MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THE INTERNET OF HUMANS: BIOPWNING YOUR FRIENDS AND FAMILY

Chris Poulin

Director, IoT Security Innovation, Booz Allen Hamilton

@ChrisPoulin

“Things” social engineer

- Maker
- Breaker
- Threat intel
- Data geek
- Provocateur
- TV & movies

THE PANORAMIC THREATSCAPE

Threats to data: ePHI / EMR

- Printouts, labels
- Laptops, thumb drives, backup tapes
- Malicious insiders, fraud
- Malware and ransomware; phishing

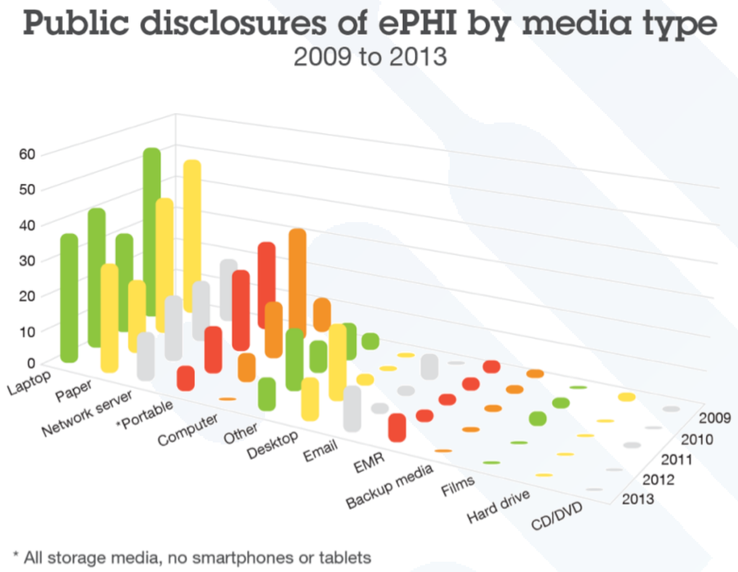
Threats to Patients

- Medical implantables
- Human augmentation

Past — **Present** — **Future**

Threats to infrastructure

- Basic network hygiene
- Connected devices
  (e.g., drug infusion, MRIs)



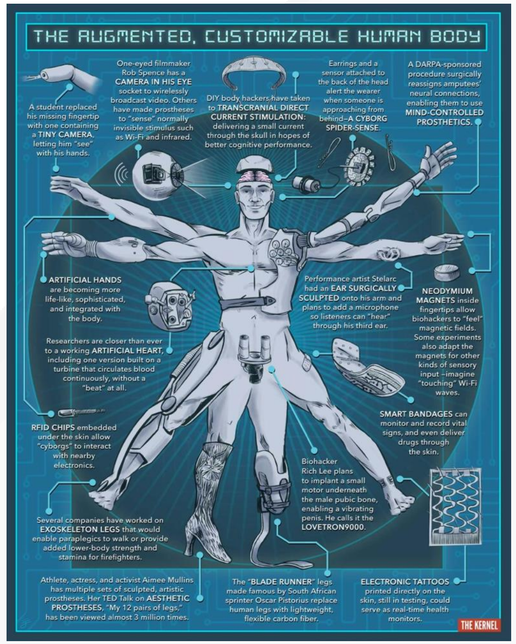
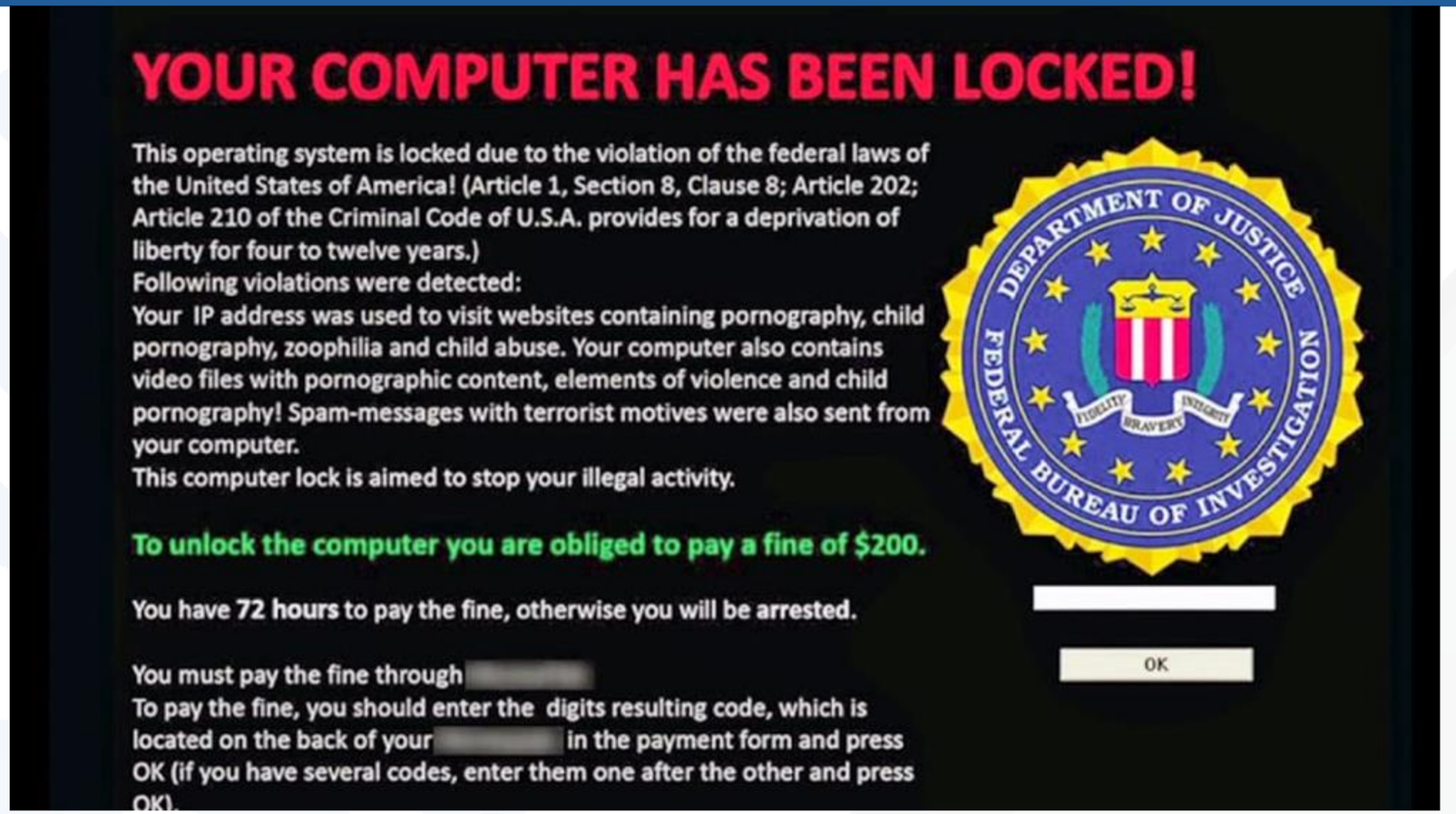


