1

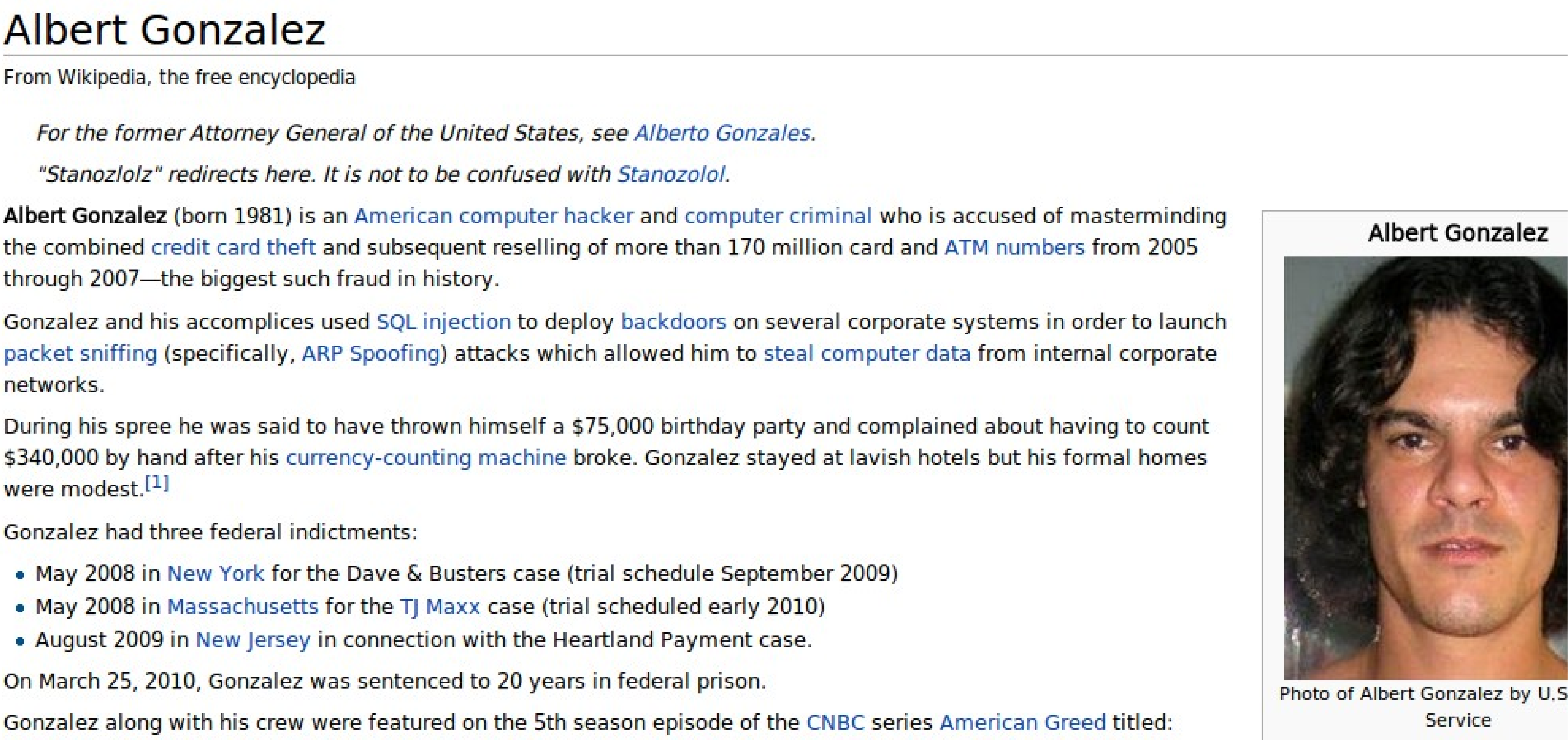
Who is the Attacker ?

Online criminals

Make money
Banking trojans to steal money from bank accounts.
Keyloggers to collect credit card information

Vladimir Tsastsin

Dimitry Golubov



Albert Gonzalez

From Wikipedia, the free encyclopedia

For the former Attorney General of the United States, see Alberto Gonzales.

"Stanozlolz" redirects here. It is not to be confused with Stanozolol.

Albert Gonzalez (born 1981) is an American computer hacker and computer criminal who is accused of masterminding the combined credit card theft and subsequent reselling of more than 170 million card and ATM numbers from 2005 through 2007—the biggest such fraud in history.

Gonzalez and his accomplices used SQL injection to deploy backdoors on several corporate systems in order to launch packet sniffing (specifically, ARP Spoofing) attacks which allowed him to steal computer data from internal corporate networks.

During his spree he was said to have thrown himself a $75,000 birthday party and complained about having to count $340,000 by hand after his currency-counting machine broke. Gonzalez stayed at lavish hotels but his formal homes were modest.[1]

Gonzalez had three federal indictments:

- May 2008 in New York for the Dave & Busters case (trial schedule September 2009)
- May 2008 in Massachusetts for the TJ Maxx case (trial scheduled early 2010)
- August 2009 in New Jersey in connection with the Heartland Payment case.

On March 25, 2010, Gonzalez was sentenced to 20 years in federal prison.

Gonzalez along with his crew were featured on the 5th season episode of the CNBC series American Greed titled:

Albert Gonzalez

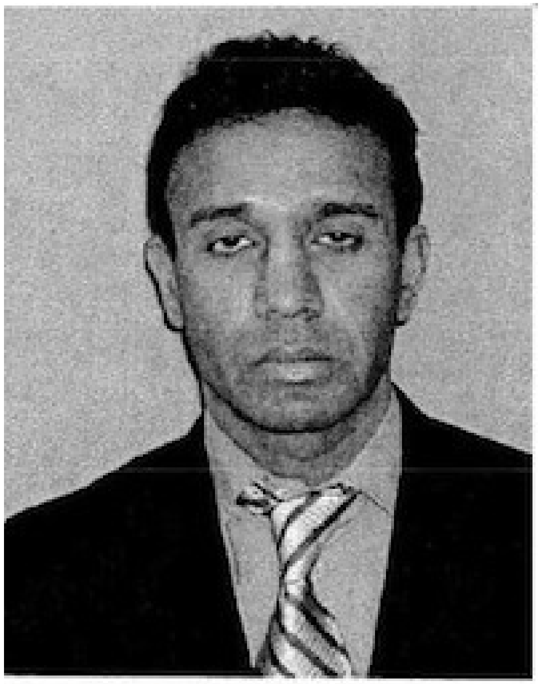
Photo of Albert Gonzalez by U.S
Service

Albert Gonzalez
American Computer Criminal

Sam Jain

US Secret Service found Swiss bank account of Mr. Sam Jain and that bank account had 14.9 million U.S. dollars on it when it was frozen.

Mr. Jain himself is on the loose; nobody knows where he is.

