The Kaspersky Security Symposium

Sep 21 – 23, 2011 | Munich | Germany

Tomorrow Has Already Arrived

Magnus Kalkuhl

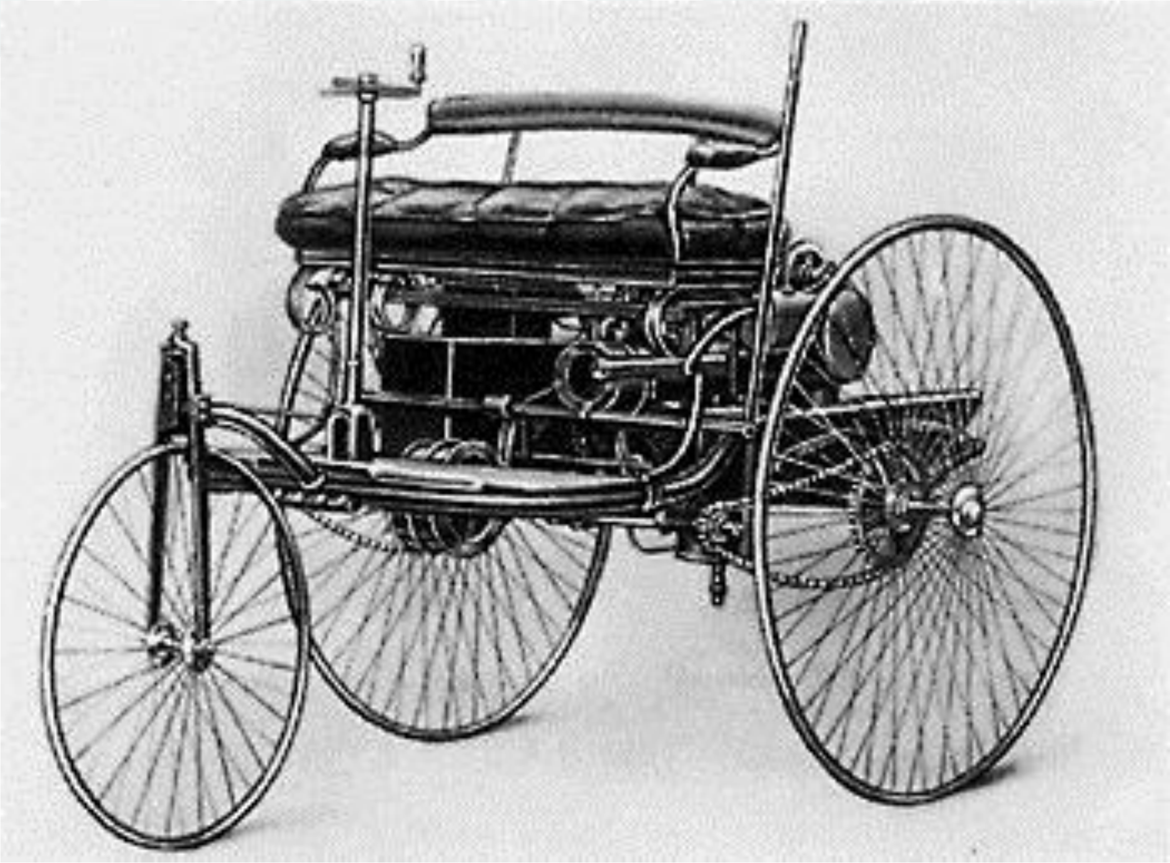
Deputy Director, Global Research and Analysis Team

Welcome

?

From: 2001: A Space Odyssey (1968)

Smart Cars

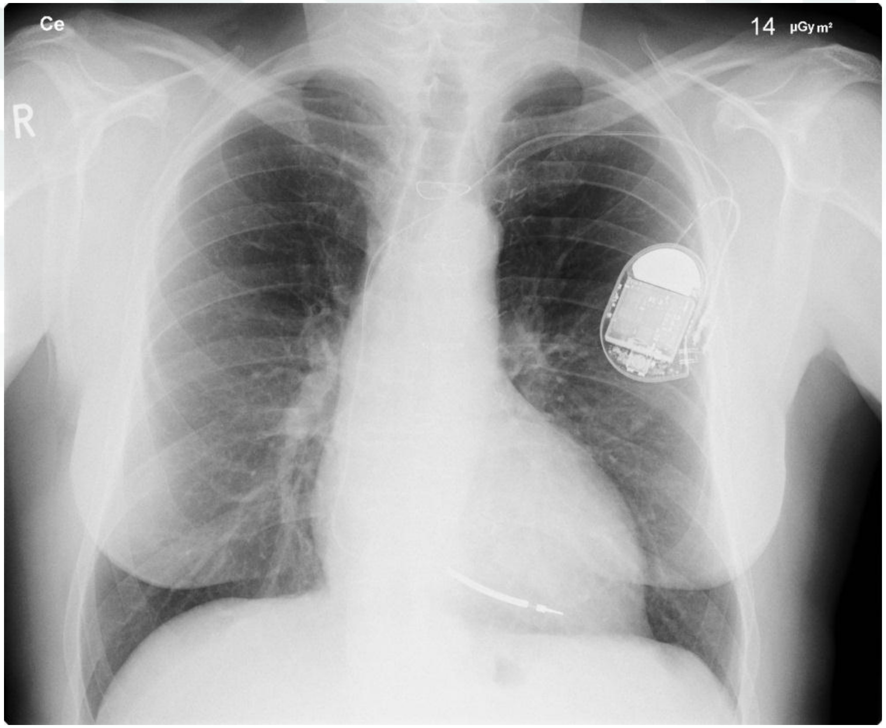


An old car!