Illustration and infographic by J. Longo

WHY TALK ABOUT THE PAST WHEN THE PRESENT IS ALREADY SO TRAGIC?

MALWARE & RANSOMWARE IN MEDICAL SETTINGS



The U.S. Food and Drug Administration (FDA) issued the following statement: "We are aware of hundreds of medical devices that have been infected by malware."

MEDICAL DEVICES EXPOSE A BROAD THREAT SURFACE

- Bluetooth and WiFi
  - Centralized monitoring
  - Remote configuration
- Often built from open source
  - Operating systems, e.g., Linux and BusyBox
  - Libraries, e.g., OpenSSL, glibc (HeartBleed, GHOST)
  - Tool suites
- Some medical devices provide built-in web servers
  - Same technology that plagues SOHO routers

POOR DEVICE SECURITY CAN CAUSE HARM TO HUMANS

Improperly securing wireless protocols can allow hackers to cause severe patient injuries and deaths, as was demonstrated by security researcher Barnaby Jack's work on pacemakers and Jay Radcliffe's research on insulin pumps.

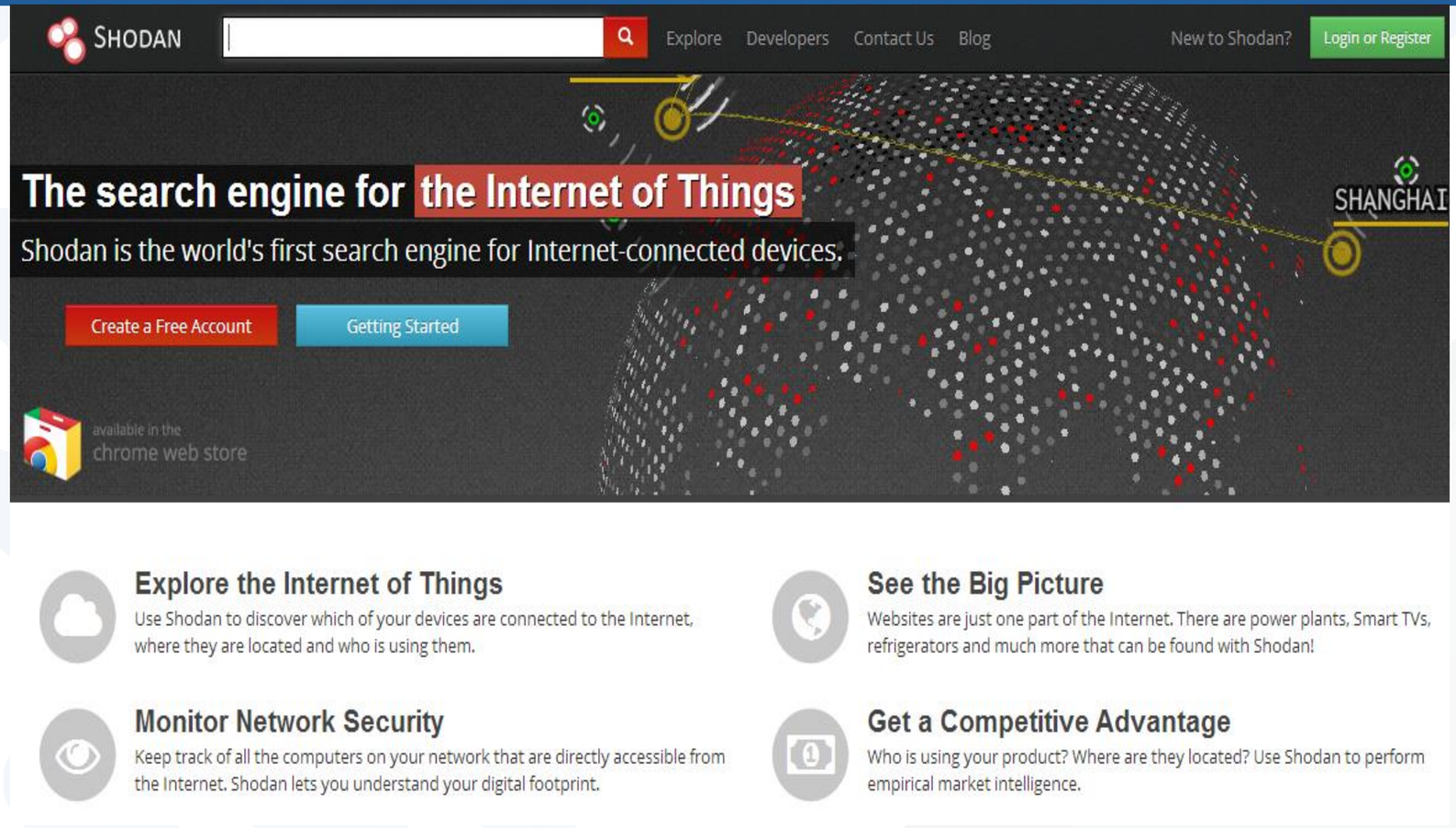
POOR DEVICE SECURITY CAN EXPOSE NETWORKS & DATA

783,000
medical devices
recalled since 2012

The FDA advised
hospitals to stop using
a particular infusion pump
because of vulnerabilities.

Security researchers have found evidence that
cyber criminals are trying to use
exposed and vulnerable medical devices
to gain access to hospital networks.

