Cyber Security – Where does technology stop and where should we stop it?

Stefan Schmid (Faculty of Computer Science, University of Vienna)

ICISSP 2020 Panel Session

Obviously: We Need Technology

In my field, communication networks, many outages are due to **human errors**, e.g.:

Entire countries disconnected…

Data Centre ▸ Networks

Google routing blunder sent Japan's Internet dark on Friday

Another big BGP blunder

By Richard Chirgwin 27 Aug 2017 at 22:35 40 SHARE ▼

Last Friday, someone in Google fat-thumbed a border gateway protocol (BGP) advertisement and sent Japanese Internet traffic into a black hole.

The trouble began when The Chocolate Factory "leaked" a big route table to Verizon, the result of which was traffic from Japanese giants like NTT and KDDI was sent to Google on the expectation it would be treated as transit.

… 1000s passengers stranded…

British Airways' latest Total Inability To Support Upwardness of Planes* caused by Amadeus system outage

Stuck on the ground awaiting a load sheet? Here's why

By Gareth Corfield 19 Jul 2018 at 11:16 109 SHARE ▼

… even 911 services affected!

Officials: Human error to blame in Minn. 911 outage

According to a press release, CenturyLink told department of public safety that human error by an employee of a third party vendor was to blame for the outage

Aug 16, 2018

Duluth News Tribune

SAINT PAUL, Minn. — The Minnesota Department of Public Safety Emergency Communication Networks division was told by its 911 provider that an Aug. 1 outage was caused by human error.

A major effort is made to make networks more automated, programmable and "**self-driving**".

But: How much can we trust *technology*?

PART OF A ZDNET SPECIAL FEATURE: CYBERWAR AND THE FUTURE OF CYBERSECURITY

Iranian hackers have been hacking VPN servers to plant backdoors in companies around the world

Iranian hackers have targeted Pulse Secure, Fortinet, Palo Alto Networks, and Citrix VPNs to hack into large companies.

By Catalin Cimpanu for Zero Day | February 16, 2020 -- 20:53 GMT (20:53 GMT) | Topic: Cyberwar and the Future of Cybersecurity

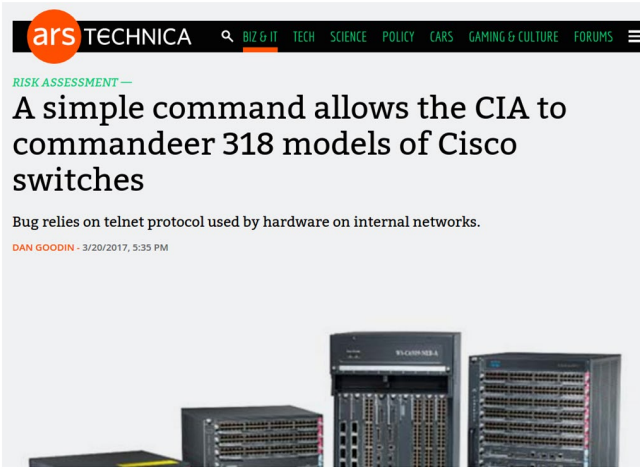
NEWSLETTERS

February 2020: Iranian hackers have targeted Palo Alto Networks and others to hack into large companies.

But: How much can we trust *technology*?

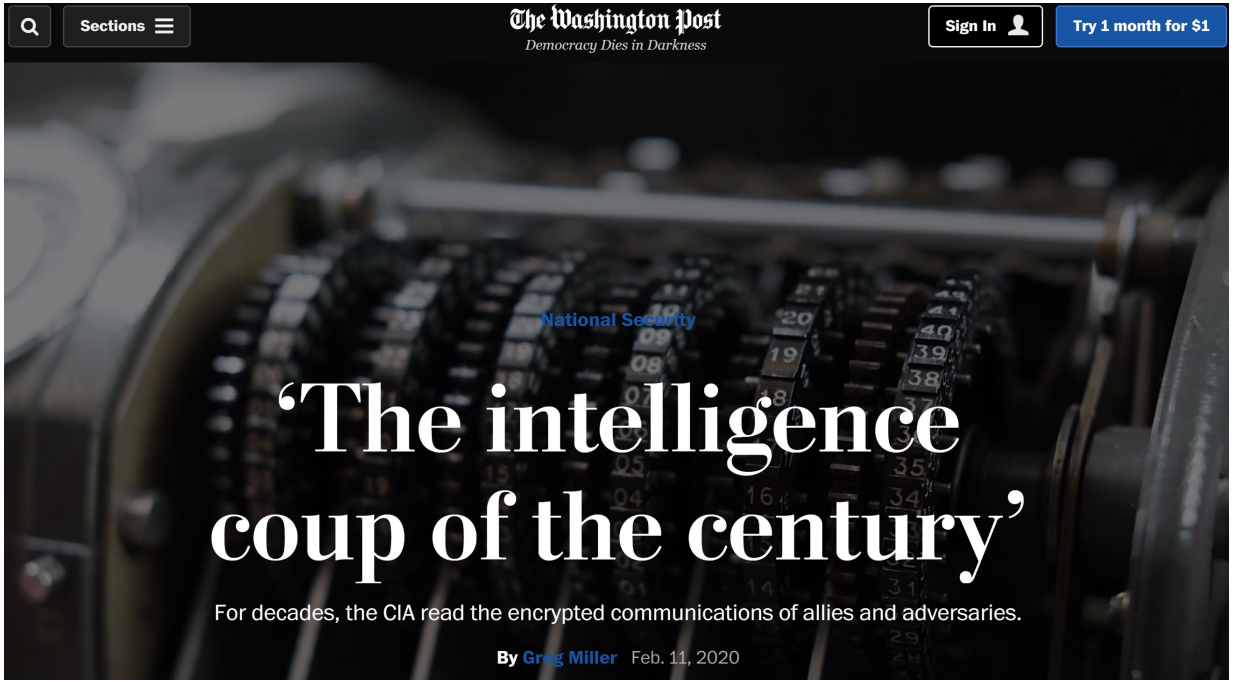
(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon



- **Hardware backdoors** and exploits
- But how can we *build a secure network if the underlying hardware can be insecure*?!

But: How much can we trust *tech companies*?



February 2020: For more than half a century, *governments all over the world* trusted a single company to keep the communications of their spies, soldiers and diplomats secret. But: Crypto AG was *secretly owned by the CIA*.

First Creative Efforts for Self-Protection

The New York Times

Activate This 'Bracelet of Silence,' and Alexa Can't Eavesdrop

Microphones and cameras lurk everywhere. You may want to slip on some privacy armor.

February 2020: Wearable microphone jamming.
(https://www.mirror.co.uk/tech/alexa-owners-can-stop-eavesdropping-21539032)

Another Example: Wearable Camera Jamming

Glasses developed by Scott Urban reflect infrared light from security cameras to blur out the wearer’s face.

Back to Networks…

- Automation and technology is good
- Adoption could be faster: conservative business

- Do we need to stop technology? The wrong question: we cannot anyway.
- And with IoT we already lost anyway.

- But can we at least make sure that technology “with good intensions” does not do more harm, e.g., due to wrong input data, measurements, etc.

- Similar to self-driving cars: can technology recognize its own limits? When inputs from human needed?