Insulin Pumps

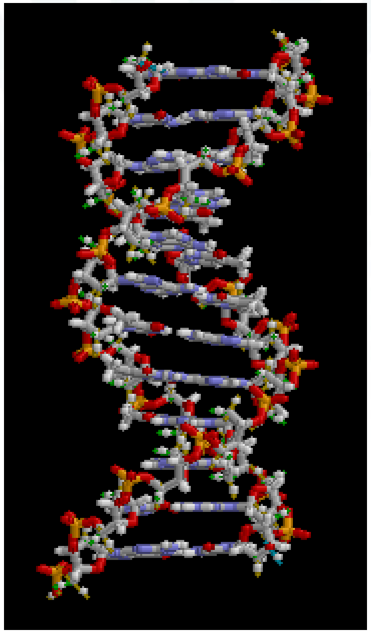
- An insulin pump can be remotely controlled via wireless communication
- Hack introduced in 2011 by Jerome Radcliffe

Pacemakers

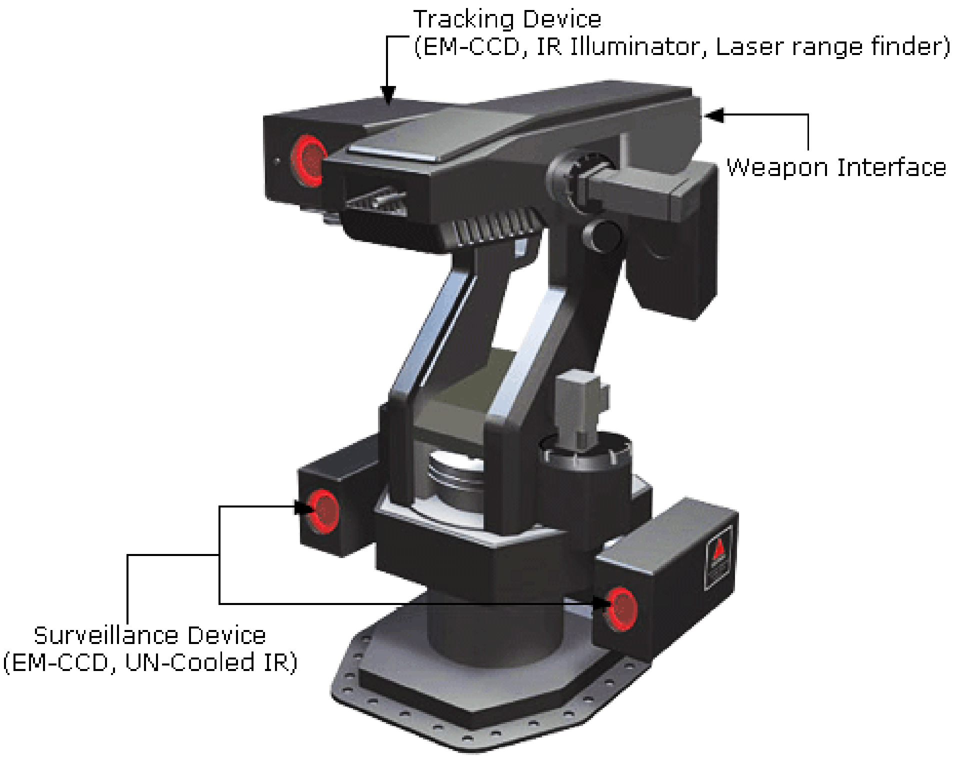


- Wireless communication between a pacemaker (older model) and its control device is unencrypted
- Hack introduced in 2008 by Kevin Fu
- Potential victims:
  2.6 million people operated on in 1990-2002

Do you know this?



Samsung SGR-A1 Military Robot

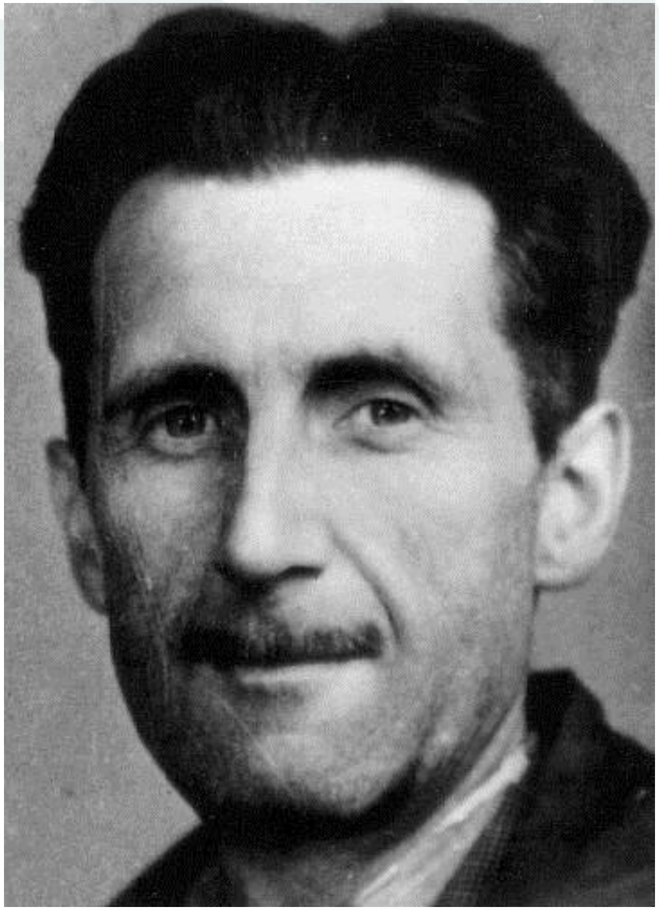


- Introduced in 2006
- Designed to guard the DMZ for South Korea
- Asks for a password
- Can react to intruders by ringing an alarm or by using a mounted machine gun!