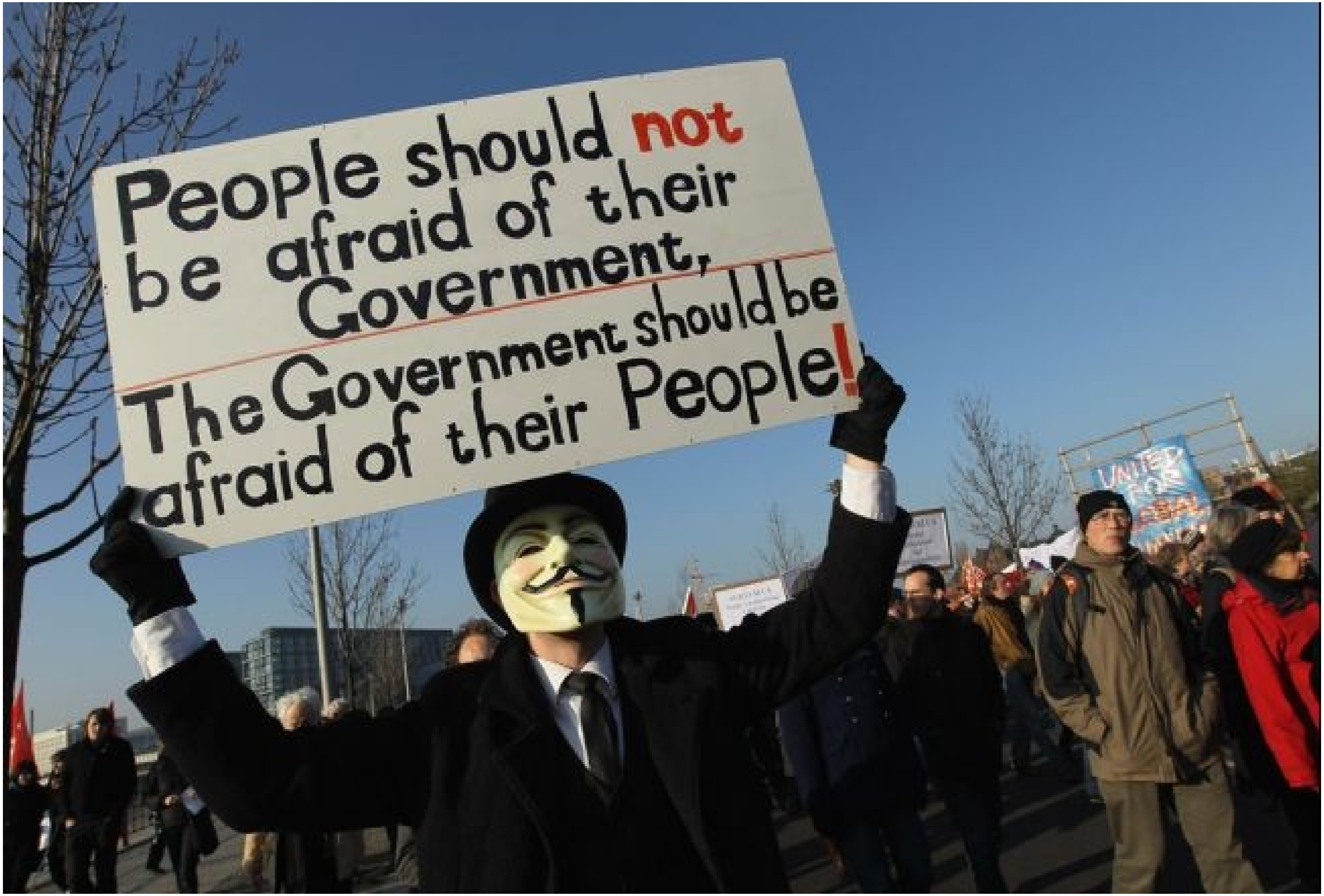


2009/13445 JAIN SHAILESHKUMAR

Motivated by an opinion

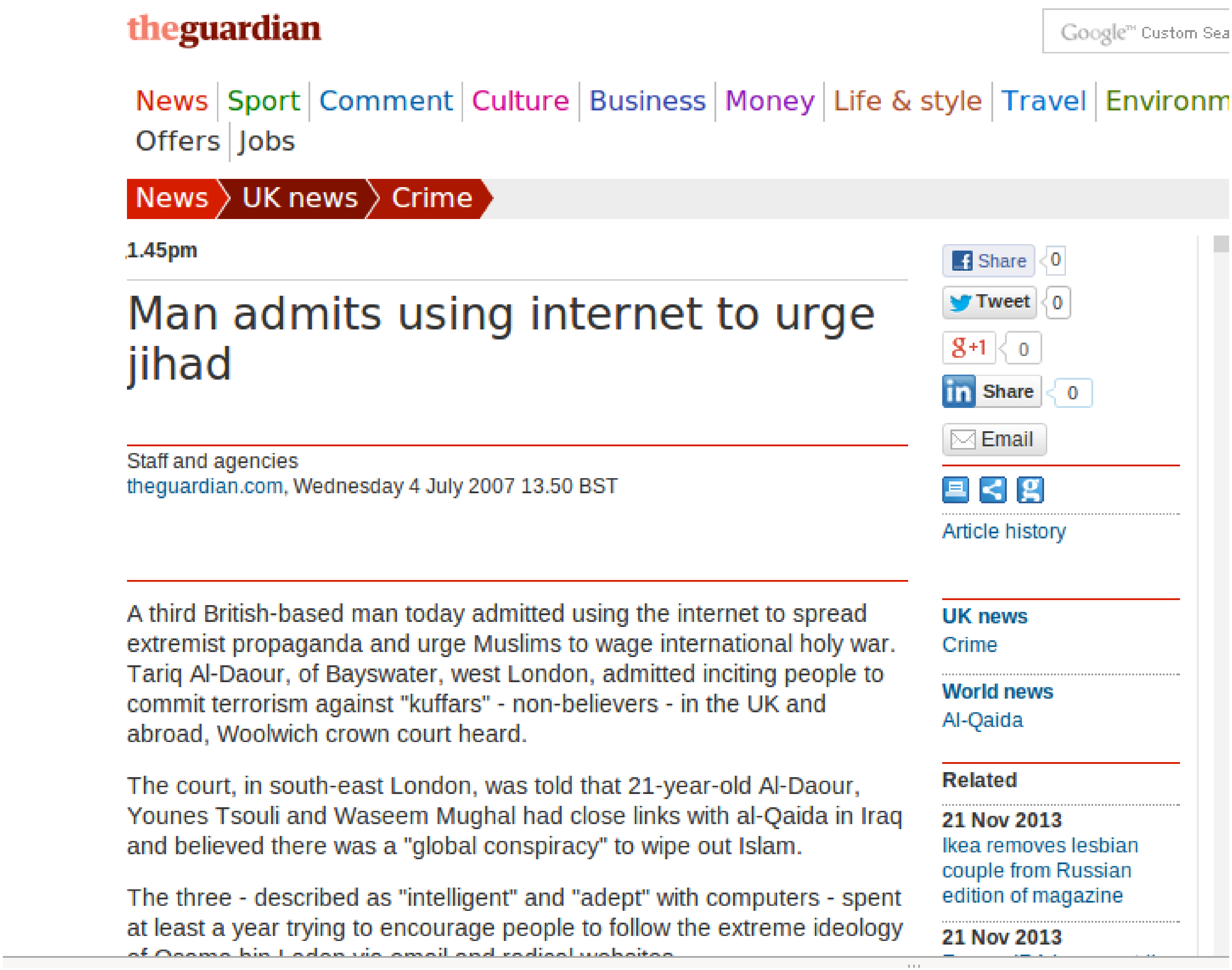
Not motivated by money
They're motivated by protests, motivated by an opinion.

Anonymous Group


People should not be afraid of their Government,
The Government should be afraid of their People!
UNITED FOR GLOBAL

Anonymous Group

Al-Qaeda



1.45pm

Man admits using internet to urge jihad

Staff and agencies
theguardian.com, Wednesday 4 July 2007 13.50 BST

A third British-based man today admitted using the internet to spread extremist propaganda and urge Muslims to wage international holy war. Tariq Al-Daour, of Bayswater, west London, admitted inciting people to commit terrorism against "kuffars" - non-believers - in the UK and abroad, Woolwich crown court heard.

The court, in south-east London, was told that 21-year-old Al-Daour, Younes Tsouli and Waseem Mughal had close links with al-Qaida in Iraq and believed there was a "global conspiracy" to wipe out Islam.

The three - described as "intelligent" and "adept" with computers - spent at least a year trying to encourage people to follow the extreme ideology of Osama bin Laden via email and radical websites.

UK news
Crime

World news
Al-Qaida

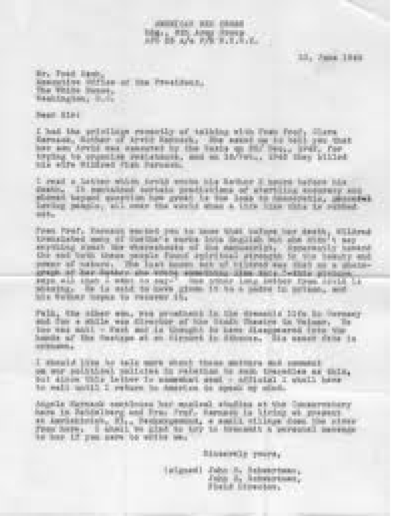
Related

21 Nov 2013
Ikea removes lesbian couple from Russian edition of magazine

21 Nov 2013

1. Online criminals Motivated by Money
2. People Motivated by an opinion

1. Online criminals Motivated by Money
2. People Motivated by an opinion
3. The Government



AMERICAN RED CROSS
[illegible]
[illegible]

10, June 1946

Mr. [illegible],
Executive Office of the President,
The White House,
Washington, D.C.

Dear Sir:

I had the privilege recently of talking with Frau Prof. Clara Harnack, mother of Arvid Harnack. She asked me to tell you that her son Arvid was executed by the Nazis on 22/ Dec., 1942, for trying to organize resistance, and on 16/Feb., 1943 they killed his wife Mildred Fish Harnack.

I read a letter which Arvid wrote his mother 2 hours before his death. It contained certain predictions of startling accuracy and showed beyond question how great is the loss to humanity, [illegible] loving people, all over the world when a life like this is rubbed out.

Frau Prof. Harnack wanted you to know that before her death, Mildred translated many of Goethe's works into English but she didn't say anything about the whereabouts of the manuscripts. Apparently toward the end both these people found spiritual strength in the beauty and power of nature. The last known act of Mildred was that on a photograph of her mother she wrote something like this-"this picture says all that I want to say." One other long letter from Arvid is missing. He is said to have given it to a padre in prison, and his mother hopes to recover it.

Falk, the other son, was prominent in the dramatic life in Germany and for a while was director of the State Theatre in Weimar. He too was anti - Nazi and is thought to have disappeared into the hands of the Gestapo at an airport in Athens. His exact fate is unknown.

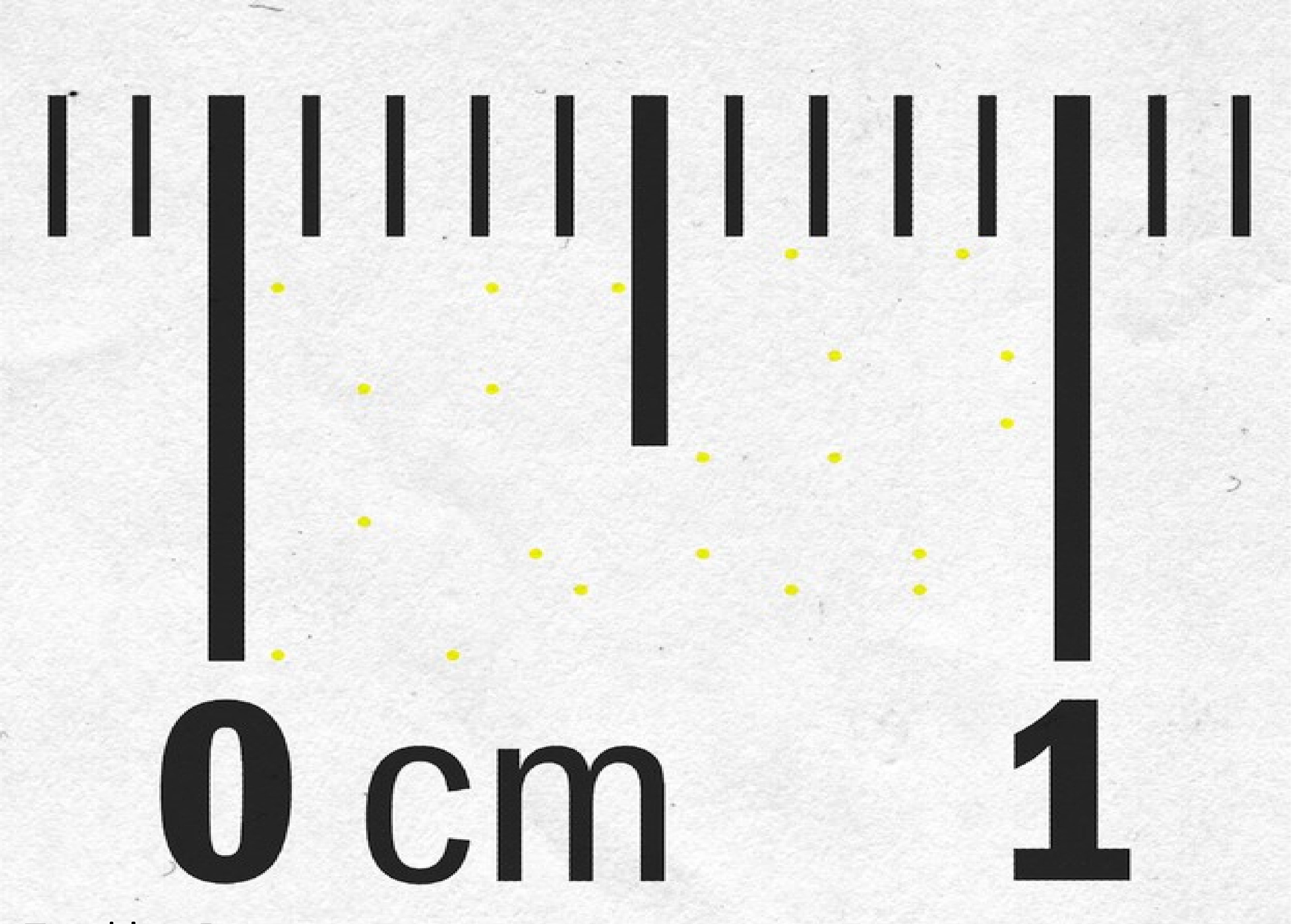
I should like to talk more about these matters and comment on our political policies in relation to such tragedies as this, but since this letter is somewhat semi - official I shall have to wait until I return to America to speak my mind.

Angela Harnack continues her musical studies at the Conservatory here in Heidelberg and Frau Prof. Harnack is living at present at [illegible], a small village down the river from here. I shall be glad to try to transmit a personal message to her if you care to write me.

Sincerely yours,

(signed) John O. [illegible],
John O. [illegible],
Field Director.