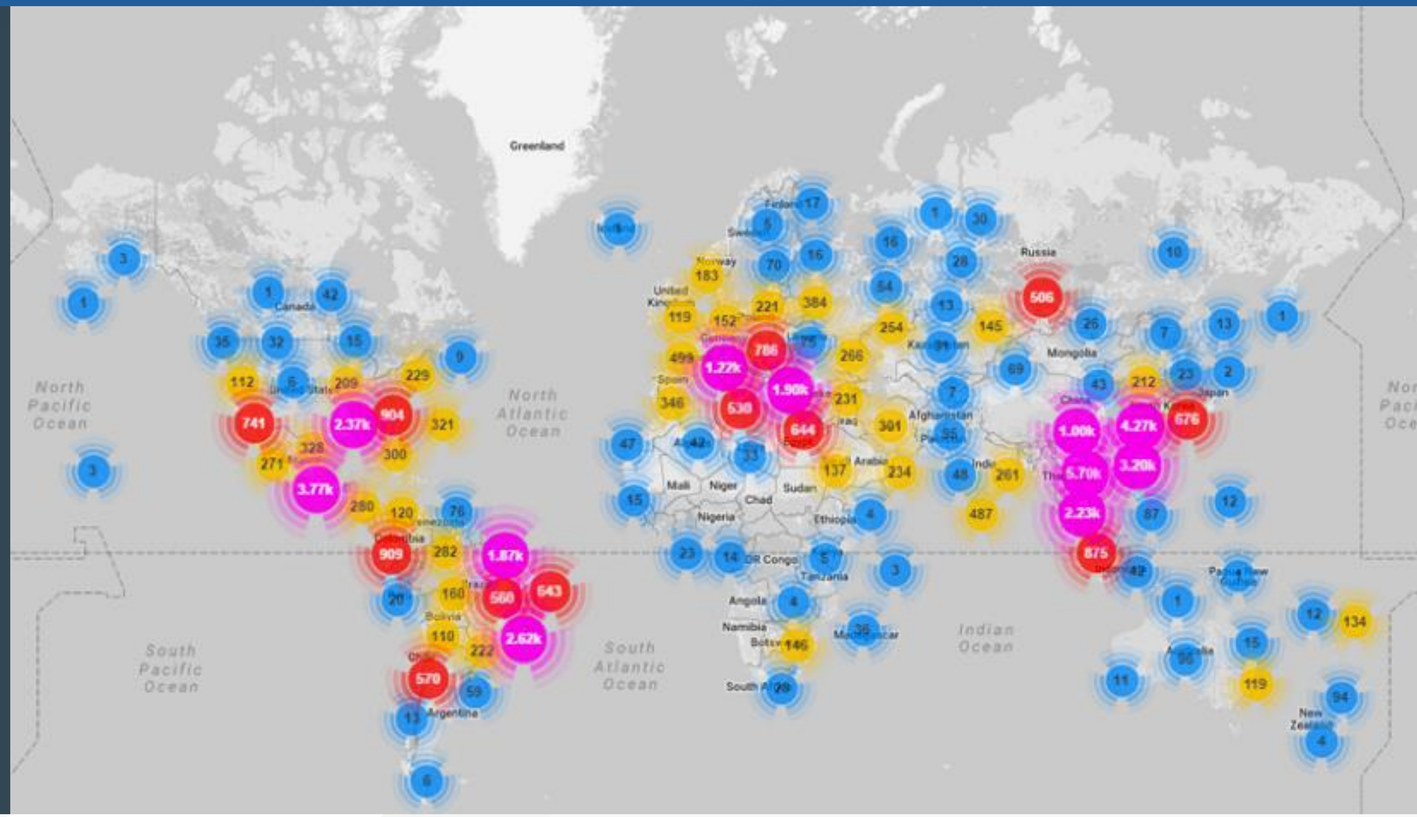
SHODAN: SEARCH ENGINE FOR THE IOT



Security researchers found over 68,000 medical systems exposed to the Internet, including drug infusion systems, MRI imaging machines, and anesthesia systems.

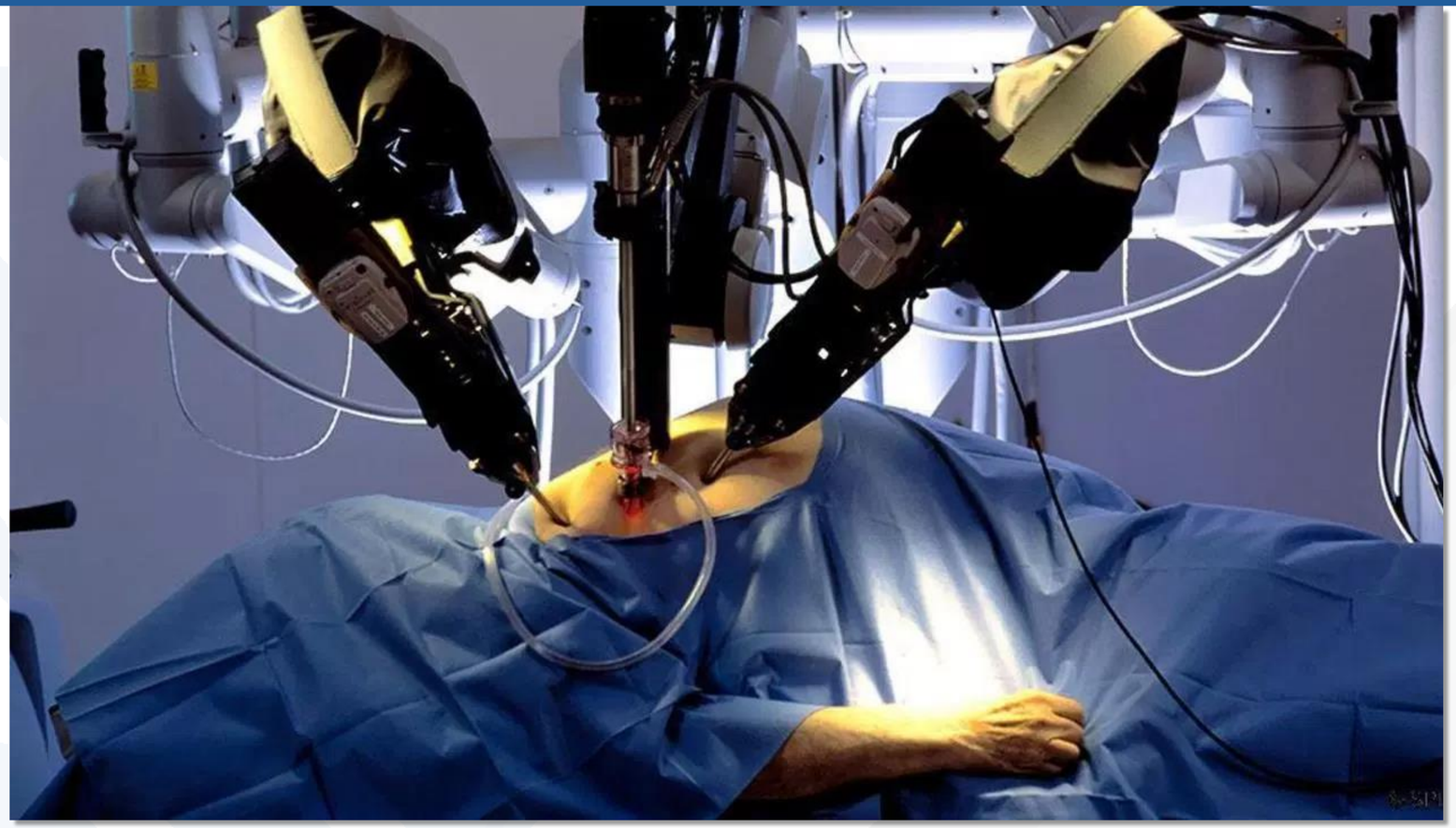
MIRAI EXPLOITED A COMMON IOT VULNERABILITY: HARDCODING

```
// root      xc3511      // root      vizxv          // root      admin
// admin     admin       // root      888888         // root      xmhdipc
// root      default     // root      juantech       // root      123456
// root      54321       // support   support        // root      (none)
// admin     password    // root      root           // root      12345
// user      user        // admin     (none)         // root      pass
// admin     admin1234   // root      1111           // admin     smcadmin
// admin     1111        // root      666666         // root      password
// root      1234        // root      klv123         // Administrator admin
// service   service     // supervisor supervisor    // guest     guest
// guest     12345       // guest     12345          // admin1    password
// administrator 1234    // 666666    666666         // 888888    888888
// ubnt      ubnt        // root      klv1234        // root      Zte521
// root      hi3518      // root      jvbzd          // root      anko
// root      zlxx.       // root      7ujMko0vizxv   // root      7ujMko0admin
// root      system      // root      ikwb           // root      dreambox
// root      user        // root      realtek        // root      00000000
// admin     1111111     // admin     1234           // admin     12345
// admin     54321       // admin     123456         // admin     7ujMko0admin
// admin     1234        // admin     pass           // admin     meinsm
// tech      tech
```