General Atomics MQ-1 Predator

- Unmanned aerial vehicle (UAV)
- Fully remote controlled
- Armed version in use since 2001
- Can be equipped with Hellfire missiles

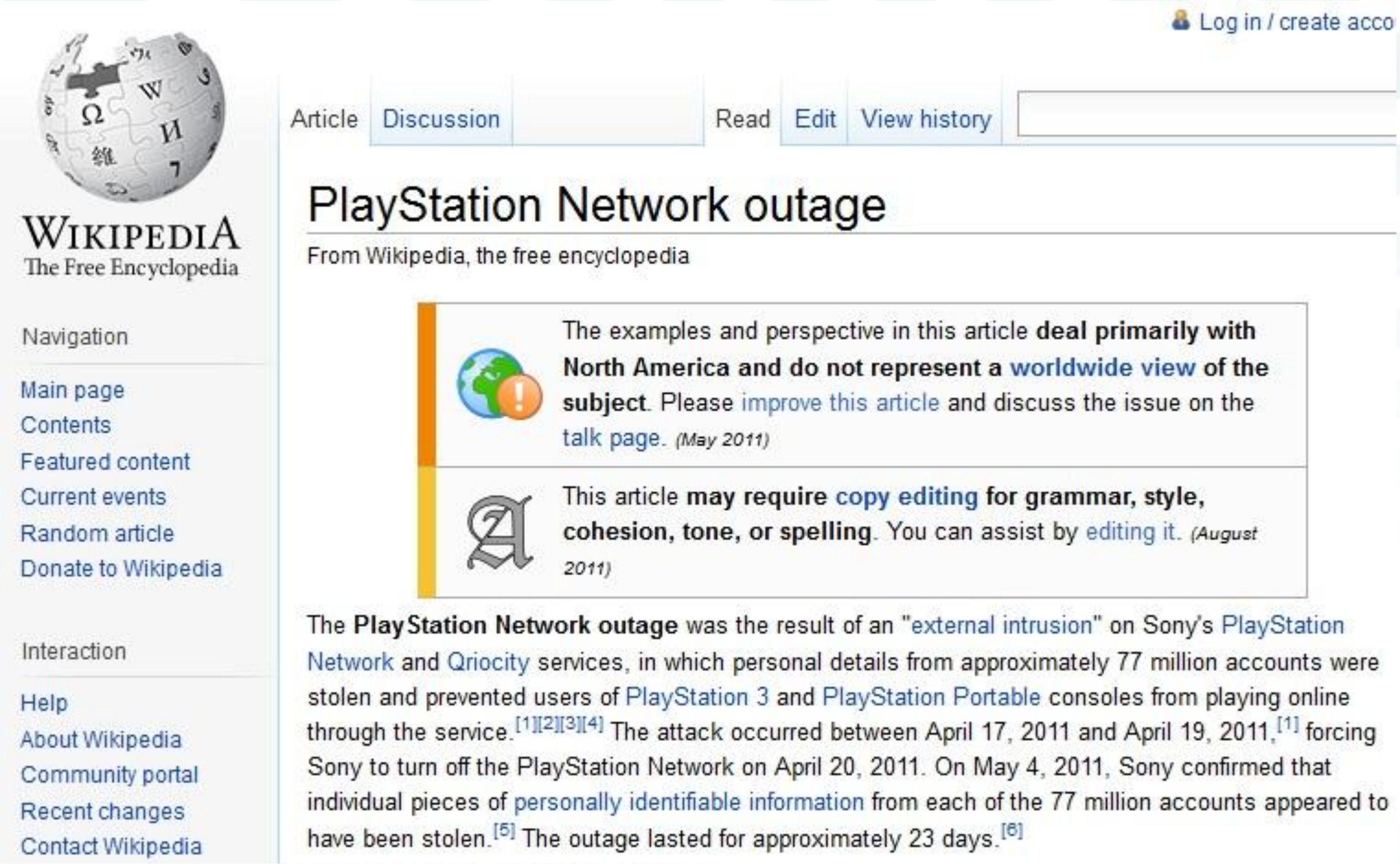
1984



- Dystopian novel written by George Orwell in 1948
- Quote:

  Behind Winston's back the voice from the telescreen was still babbling (…) The telescreen received and transmitted simultaneously.

But Gamers Are Safe, Aren‘t They?



