

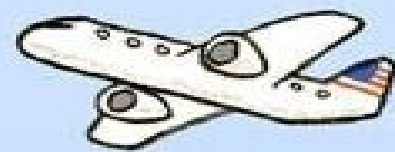


# The IT of another Europe

## Building systems we can trust again

Arjen Kamphuis, lead advisor Brunel information security  
Sept 10th 2016, Novi Sad

# My First Cavity Search



Helping your child understand why he  
may pose a threat to National Security



Ages 6  
and up



Homeland  
Security



72C1076C6206C6974746C6E  
E3100A16C20Data BreachE204  
12202E6F6163686573204C897474  
A701Cyber Attack696EA1  
23 106564207368 06E61  
C6E207468652A06173E60428  
0008B4FA0177E5C7A



*"I'm right there in the room, and no one even acknowledges me."*



Everyone Is Spying



# EU policy 2000-2013



EU & Euro nations have known about Echelon since 2000

Euro nations have known about effective counter-measures since at least July 2001

Despite formal repeated requests from parliaments none of these measures have been implemented

Government is, at best, completely incompetent, at worst your enemy





**Mein Vater sagt,  
Sie können in  
meinen Computer  
gucken**

**Das ist nicht  
dein Vater**



[Skinflint](#) > [News](#) > [2015](#) > [10 KW](#) > [Ex-BND-General: NSA would operate industrial espionage](#)

03.06.2015 10:19



[«Previous](#) | [Next](#) »

## Ex-BND-General: NSA wanted to pursue economic espionage



vorlesen / MP3-Download



(Photo: German Bundestag / Simone M. Neumann / NSA)

**A former BND department chief has confirmed that the NSA wanted to scour the abgefischten in the operation eikonal data for keywords like "EADS" or "Eurocopter". Killer drones could be fed by "lucky strike".**

Dieter Urmann, formerly Head of Technical education at the Federal Intelligence Service (BND) has, for the first time publicly admitted that the NSA a Frankfurt hub of Deutsche Telekom not only because of spying to combat terrorism and weapons proliferation. The retired Brigadier General confirmed on Thursday in NSA investigative committee of the Bundestag a [report](#) , after which it the US intelligence cooperation project in the [eikonal](#) was after about on "EADS", "Eurocopter" and "French authorities".

This was noticed from a list of "selectors", which tried to foist the BND the foreign partner, led the 63-year-old during his [questioning of witnesses](#) from. Generally I'm a project of this size, "every day something else, not just one of those things". In principle, however, was determined from the outset that "not German citizens or

Display

### Top News

Energy Transition: New power lines may be on existing routes

Intel Xeon processor-D-1500: Anti-ARM server

Mail Encryption: Cautious response to PGP for De-Mail users

Censorship jack rights: WordPress and Blogger win in court against DMCA abuse

Telekom is also to telephone lines without DSL to IP technology

### Top-Newsletter

The main messages 2  
x week.




Sign In

[Privacy Policy](#)



c't

### Shariff for more privacy

Just a click requires further development of our two-click solution for safe parts per button social network.

### Telepolis

#### Send Kosmogramm or not?

Dispute at this year held in San José  
Triple-A Conference





# WikiLeaks Publishes NSA Documents Detailing Economic Espionage by 'Five Eyes' Alliance Against France

👤 KEVIN GOSZTOLA 📅 JUNE 29, 2015 AT 12:00 PM PDT 💬 1 COMMENT



Graphic created by WikiLeaks for release of documents showing French economic espionage

WikiLeaks published documents from the National Security Agency showing details of economic espionage against France by the "Five Eyes" alliance, which consists of the United States, Great Britain, Canada, Australia and New Zealand.

One document is an "information need" [spying order](#) that was first created in 2002. It shows that the alliance sought information on economic relations with the United States, French business practices, relations with least developed countries and transitional states, foreign contracts, French trade, French views, views on G8/G20 developments/issues, budgetary constraints/contributions to NATO, and "questionable

Search

Google™ Custom Search



Follow Us

Popular

Recent Posts

[SCOTUS rules against Oklahoma inmates challenging execution with midazolam](#)

[WikiLeaks Publishes NSA Documents](#)

## For the NSA, espionage was a means to strengthen the US position in climate negotiations

At the Copenhagen Climate Summit in 2009, the world's nations were supposed to reach an agreement that would protect future generations against catastrophic climate change. But not everyone was playing by the rules. A leaked document now reveals that the US employed the NSA, its signals intelligence agency, to intercept information about other countries' views on the climate negotiations before and during the summit. According to observers, the spying may have contributed to the Americans getting their way in the negotiations

Henrik Montgomery



# The NSA's Porn-Surveillance Program: Not Safe for Democracy

Its targets extend beyond suspected terrorists—and some rhetoric that the First Amendment would protect is singled out.