- Security researchers purchasing used medical devices have found hospital WiFi passwords and other configuration artifacts.
- Hardcoded usernames and passwords have been a large source of vulnerabilities in routers and consumer IoT devices and medical systems.

JUST COUNT BACK FROM 100…



Lack of authentication and encryption in medical device communications can allow attackers take over devices, as was demonstrated by security researchers working on tele-surgical robots.

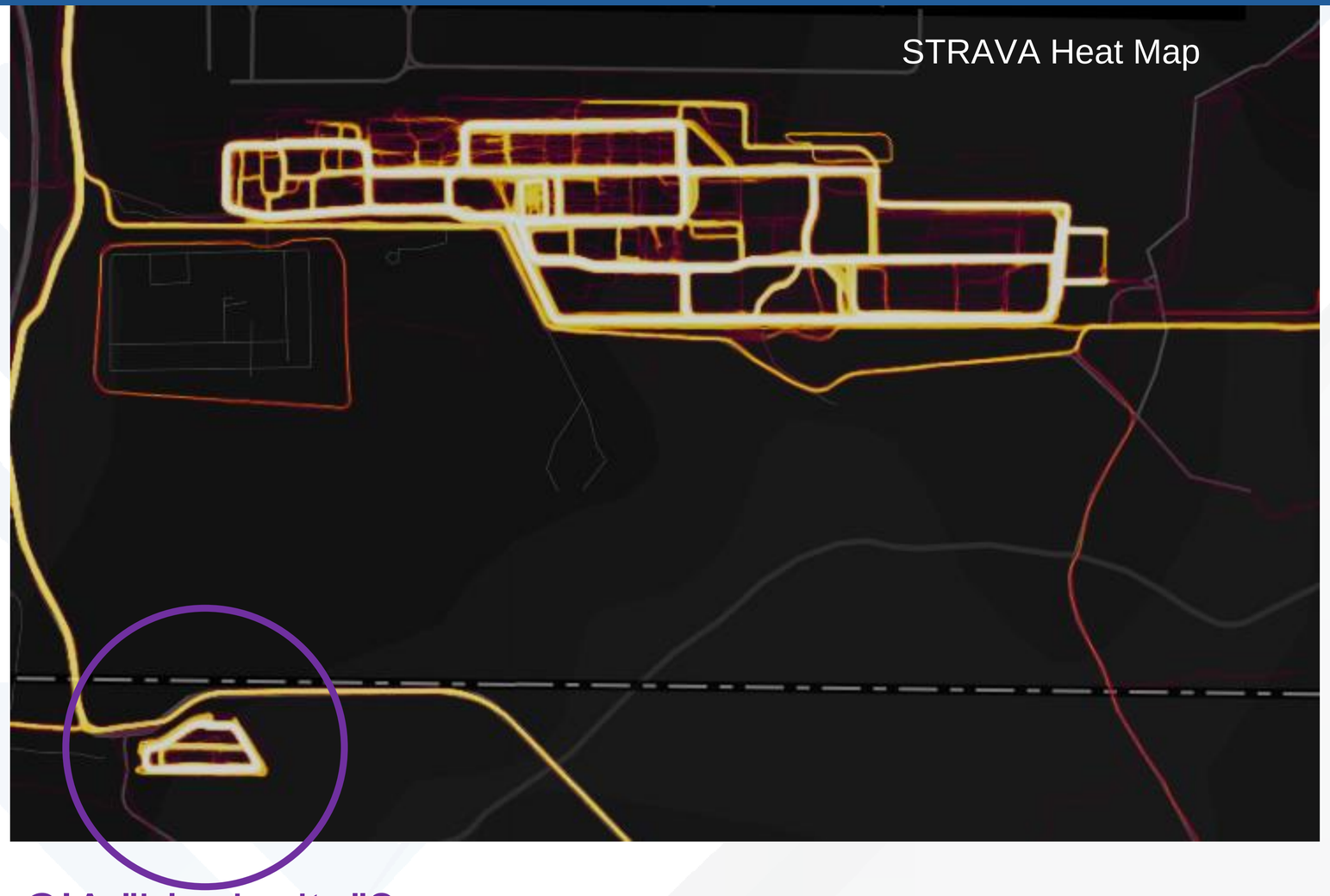
IS HEARTRATE AND FITNESS DATA ePHI?