East German Typewriter



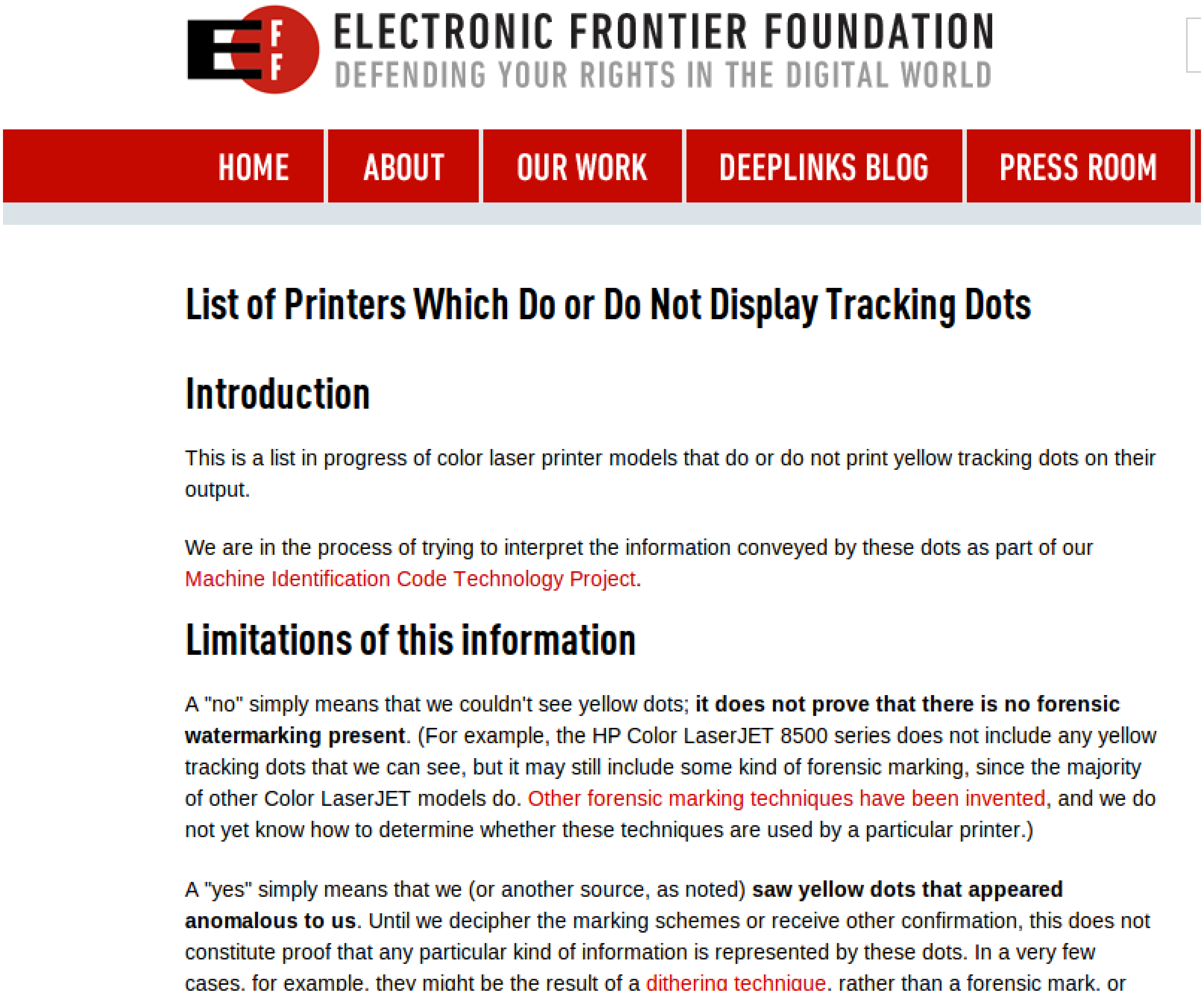
Tracking Dots

Printer steganography

Brother, Canon, Dell, Epson, HP, IBM, Konica Minolta, Kyocera, Lanier, Lexmark, Ricoh, Toshiba and Xerox brand color laser printers,

Tiny yellow dots are added to each page.

The dots are barely visible and contain encoded printer serial numbers and timestamps.



ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD
HOME
ABOUT
OUR WORK
DEEPLINKS BLOG
PRESS ROOM

List of Printers Which Do or Do Not Display Tracking Dots

Introduction

This is a list in progress of color laser printer models that do or do not print yellow tracking dots on their output.

We are in the process of trying to interpret the information conveyed by these dots as part of our Machine Identification Code Technology Project.

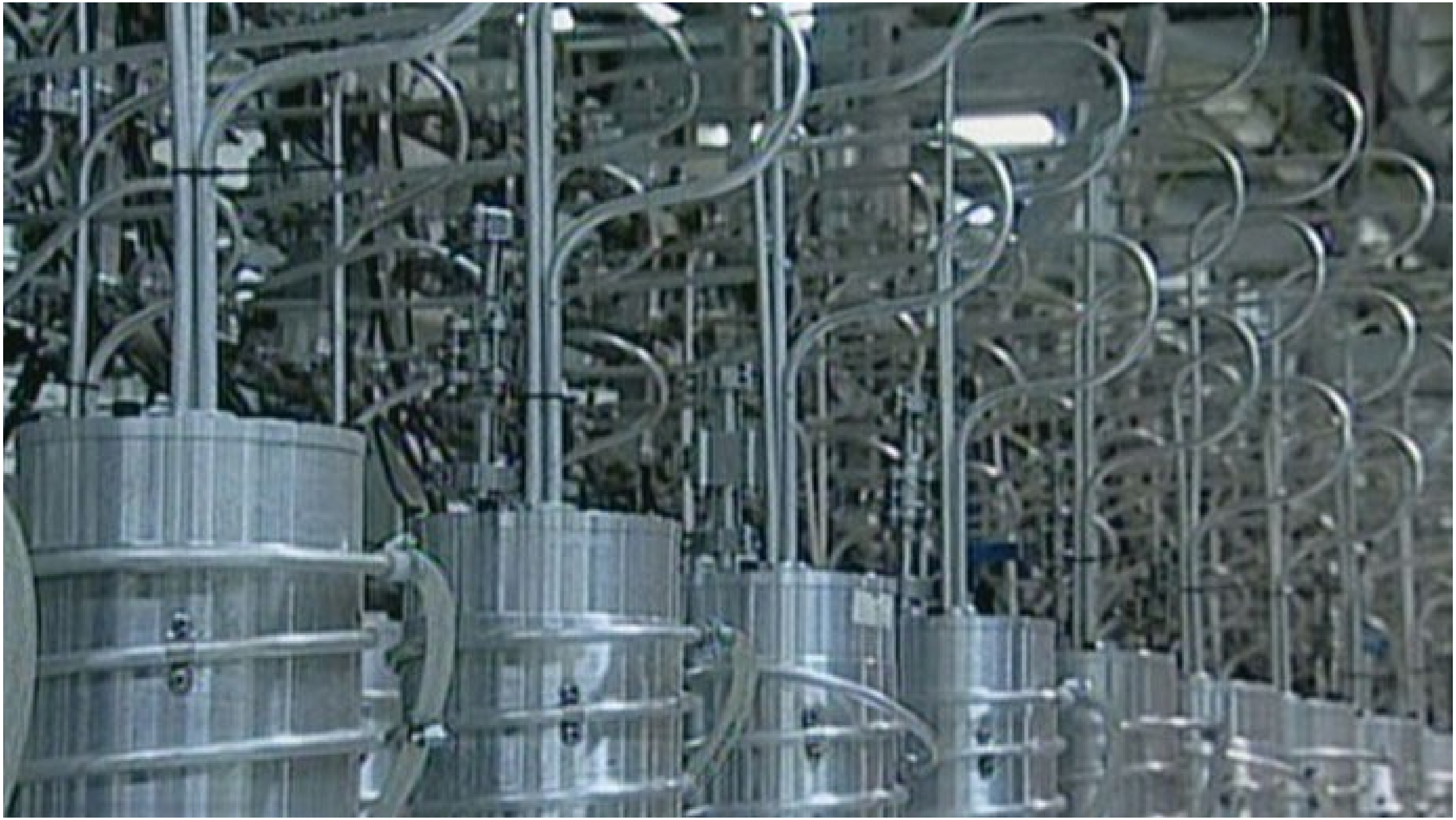
Limitations of this information

A "no" simply means that we couldn't see yellow dots; **it does not prove that there is no forensic watermarking present**. (For example, the HP Color LaserJET 8500 series does not include any yellow tracking dots that we can see, but it may still include some kind of forensic marking, since the majority of other Color LaserJET models do. Other forensic marking techniques have been invented, and we do not yet know how to determine whether these techniques are used by a particular printer.)

A "yes" simply means that we (or another source, as noted) **saw yellow dots that appeared anomalous to us**. Until we decipher the marking schemes or receive other confirmation, this does not constitute proof that any particular kind of information is represented by these dots. In a very few cases, for example, they might be the result of a dithering technique, rather than a forensic mark, or

2

Cyber Warfare



IR Centrifuges

SIMATIC S7-315

SIMATIC S7-417

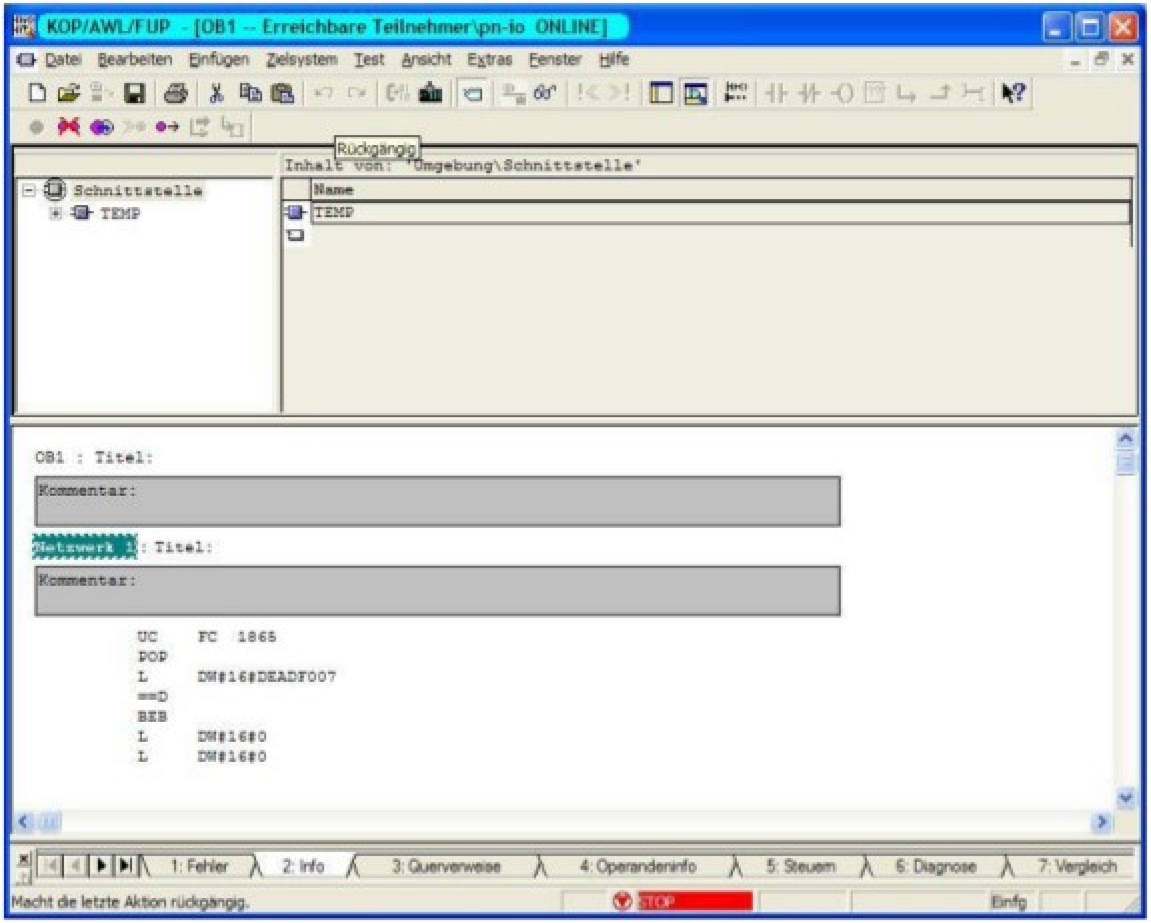
Microsoft® Windows®

SIEMENS

SIMATIC STEP 7: the comprehensive engineering system

Even the basic version of SIMATIC STEP 7 gives you easy access to the full potential of Siemens' controllers. STEP 7 Professional opens even more possibilities thanks to a wide selection of program editors, while the Basic version provides a shared platform for programming S7-1200 controllers and SIMATIC HMI basic panels