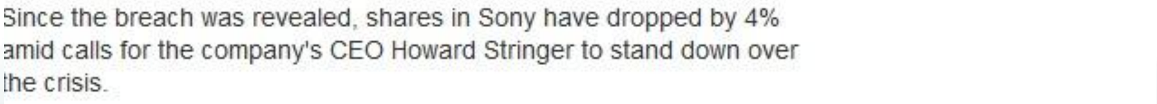
PlayStation Network outage

From Wikipedia, the free encyclopedia

The examples and perspective in this article **deal primarily with North America and do not represent a worldwide view of the subject**. Please improve this article and discuss the issue on the talk page. *(May 2011)*

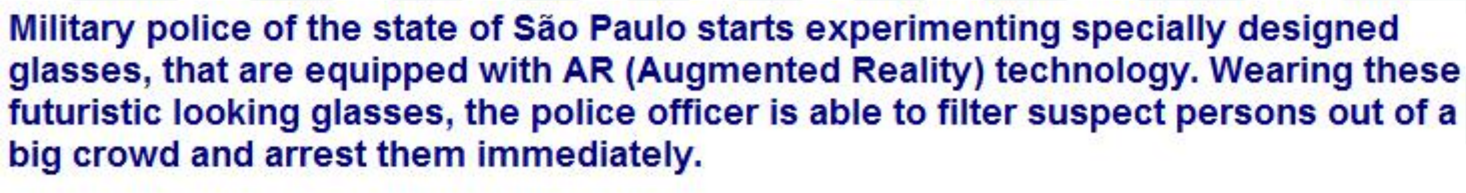
This article **may require copy editing for grammar, style, cohesion, tone, or spelling**. You can assist by editing it. *(August 2011)*

The **PlayStation Network outage** was the result of an "external intrusion" on Sony's PlayStation Network and Qriocity services, in which personal details from approximately 77 million accounts were stolen and prevented users of PlayStation 3 and PlayStation Portable consoles from playing online through the service.[1][2][3][4] The attack occurred between April 17, 2011 and April 19, 2011,[1] forcing Sony to turn off the PlayStation Network on April 20, 2011. On May 4, 2011, Sony confirmed that individual pieces of personally identifiable information from each of the 77 million accounts appeared to have been stolen.[5] The outage lasted for approximately 23 days.[6]

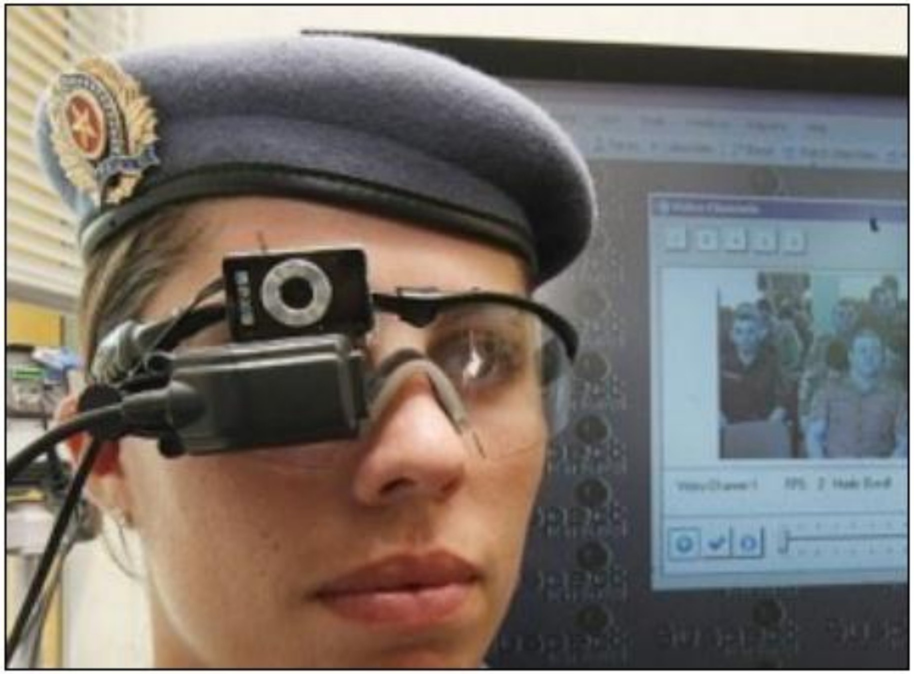


Since the breach was revealed, shares in Sony have dropped by 4% amid calls for the company's CEO Howard Stringer to stand down over the crisis.