WATCH

powered by android wear

Fitness Trackers

…OR IS FITNESS DATA CLASSIFIED NATIONAL SECURITY INTEL?

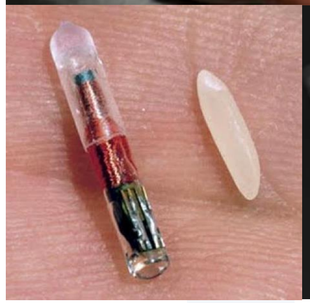


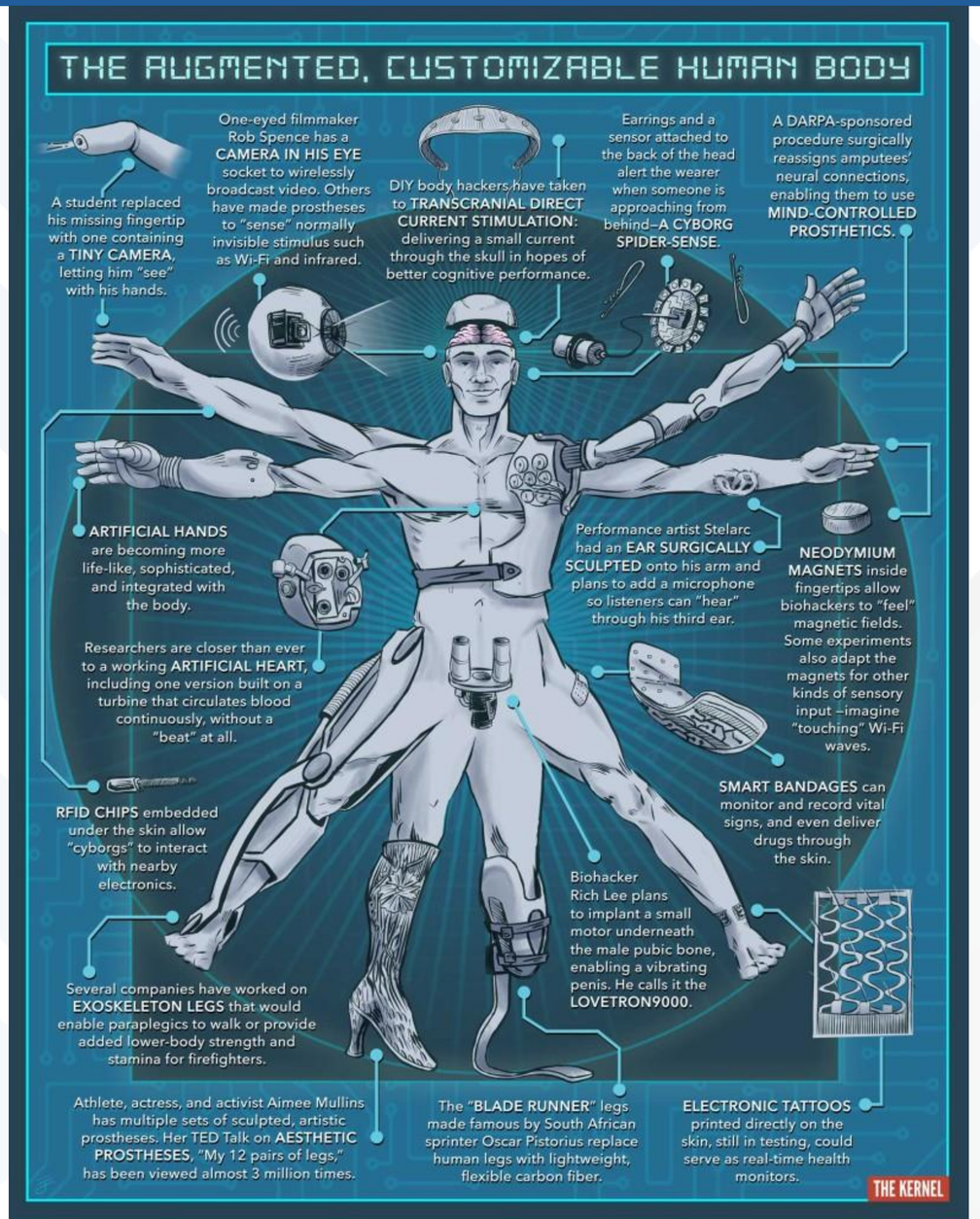
CIA ”black site”?

http://road.cc/content/news/236353-strava-accused-giving-away-military-secrets-through-its-global-heatmaps