SIMATIC STEP 7 Running on Windows


KOP/AWL/FUP - [OB1 -- Erreichbare Teilnehmer\pn-io ONLINE]
Datei Bearbeiten Einfügen Zielsystem Test Ansicht Extras Fenster Hilfe
Rückgängig
Inhalt von: 'Umgebung\Schnittstelle'
Schnittstelle
TEMP
Name
TEMP
1: Fehler 2: Info 3: Querverweise 4: Operandeninfo 5: Steuern 6: Diagnose 7: Vergleich
Macht die letzte Aktion rückgängig.
STOP
Einfg

```
OB1 : Titel:
Kommentar:
Netzwerk 1 : Titel:
Kommentar:
          UC     FC  1865
          POP
          L      DW#16#DEADF007
          ==D
          BEB
          L      DW#16#0
          L      DW#16#0
```

SIMATIC STEP 7

PLC

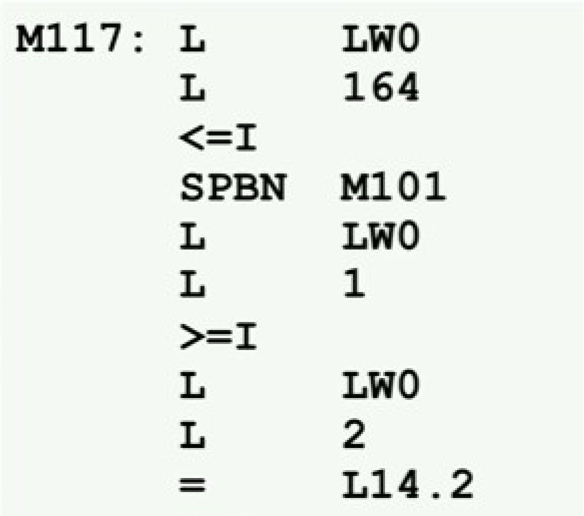
IR Centrifuges

Langner

To Kill a Centrifuge

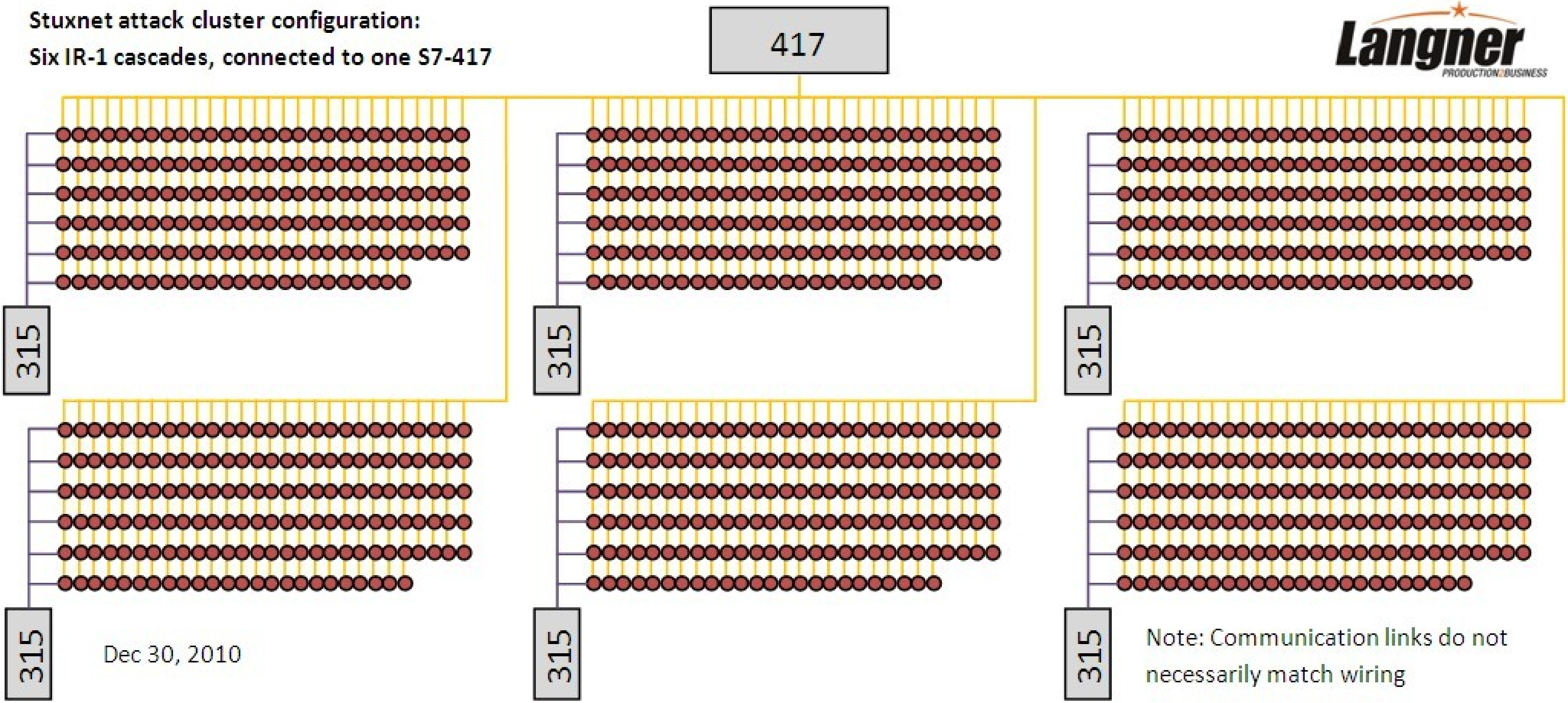
A Technical Analysis of
What Stuxnet's Creators
Tried to Achieve

20 November 2013



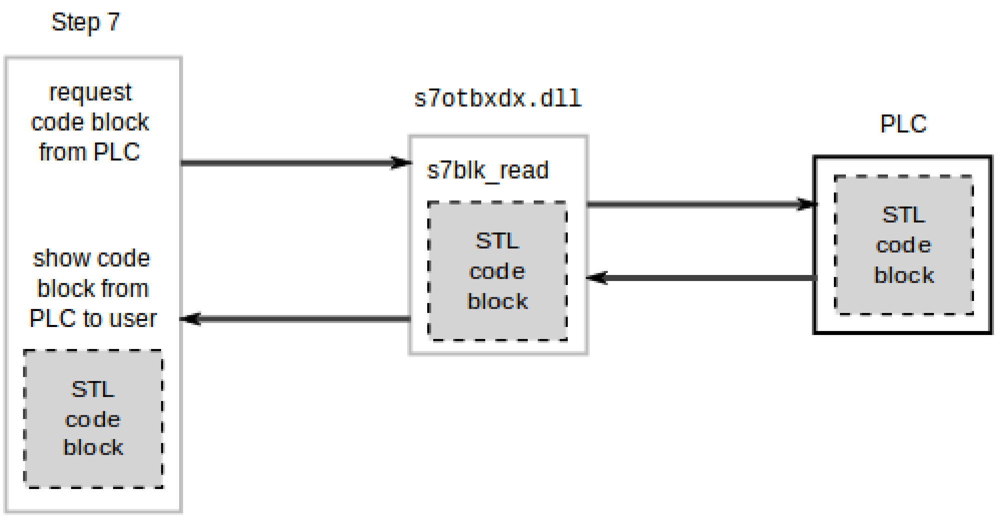
```
M117: L     LW0
      L     164
      <=I
      SPBN  M101
      L     LW0
      L     1
      >=I
      L     LW0
      L     2
      =     L14.2
```