Face Recognition

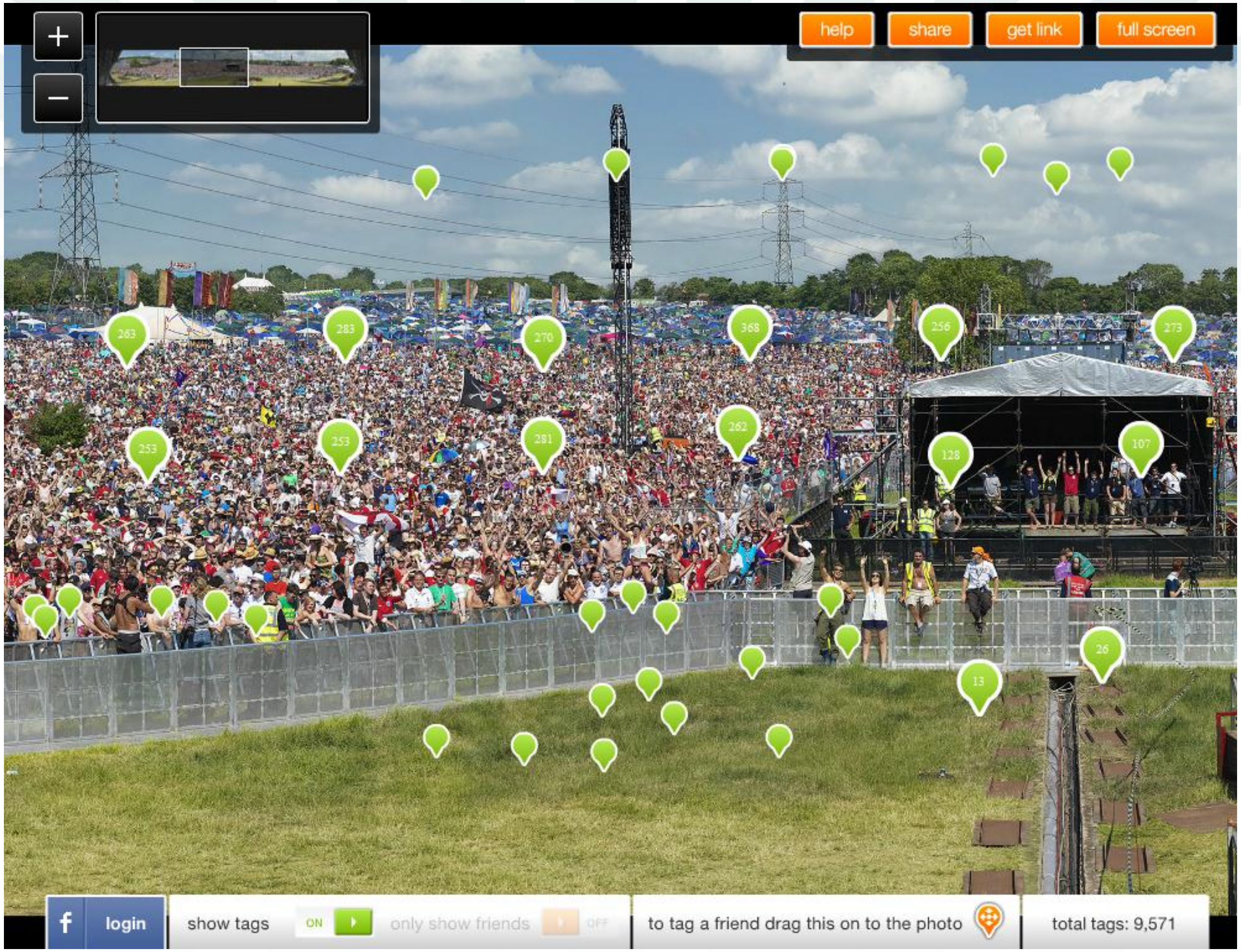


Military police of the state of São Paulo starts experimenting specially designed glasses, that are equipped with AR (Augmented Reality) technology. Wearing these futuristic looking glasses, the police officer is able to filter suspect persons out of a big crowd and arrest them immediately.