THE FUTURE IS IN PROGRESS ALREADY—AND IT'S !$%&* SCARY

TOTAL HUMAN AUGMENTATION & TRAN-HUMANISM



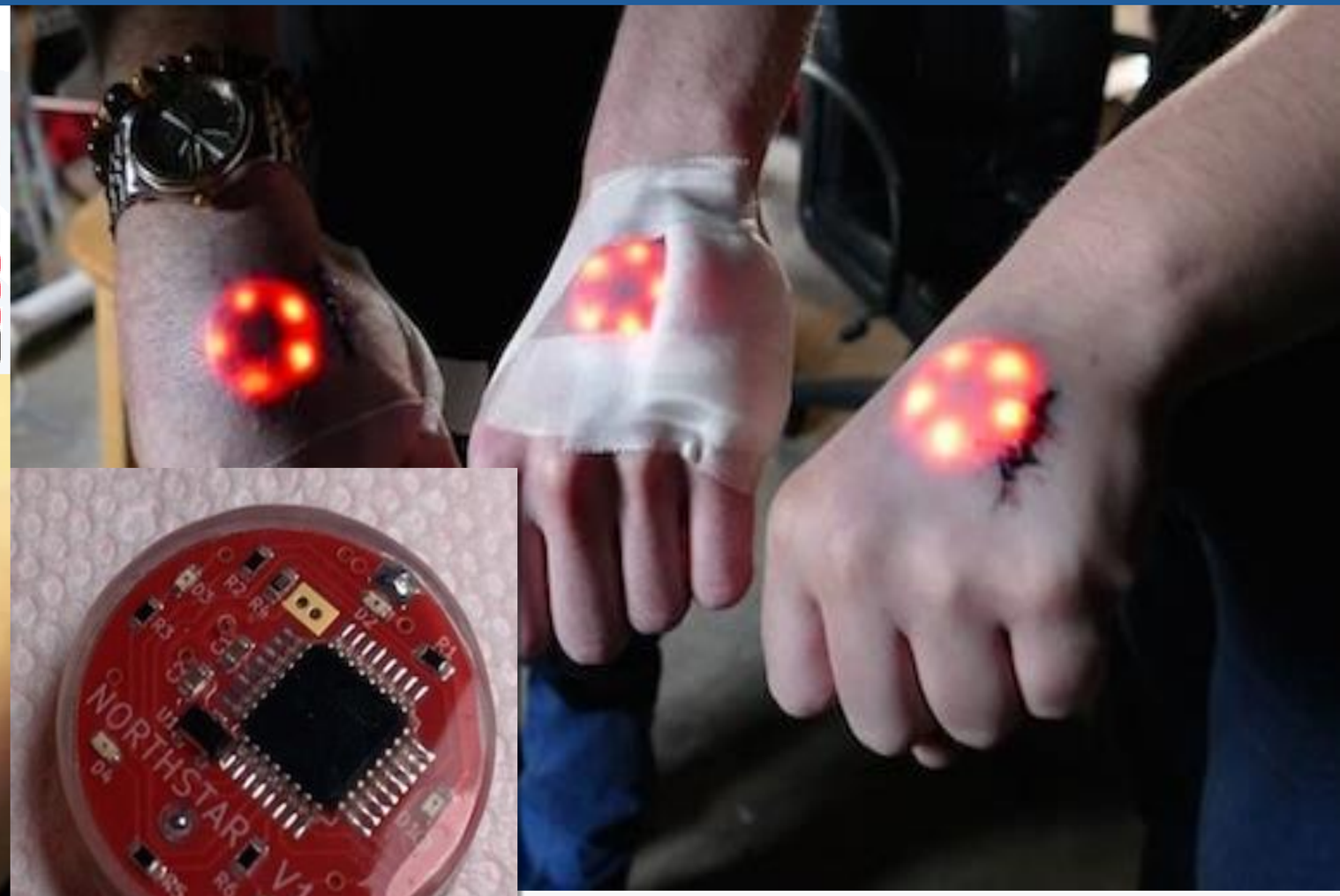


InfoSecWorld
Conference & Expo 2018

DIY “GRINDING”

