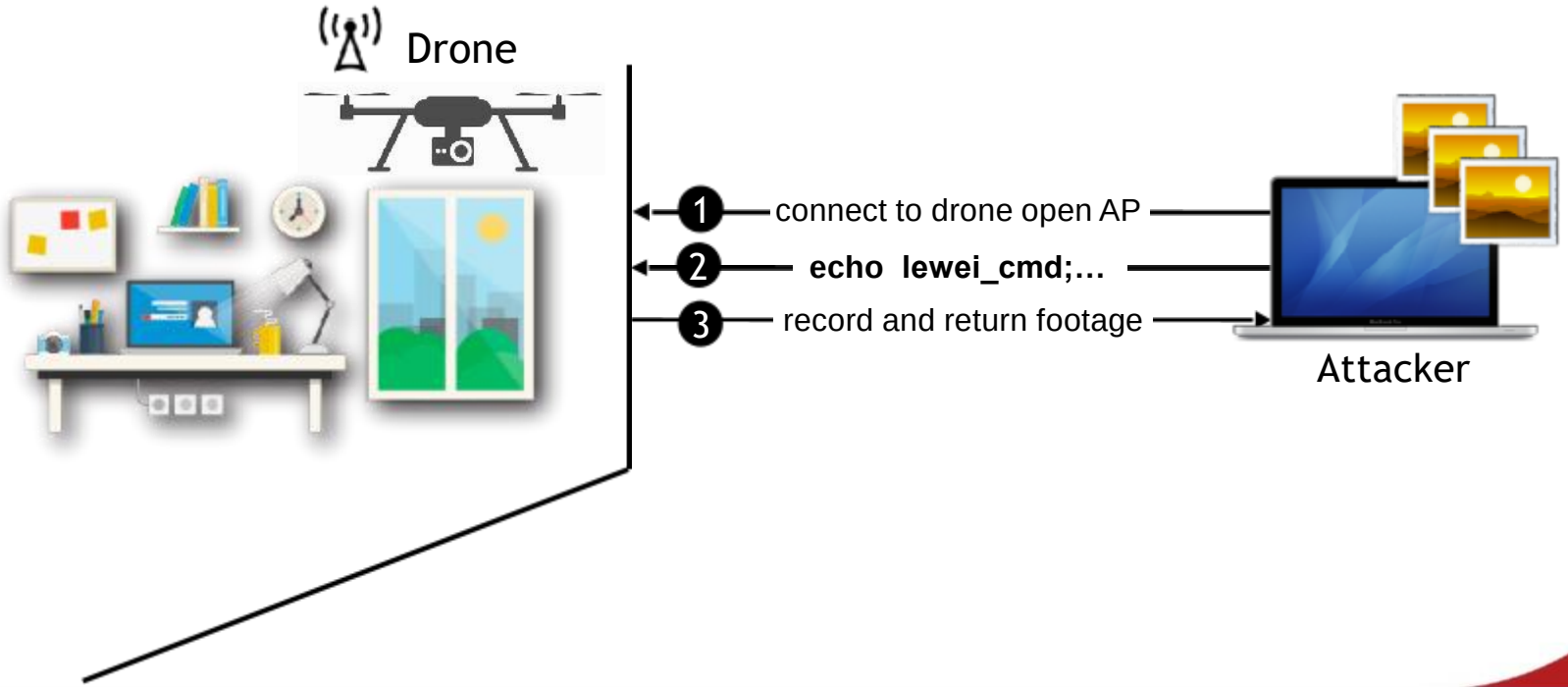
So This Is How It Begins: Guy Refuses to Stop Drone-Spying on Seattle Woman

Is this legal?

REBECCA J. ROSEN | MAY 13, 2013 | TECHNOLOGY

Share Tweet ...

"...since airplanes and helicopters often fly over private property, citizens do not have a reasonable expectation of privacy that their activities will not be observed from the air"
- U.S. Supreme Court (Florida v. Riley)