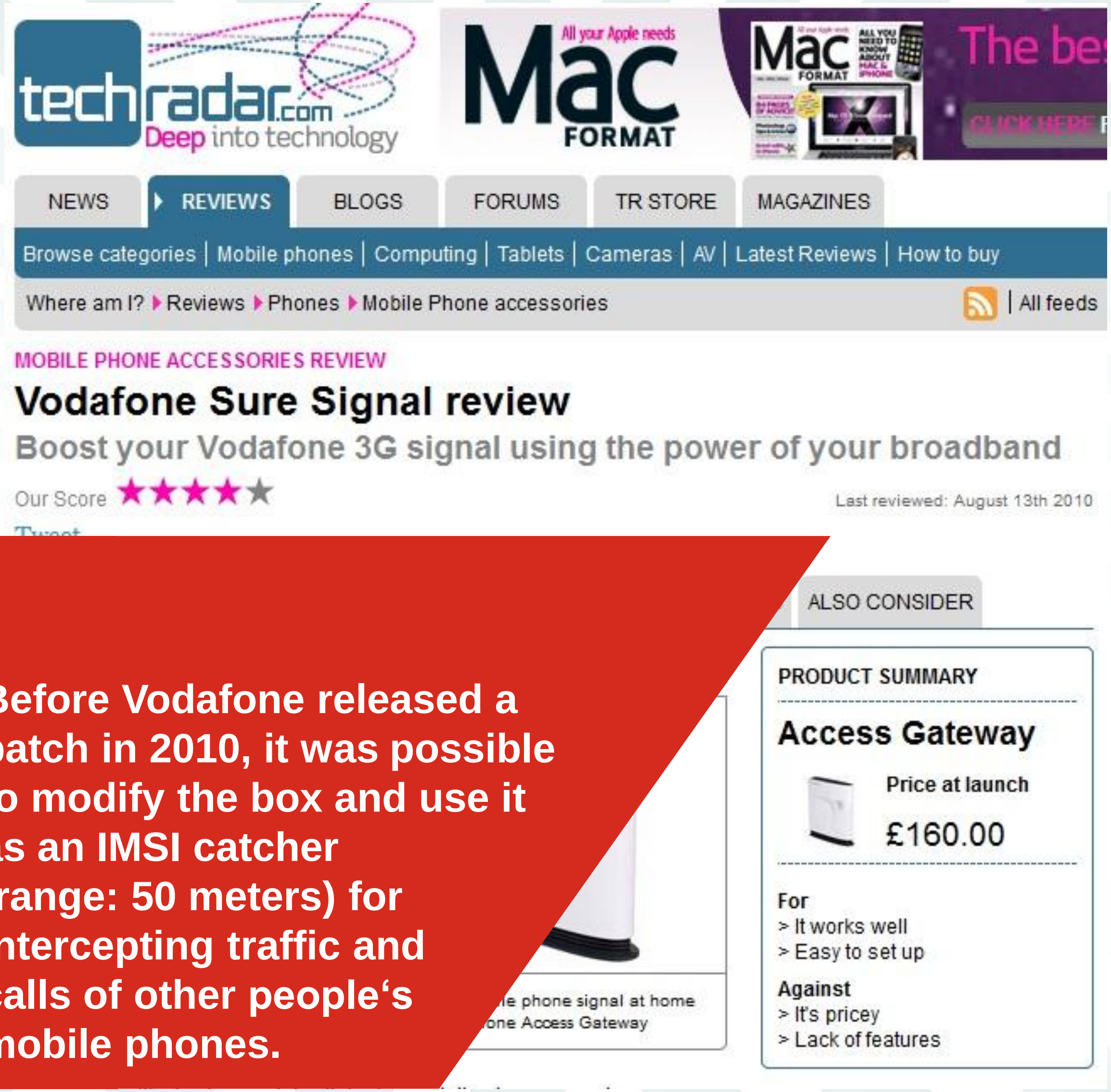
Source: http://www.eyebrazil.com

The Glastonbury Experiment



Source: http://glastonbury.orange.co.uk/glastotag/

Fun with Phones



techradar.com Deep into technology

All your Apple needs Mac FORMAT

The bes CLICK HERE

NEWS
REVIEWS
BLOGS
FORUMS
TR STORE
MAGAZINES
Browse categories | Mobile phones | Computing | Tablets | Cameras | AV | Latest Reviews | How to buy
Where am I? Reviews Phones Mobile Phone accessories
All feeds

MOBILE PHONE ACCESSORIES REVIEW

Vodafone Sure Signal review

Boost your Vodafone 3G signal using the power of your broadband

Our Score ★★★★★

Last reviewed: August 13th 2010

Tweet

ALSO CONSIDER

PRODUCT SUMMARY

Access Gateway

Price at launch

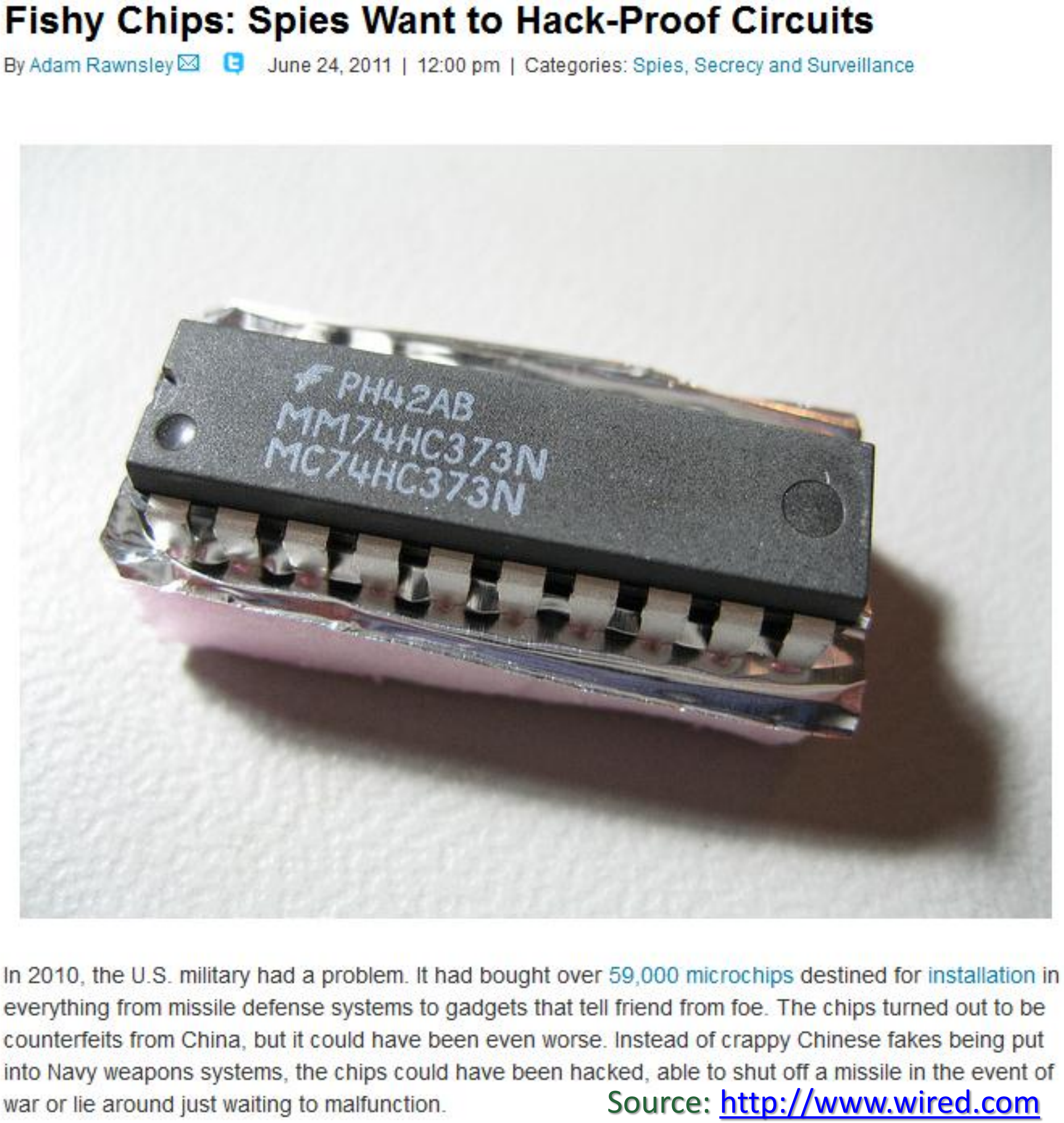
£160.00

For
> It works well
> Easy to set up

Against
> It's pricey
> Lack of features

e phone signal at home
one Access Gateway

Before Vodafone released a patch in 2010, it was possible to modify the box and use it as an IMSI catcher (range: 50 meters) for intercepting traffic and calls of other people‘s mobile phones.