GRIND HOUSE WETWARE

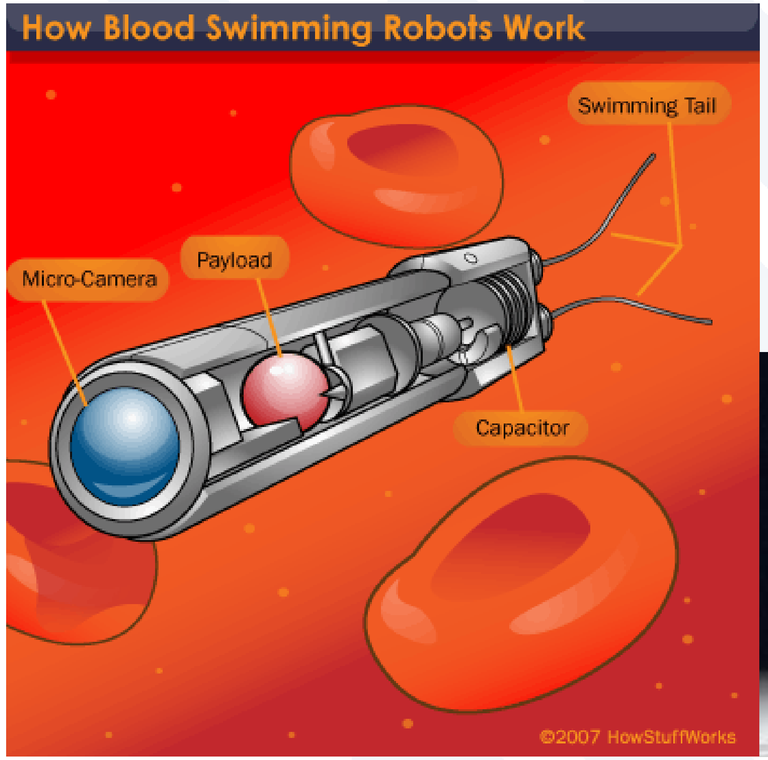
WWW.GRINDHOUSEWETWARE.COM

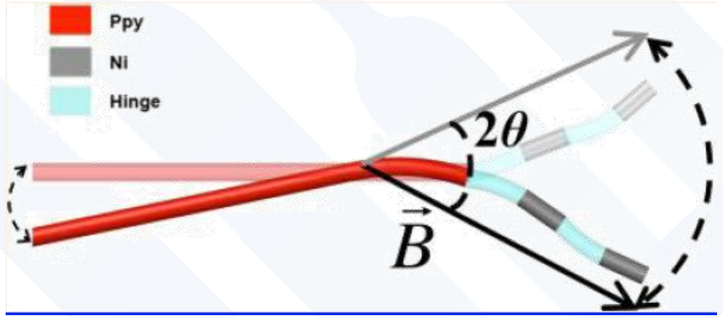


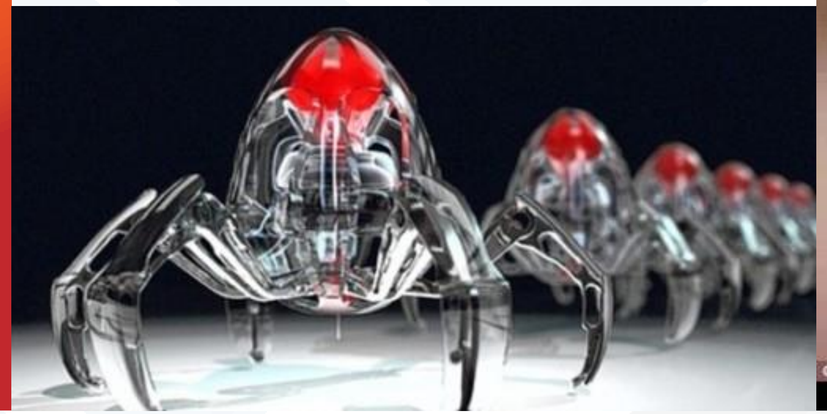
I WANT THIS

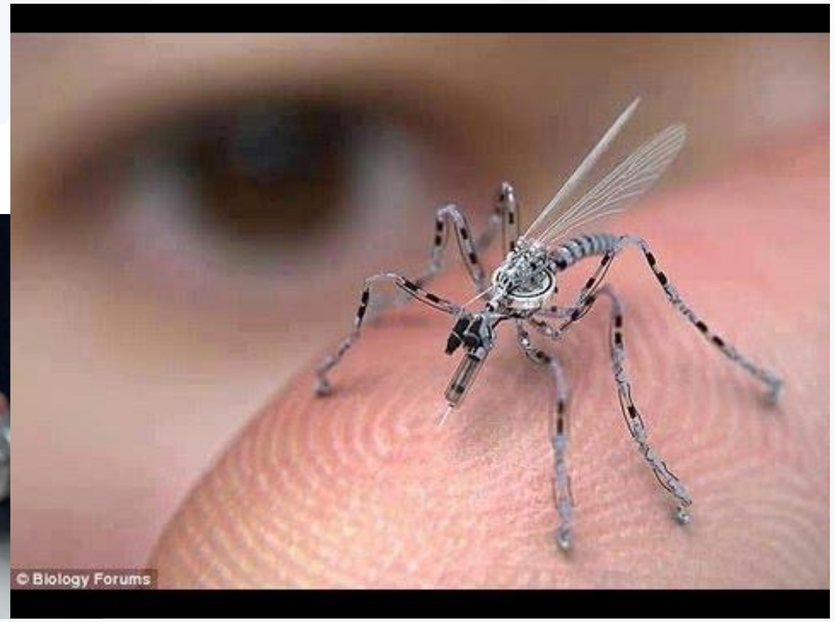
NEURAL LACE

NANOTECHNOLOGY—NANOBOTS









http://electronics.howstuffworks.com/nanorobot.htm

http://www.kurzweilai.net/magnetically-controlled-nanoswimmer-could-deliver-drugs-via-bloodstream

https://futurism.com/pfizer-to-collaborate-with-prof-ido-bachelet/

https://www.youtube.com/watch?v=z78mgfKprdg

Q

?

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Chris Poulin

Director, IoT Security Innovation, Booz Allen Hamilton

@ChrisPoulin