Stuxnet attack cluster configuration:
Six IR-1 cascades, connected to one S7-417



Note: Communication links do not necessarily match wiring

Dec 30, 2010



Step 7

request code block from PLC

show code block from PLC to user

STL code block

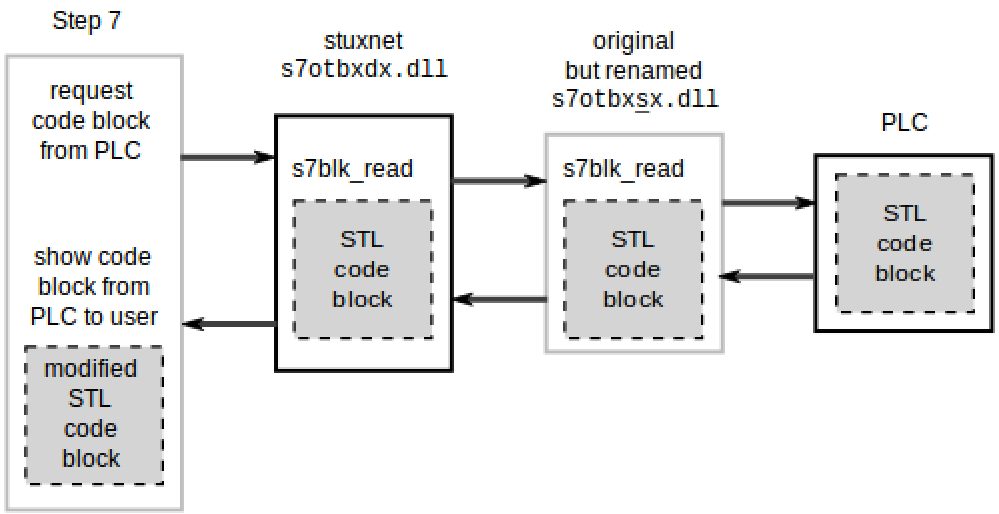
`s7otbxdx.dll`

s7blk_read

STL code block

PLC

STL code block



Step 7

request code block from PLC

show code block from PLC to user

modified STL code block

stuxnet `s7otbxdx.dll`

s7blk_read

STL code block

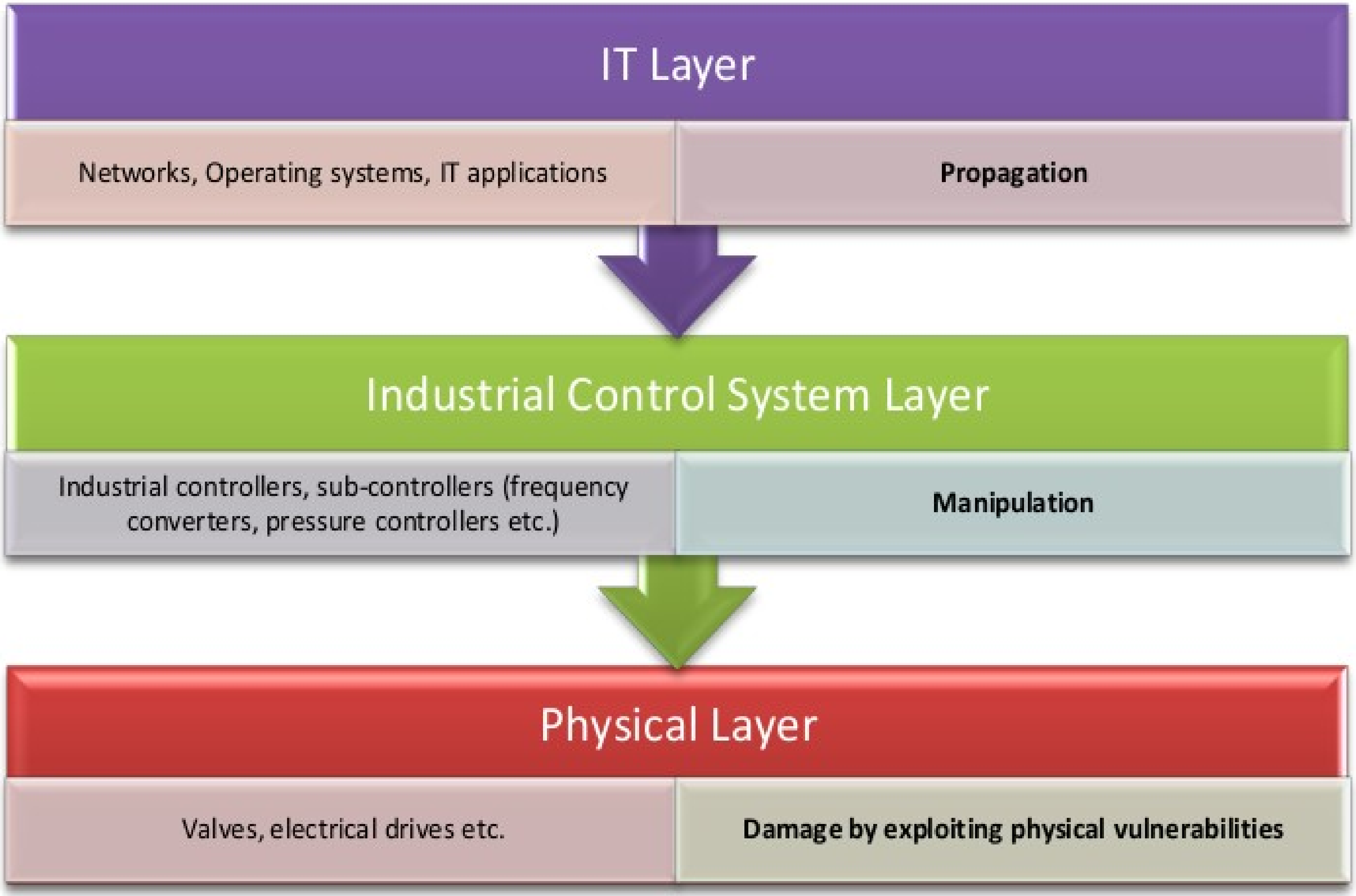
original but renamed `s7otbxsx.dll`

s7blk_read

STL code block

PLC

STL code block



IT Layer

Networks, Operating systems, IT applications

Propagation

Industrial Control System Layer

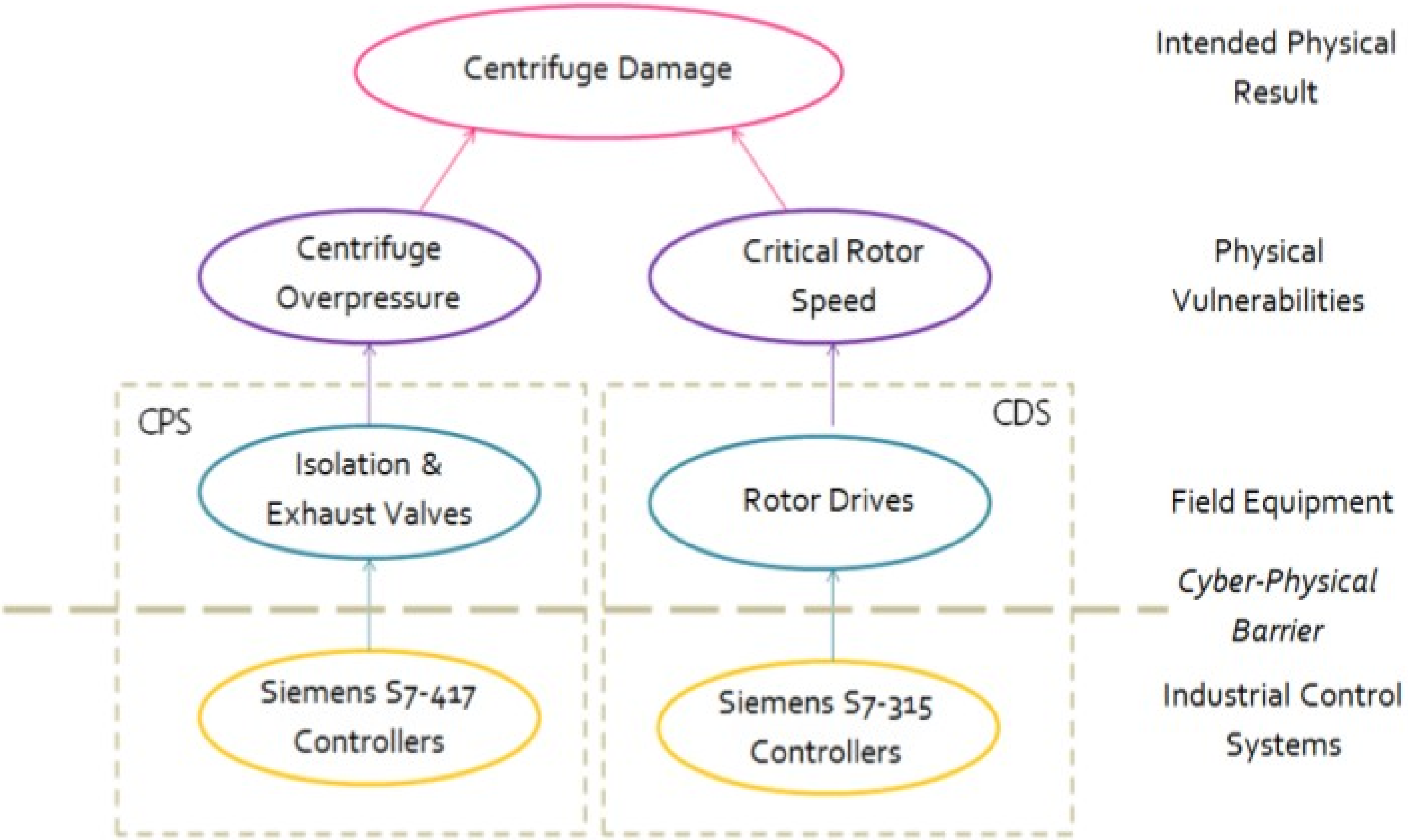
Industrial controllers, sub-controllers (frequency converters, pressure controllers etc.)

Manipulation

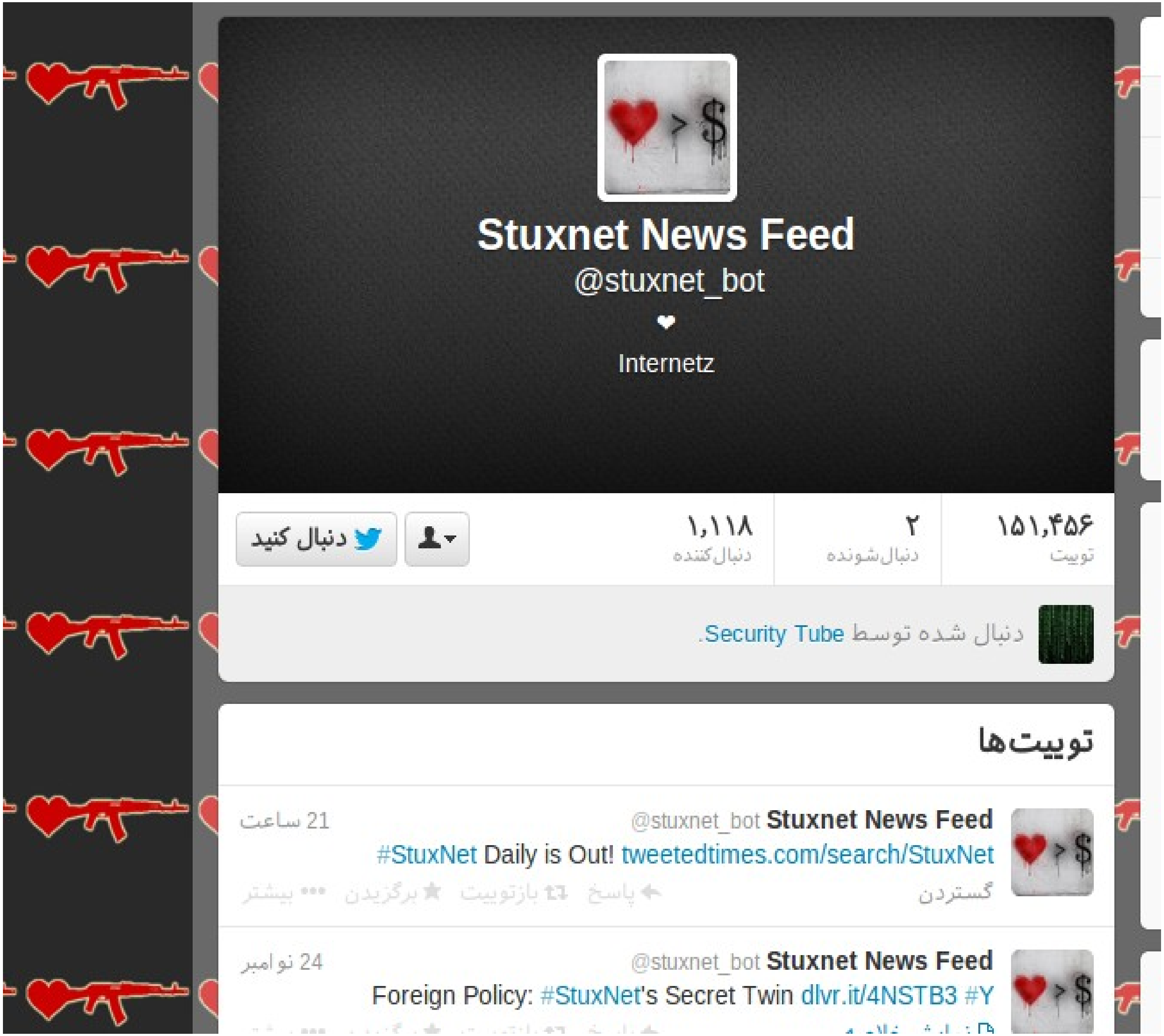
Physical Layer

Valves, electrical drives etc.