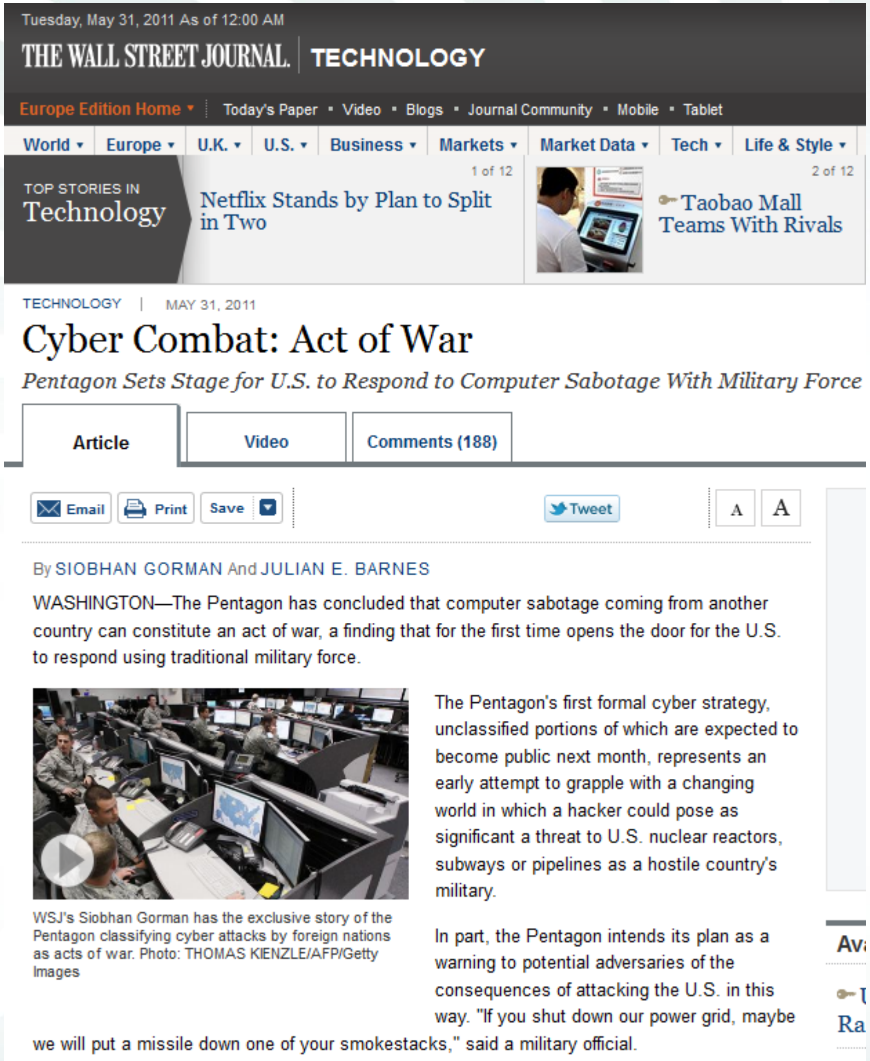
Fishy Chips: Spies Want to Hack-Proof Circuits

By Adam Rawnsley | June 24, 2011 | 12:00 pm | Categories: Spies, Secrecy and Surveillance

In 2010, the U.S. military had a problem. It had bought over 59,000 microchips destined for installation in everything from missile defense systems to gadgets that tell friend from foe. The chips turned out to be counterfeits from China, but it could have been even worse. Instead of crappy Chinese fakes being put into Navy weapons systems, the chips could have been hacked, able to shut off a missile in the event of war or lie around just waiting to malfunction.

Source: http://www.wired.com

Cyber Combat Doesn‘t Come Without Risks



Tuesday, May 31, 2011 As of 12:00 AM

THE WALL STREET JOURNAL. | TECHNOLOGY

Europe Edition Home ▾
Today's Paper · Video · Blogs · Journal Community · Mobile · Tablet
World ▾ | Europe ▾ | U.K. ▾ | U.S. ▾ | Business ▾ | Markets ▾ | Market Data ▾ | Tech ▾ | Life & Style ▾

TOP STORIES IN Technology

1 of 12 Netflix Stands by Plan to Split in Two

2 of 12 Taobao Mall Teams With Rivals

TECHNOLOGY | MAY 31, 2011

Cyber Combat: Act of War

Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force

Article
Video
Comments (188)
Email
Print
Save
Tweet
A
A

By SIOBHAN GORMAN And JULIAN E. BARNES

WASHINGTON—The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force.