Location Privacy

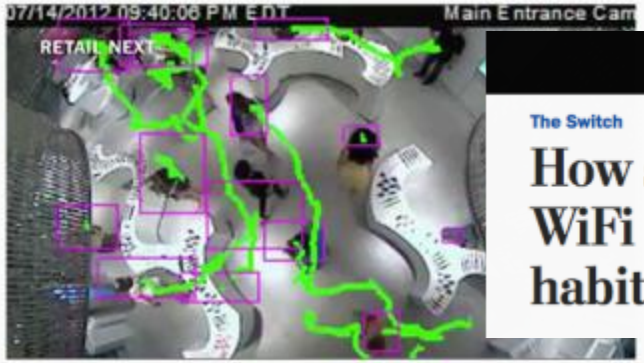
CyBOK

The New York Times

BUSINESS DAY

Attention, Shoppers: Store Is Tracking Your Cell

By STEPHANIE CLIFFORD and QUENTIN HARDY JULY 14, 2013



The Washington Post

The Switch

How stores use your phone's WiFi to track your shopping habits

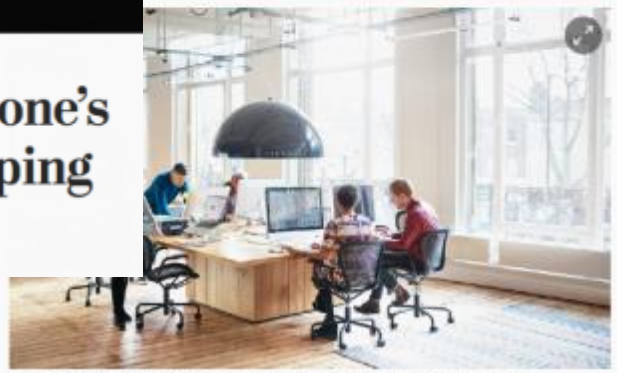
theguardian

home › environment › energy pollution climate change wildlife election 20 all

Guardian sustainable business Smart cities

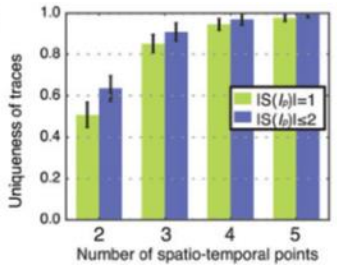
Smart buildings monitor energy efficiency, but what are they really tracking?

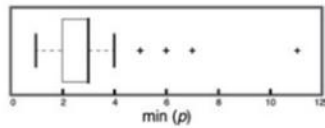
Space utilisation technology aims to make offices more efficient and people friendly but there are concerns around privacy



THE WALL STREET JOURNAL.

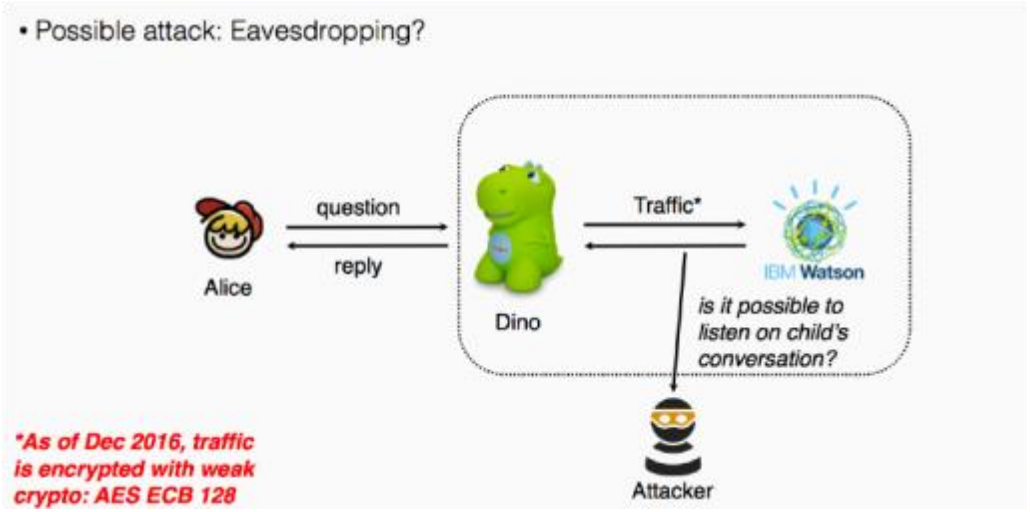
What Secrets Your Phone Is Sharing About You





IoT for Children

Children are easy molded.
Accept standards of surveillance.



Smart Homes and Privacy

University of BRISTOL

CyBOK

Policy and Political Aspects

bristol.ac.uk

Security is a Hard Business Case

CyBOK

- *"Making a strong business case for cybersecurity investment is complicated by the difficulty of quantifying risk in an environment of rapidly changing, unpredictable threats with consequences that are hard to demonstrate"*
  - DoE. Roadmap to Achieve Energy Delivery Systems Cybersecurity

As a Result Systems are Vulnerable with Basic Security Gaffes

CyBOK

- Unauthenticated remote connection to devices
- Unencrypted communications
- Hardcoded backdoor from manufacturer
- Hardcoded keys in devices
- Devices have several easily exploitable vulnerabilities

- Security incentives (regulation?) represent the most pressing challenge for improving the security posture of critical infrastructures

Cyberconflict

CyBOK

- Computer networks are an extension to the way we interact with others
  - Any conflict will have its equivalent representation in cyberspace.
- Cybercrime (violation of domestic law)
- Cyberespionage (OK under international law; nation-states)
- Cyberwar (cyber attacks in armed conflict)

  - M. Schmitt. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, 2012.

The Law of War Applies in Cyberspace

CyBOK

- Tallin Manual: Non-binding study on how International Law applies to cyber conflicts. NATO's cooperative cyber-defense center of excellence.
- The Koh Speech: State Dept. legal advisor Harold Koh, explaining how U.S. interprets international law to cyberspace
  - jus ad bellum (right to enter a war)
  - jus in bellum (acceptable wartime conduct)
- Physical effects of a cyber-operation are key
  - Are they similar to kinetic effects caused by e.g. missile?
  - Grey area: cyber-attacks that do not rise to the level of armed attacks
- Challenges: proportionality, attribution, and distinction (civilian and military objectives)

Conclusions

CyBOK

- Attacks to CPS are growing: Attackers have the motivations, knowledge, resources, and persistence to launch attacks that will damage the physical world (even humans)
  - We need to be prepared to prevent, detect, mitigate, and respond to these attacks
- Privacy issues are also a growing concern
  - We need to design mechanisms to facilitate the utility of the CPS system while minimizing privacy loses
- Policy and political aspects
  - Incentives for securing CPS
  - Need new international legal frameworks for cyber conflict