Damage by exploiting physical vulnerabilities


Centrifuge Damage
Intended Physical Result
Centrifuge Overpressure
Critical Rotor Speed
Physical Vulnerabilities
CPS
CDS
Isolation & Exhaust Valves
Rotor Drives
Field Equipment
Cyber-Physical Barrier
Siemens S7-417 Controllers
Siemens S7-315 Controllers
Industrial Control Systems

Power generation and distribution
Chemical industry and petrochemicals
Oil, Gas
Refineries
Pharmaceuticals
Airport automation
Waterworks and water treatment plants
Transport technology
Traffic flow automation
Shipbuilding
Turbine development



Stuxnet News Feed

@stuxnet_bot

❤

Internetz

۱۵۱,۴۵۶	۲	۱,۱۱۸
توییت	دنبال‌شونده	دنبال‌کننده

دنبال شده توسط Security Tube.

Stuxnet News Feed @stuxnet_bot 21 ساعت

#StuxNet Daily is Out! tweetedtimes.com/search/StuxNet

Stuxnet News Feed @stuxnet_bot 24 نوامبر

Foreign Policy: #StuxNet's Secret Twin dlvr.it/4NSTB3 #Y

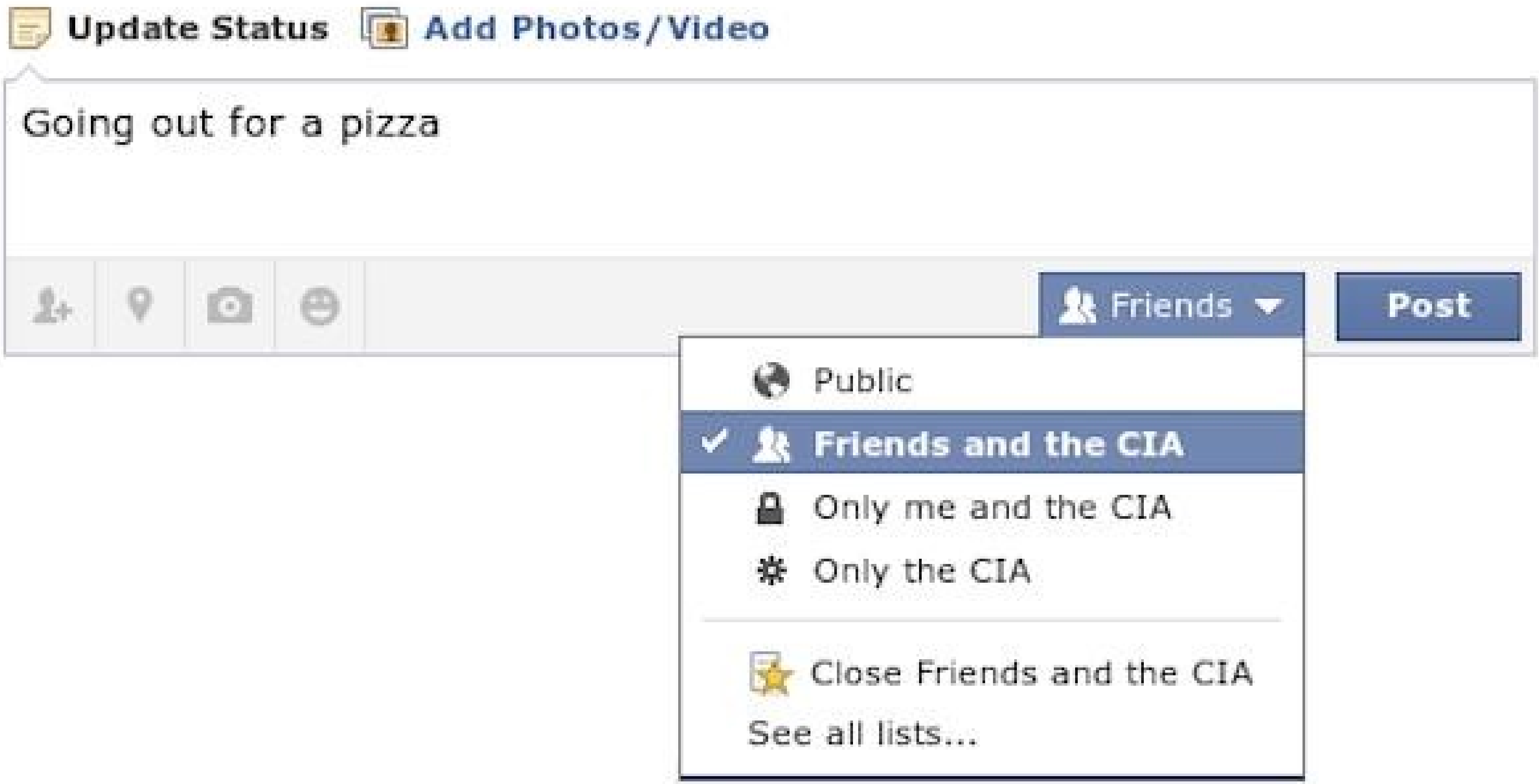
3

Online Privacy

NATIONAL SECURITY AGENCY

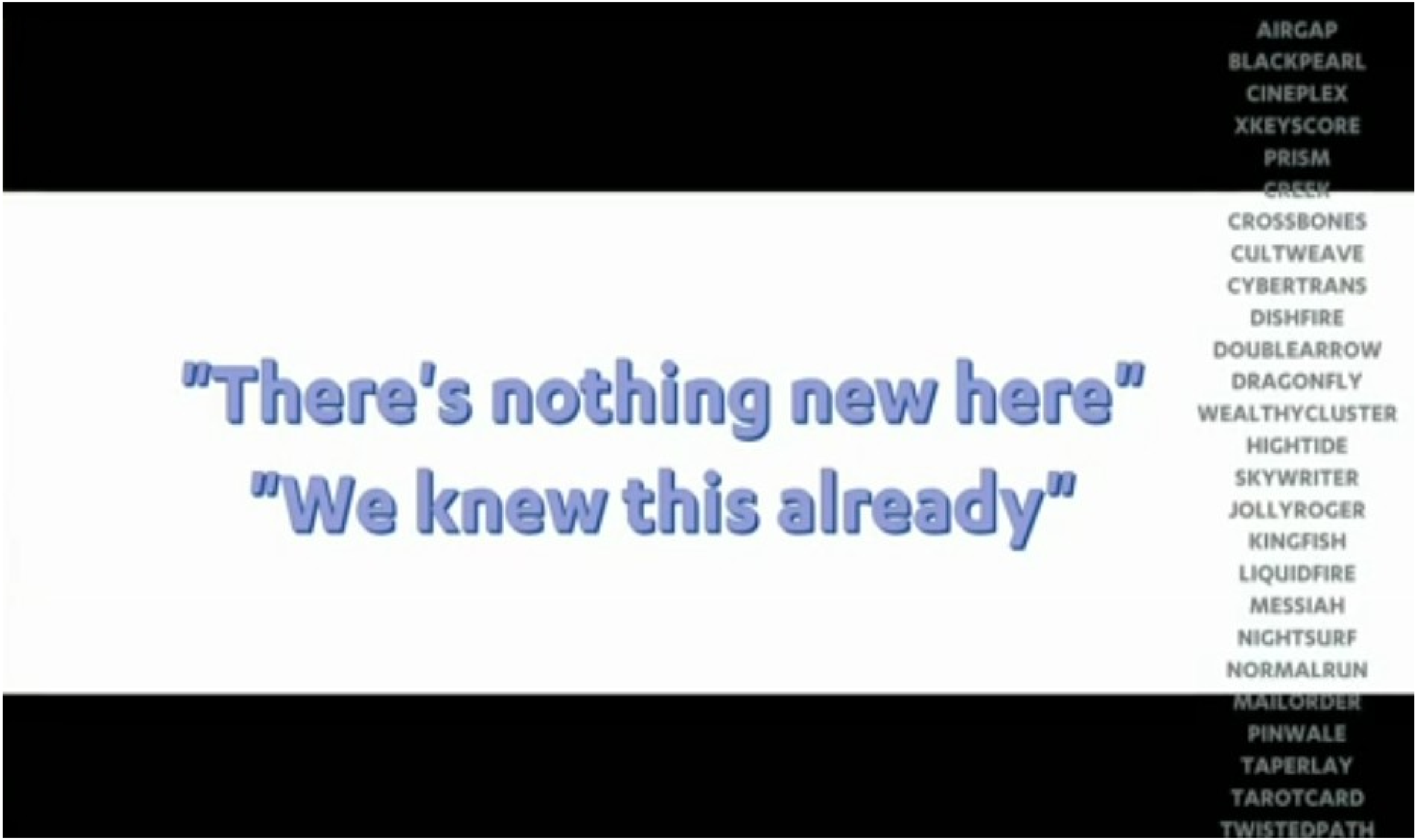
UNITED STATES OF AMERICA

PRISM



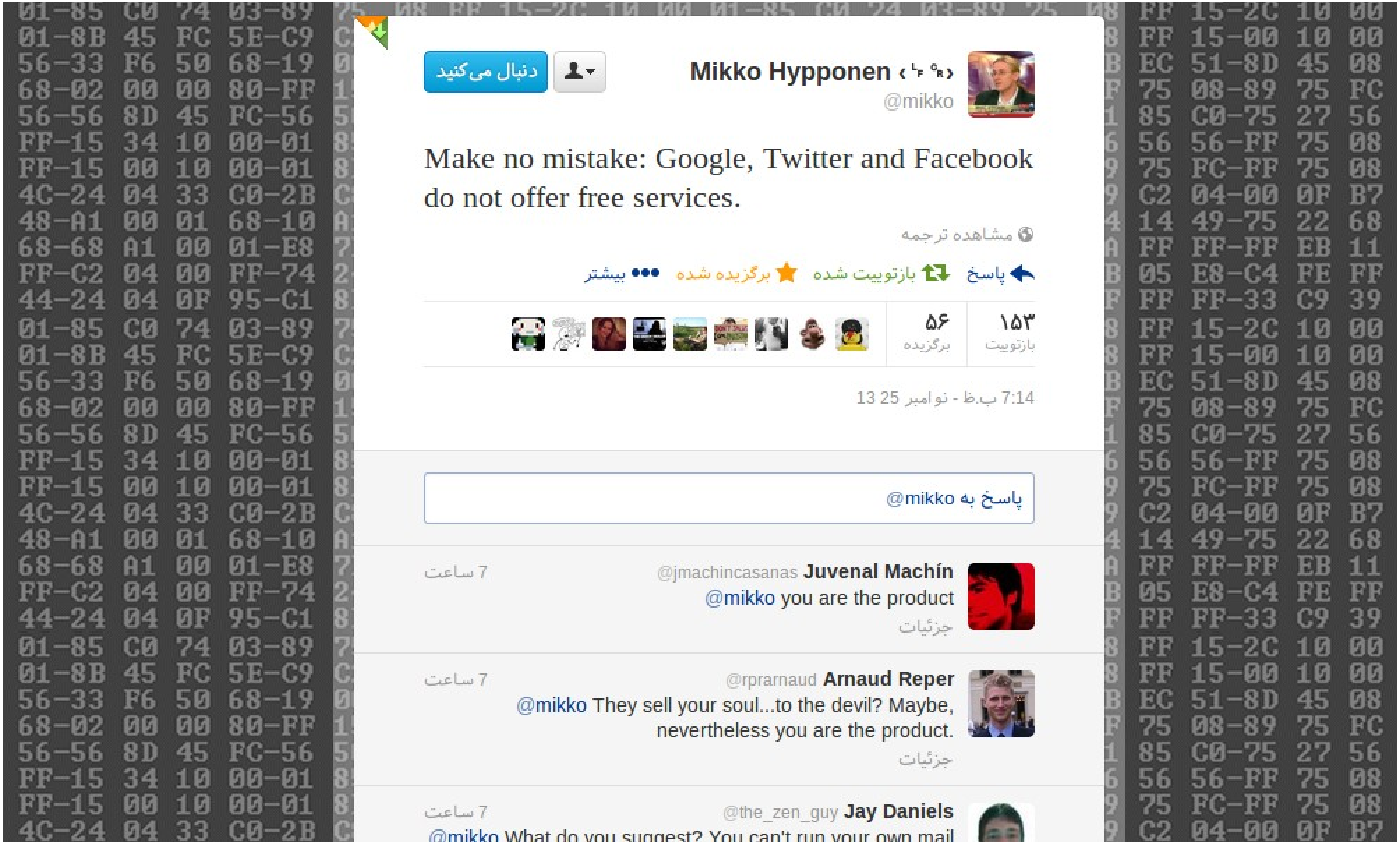
Going out for a pizza

THOSE WHO SACRIFICE FREEDOM 4 SECURITY DESERVE NEITHER
1984 IS NOW
Die NSA wusste schon vorher, was für ein Schild ich malen würde
You are the first Afro PRESIDENT need to also for the SYSTEM?
Ich w Was mach
YES WE SCAN
YES WE SCAN
TRANSPARENTER STAAT STATT GLÄSERNER BÜRGER!
change.org/prism



"There's nothing new here"
"We knew this already"

AIRGAP
BLACKPEARL
CINEPLEX
XKEYSCORE
PRISM
GREEN
CROSSBONES
CULTWEAVE
CYBERTRANS
DISHFIRE
DOUBLEARROW
DRAGONFLY
WEALTHYCLUSTER
HIGHTIDE
SKYWRITER
JOLLYROGER
KINGFISH
LIQUIDFIRE
MESSIAH
NIGHTSURF