WSJ's Siobhan Gorman has the exclusive story of the Pentagon classifying cyber attacks by foreign nations as acts of war. Photo: THOMAS KIENZLE/AFP/Getty Images

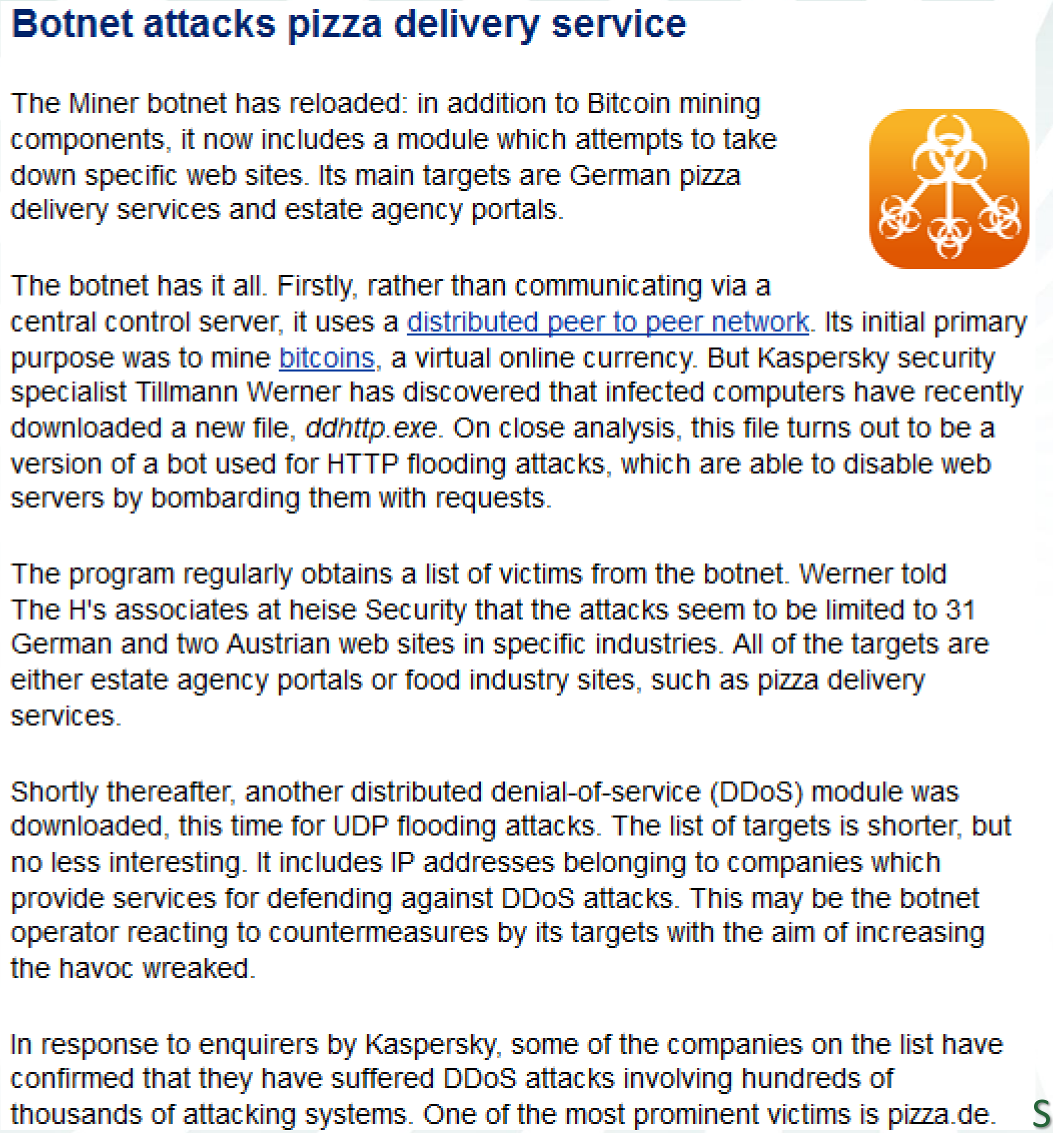
The Pentagon's first formal cyber strategy, unclassified portions of which are expected to become public next month, represents an early attempt to grapple with a changing world in which a hacker could pose as significant a threat to U.S. nuclear reactors, subways or pipelines as a hostile country's military.

In part, the Pentagon intends its plan as a warning to potential adversaries of the consequences of attacking the U.S. in this way. "If you shut down our power grid, maybe we will put a missile down one of your smokestacks," said a military official.

- Quote:

  "“If you shut down our power grid, maybe we will put a missile down one of your smokestacks‘ said a military official"

Who would do such a thing?



Botnet attacks pizza delivery service

The Miner botnet has reloaded: in addition to Bitcoin mining components, it now includes a module which attempts to take down specific web sites. Its main targets are German pizza delivery services and estate agency portals.

The botnet has it all. Firstly, rather than communicating via a central control server, it uses a distributed peer to peer network. Its initial primary purpose was to mine bitcoins, a virtual online currency. But Kaspersky security specialist Tillmann Werner has discovered that infected computers have recently downloaded a new file, *ddhttp.exe*. On close analysis, this file turns out to be a version of a bot used for HTTP flooding attacks, which are able to disable web servers by bombarding them with requests.

The program regularly obtains a list of victims from the botnet. Werner told The H's associates at heise Security that the attacks seem to be limited to 31 German and two Austrian web sites in specific industries. All of the targets are either estate agency portals or food industry sites, such as pizza delivery services.

Shortly thereafter, another distributed denial-of-service (DDoS) module was downloaded, this time for UDP flooding attacks. The list of targets is shorter, but no less interesting. It includes IP addresses belonging to companies which provide services for defending against DDoS attacks. This may be the botnet operator reacting to countermeasures by its targets with the aim of increasing the havoc wreaked.

In response to enquirers by Kaspersky, some of the companies on the list have confirmed that they have suffered DDoS attacks involving hundreds of thousands of attacking systems. One of the most prominent victims is pizza.de.

Source: http://www.h-online.com

Thank you

- Magnus Kalkuhl
  magnus.kalkuhl@kaspersky.com