NORMALRUN
MAILORDER
PINWALE
TAPERLAY
TAROTCARD
TWISTEDPATH



Mikko Hypponen ‹␊␍›
@mikko

Make no mistake: Google, Twitter and Facebook do not offer free services.

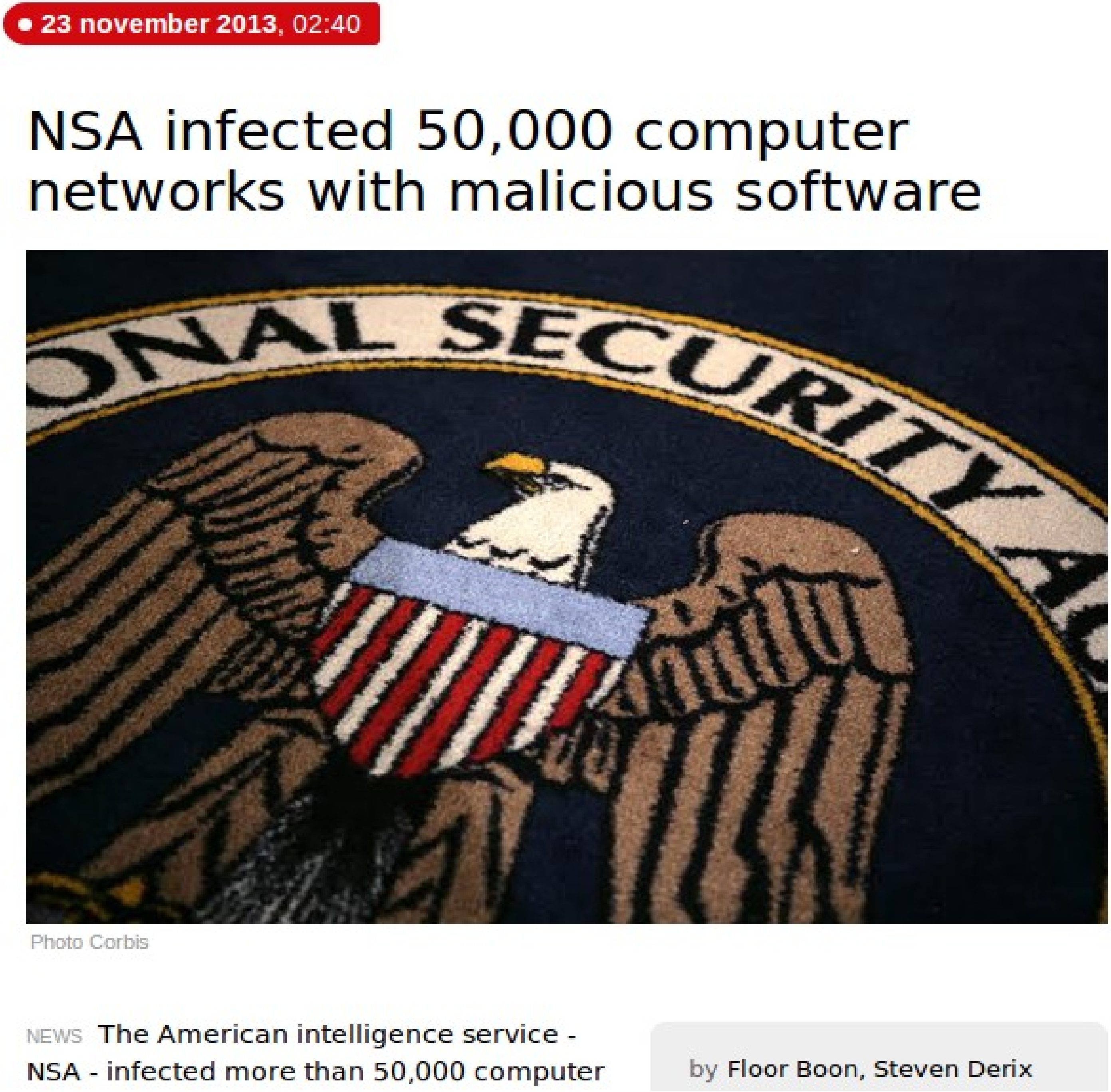
۱۵۳ بازتوییت
۵۶ برگزیده

7:14 ب.ظ - نوامبر 25 13

Juvenal Machín @jmachincasanas 7 ساعت
@mikko you are the product

Arnaud Reper @rprarnaud 7 ساعت
@mikko They sell your soul...to the devil? Maybe, nevertheless you are the product.

Jay Daniels @the_zen_guy 7 ساعت
@mikko What do you suggest? You can't run your own mail



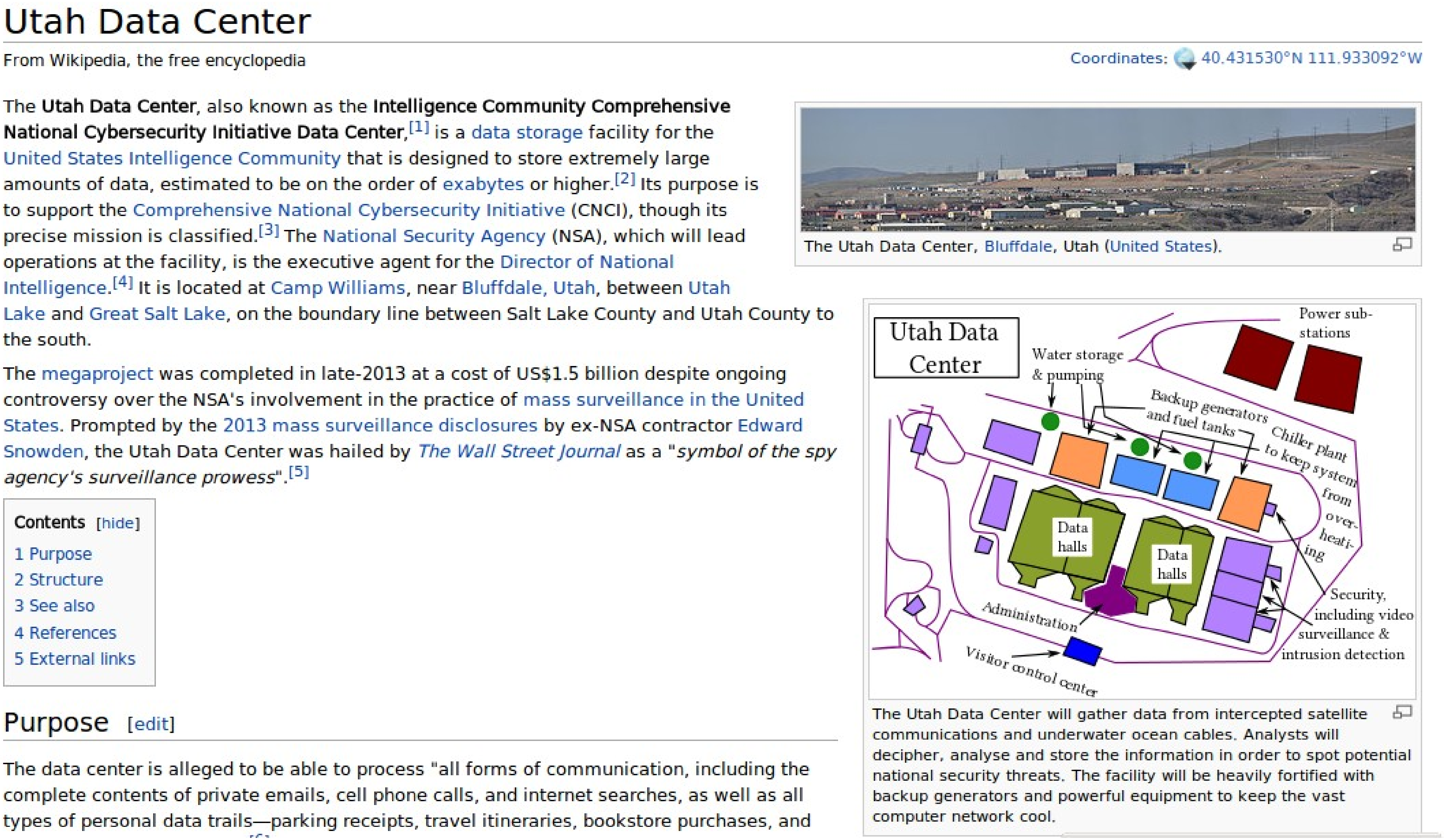
● 23 november 2013, 02:40

NSA infected 50,000 computer networks with malicious software

Photo Corbis

NEWS The American intelligence service - NSA - infected more than 50,000 computer

by Floor Boon, Steven Derix



Utah Data Center

From Wikipedia, the free encyclopedia

Coordinates: 40.431530°N 111.933092°W

The **Utah Data Center**, also known as the **Intelligence Community Comprehensive National Cybersecurity Initiative Data Center**,[1] is a data storage facility for the United States Intelligence Community that is designed to store extremely large amounts of data, estimated to be on the order of exabytes or higher.[2] Its purpose is to support the Comprehensive National Cybersecurity Initiative (CNCI), though its precise mission is classified.[3] The National Security Agency (NSA), which will lead operations at the facility, is the executive agent for the Director of National Intelligence.[4] It is located at Camp Williams, near Bluffdale, Utah, between Utah Lake and Great Salt Lake, on the boundary line between Salt Lake County and Utah County to the south.

The Utah Data Center, Bluffdale, Utah (United States).

Utah Data Center
Power sub-stations
Water storage & pumping
Backup generators and fuel tanks
Chiller plant to keep system from over-heating
Data halls
Data halls
Administration
Security, including video surveillance & intrusion detection
Visitor control center

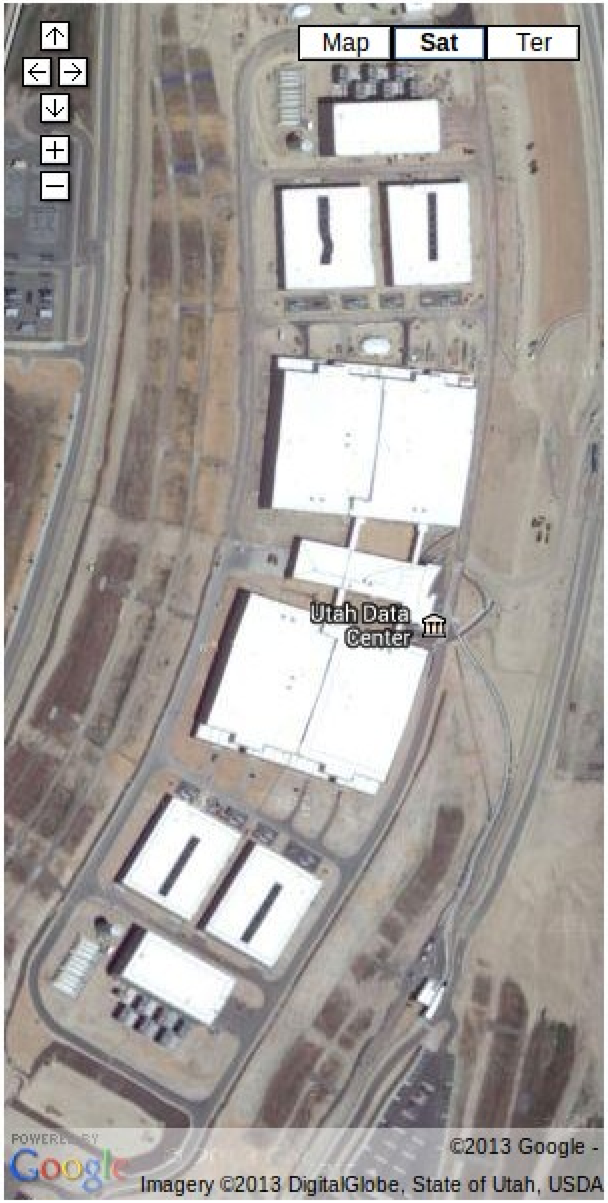
The Utah Data Center will gather data from intercepted satellite communications and underwater ocean cables. Analysts will decipher, analyse and store the information in order to spot potential national security threats. The facility will be heavily fortified with backup generators and powerful equipment to keep the vast computer network cool.

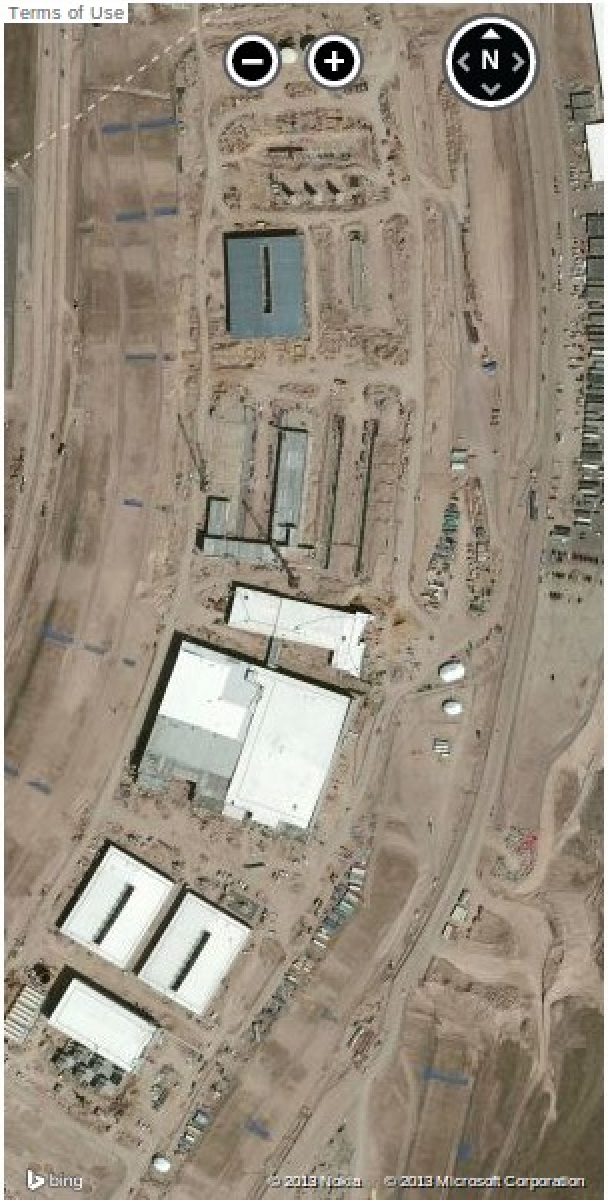
The megaproject was completed in late-2013 at a cost of US$1.5 billion despite ongoing controversy over the NSA's involvement in the practice of mass surveillance in the United States. Prompted by the 2013 mass surveillance disclosures by ex-NSA contractor Edward Snowden, the Utah Data Center was hailed by *The Wall Street Journal* as a "*symbol of the spy agency's surveillance prowess*".[5]

Contents [hide]

Purpose [edit]

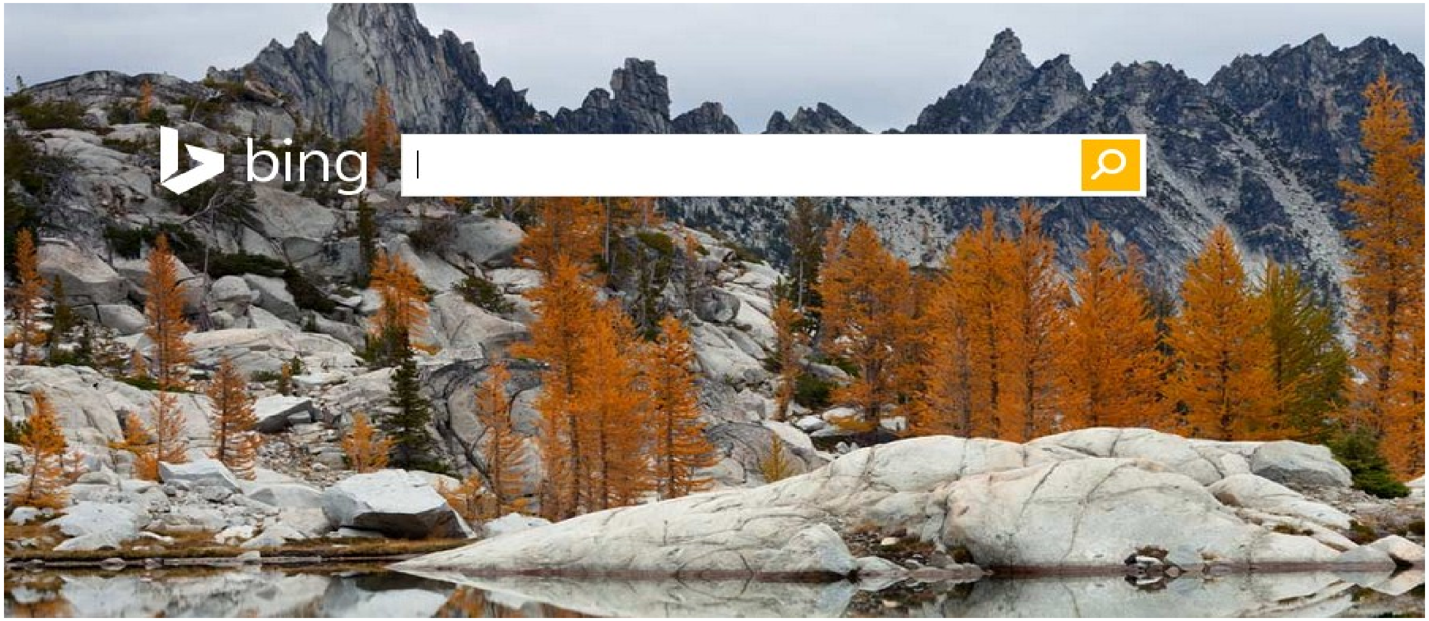
The data center is alleged to be able to process "all forms of communication, including the complete contents of private emails, cell phone calls, and internet searches, as well as all types of personal data trails—parking receipts, travel itineraries, bookstore purchases, and


Map
Sat
Ter
Utah Data Center
POWERED BY Google
©2013 Google -
Imagery ©2013 DigitalGlobe, State of Utah, USDA


Terms of Use
N
bing
© 2013 Nokia
© 2013 Microsoft Corporation

“If there is no right to privacy, there can be no true freedom of expression and opinion, and therefore, there can be no effective democracy.”
Dilma Rousseff – Brazilian President Speech at UNGA

Google
Google Search
I'm Feeling Lucky


bing

Open Source

By building together open, free, secure systems, we can go around such surveillance, and then one country doesn't have to solve the problem by itself.

روز جهانی منع خشونت علیه زنان

#ViolenceAgainstWomen

مصادیق خشونت علیه زنان :

مزاحمت‌های خیابانی

خشونت کلامی

کتک زدن

کشیدن مو

تهدید با هر نوع سلاح سرد و گرم

تجاوز

سیلی زدن

براساس آمار سازمان جهانی بهداشت هر ۱۱ ثانیه یک زن در دنیا مورد آزار و خشونت قرار می گیرد و حتی بارداری نیز برای آنها مصونیت ندارد.

Datasec Middle East