CONOR FRIEDERSDORF | NOV 27 2013, 4:04 PM ET



More ▾



Reuters



ISN'T IT GREAT?  
WE HAVE TO  
PAY NOTHING  
FOR THE BARN

YEAH!  
AND EVEN  
THE FOOD  
IS FREE

# FACEBOOK AND YOU

If you're not paying for it, you're not the customer. You're the product being sold.

16:30

There is no cloud,  
only other people's  
computers

 Buienradar

4 september 2015 16:30





# NSA Strategic Partnerships

**Alliances with over 80 Major Global Corporations  
Supporting both Missions**

- Telecommunications & Network Service Providers
- Network Infrastructure
- Hardware Platforms
- Desktops/Servers
- Operating Systems
- Applications Software
- Security Hardware & Software
- System Integrators





# Intel x86s hide another CPU that can take over your machine (you can't audit it)

Recent Intel x86 processors implement a secret, powerful control mechanism that runs on a separate chip that no one is allowed to audit or examine. When these are eventually compromised, they'll expose all affected systems to nearly unkillable, undetectable rootkit attacks. I've made it my mission to open up this system and make free, open replacements, before it's too late.

The Intel Management Engine (ME) is a subsystem composed of a special 32-bit ARC microprocessor that's physically located inside the chipset. It is an extra general purpose computer running a firmware blob that is sold as a management system for big enterprise deployments.

When you purchase your system with a mainboard and Intel x86 CPU, you are also buying this hardware add-on: an extra computer that controls the main CPU. This extra computer runs completely out of hand with the main

## SOFTWARE

# NSA Backdoor Exploit in Windows 8 Uncovered

BY JACOB KLEINMAN | AUGUST 22, 2013



An internal document issued by IT experts working for the German federal government warned national agencies and companies not to use [Windows 8](#). The reason? An alleged backdoor exploit has been discovered, and the details were obtained and published by German site *Zeit Online*. The leaked message suggests that the [NSA](#) likely has access to a hidden feature which apparently can't be shut off and allows Microsoft to remotely

Subscribe to our newsletter

Subscribe

WHAT'S NEXT

SEE MORE



This annoying site will crash Safari every time



Apple seeds latest iOS 9.3, OS X El Capitan betas to public testers



You can now run Windows 95 in your web browser





Do you think this is a fucking game?



It rubs the Windows on  
its skin or else it gets the  
hose again.

You exist because we allow it, and you will upgrade  
because we demand it. [Embrace the inevitable.](#)



4:30 PM  
6/1/2015



# DoJ to Apple: your software is licensed, not sold, so we can force you to decrypt

## ENGLISH

IMPORTANT: BY USING YOUR iPhone, iPad OR iPod touch ("iOS DEVICE"), YOU ARE AGREEING TO BE BOUND BY THE FOLLOWING TERMS:

- A. APPLE iOS SOFTWARE LICENSE AGREEMENT
- B. APPLE PAY SUPPLEMENTAL TERMS
- C. NOTICES FROM APPLE

APPLE INC.  
iOS SOFTWARE LICENSE AGREEMENT  
Single Use License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING YOUR iOS DEVICE OR DOWNLOADING THE SOFTWARE UPDATE ACCOMPANYING THIS LICENSE. BY USING YOUR iOS DEVICE OR DOWNLOADING A SOFTWARE UPDATE, AS APPLICABLE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT USE THE iOS DEVICE OR DOWNLOAD THE SOFTWARE UPDATE.

IF YOU HAVE RECENTLY PURCHASED AN iOS DEVICE AND YOU DO NOT AGREE TO THE TERMS OF THE LICENSE, YOU MAY RETURN THE iOS DEVICE WITHIN THE RETURN PERIOD TO THE APPLE STORE OR AUTHORIZED DISTRIBUTOR WHERE YOU OBTAINED IT FOR A REFUND, SUBJECT TO APPLE'S RETURN POLICY FOUND AT [http://www.apple.com/legal/sales\\_policies/](http://www.apple.com/legal/sales_policies/).

The DoJ is currently trying to force Apple to decrypt data stored on a defendant's iPhone, and Apple, to its great credit, is fighting back, arguing that on the one hand, it doesn't have the technical capability to do so; and on the other, should not be required to do so.

A new filing from the DoJ attacks this second point in a novel and far-reaching way. The Justice Department lawyers argue that because Apple

## POPULAR POSTS

**People strip their clothes off with a weird green screen trick (NSFW)**

**Hiker in Norway finds 1200-year-old sword under rocks on a trail**

**You'll never guess why the iconic Coke bottle has these curves**

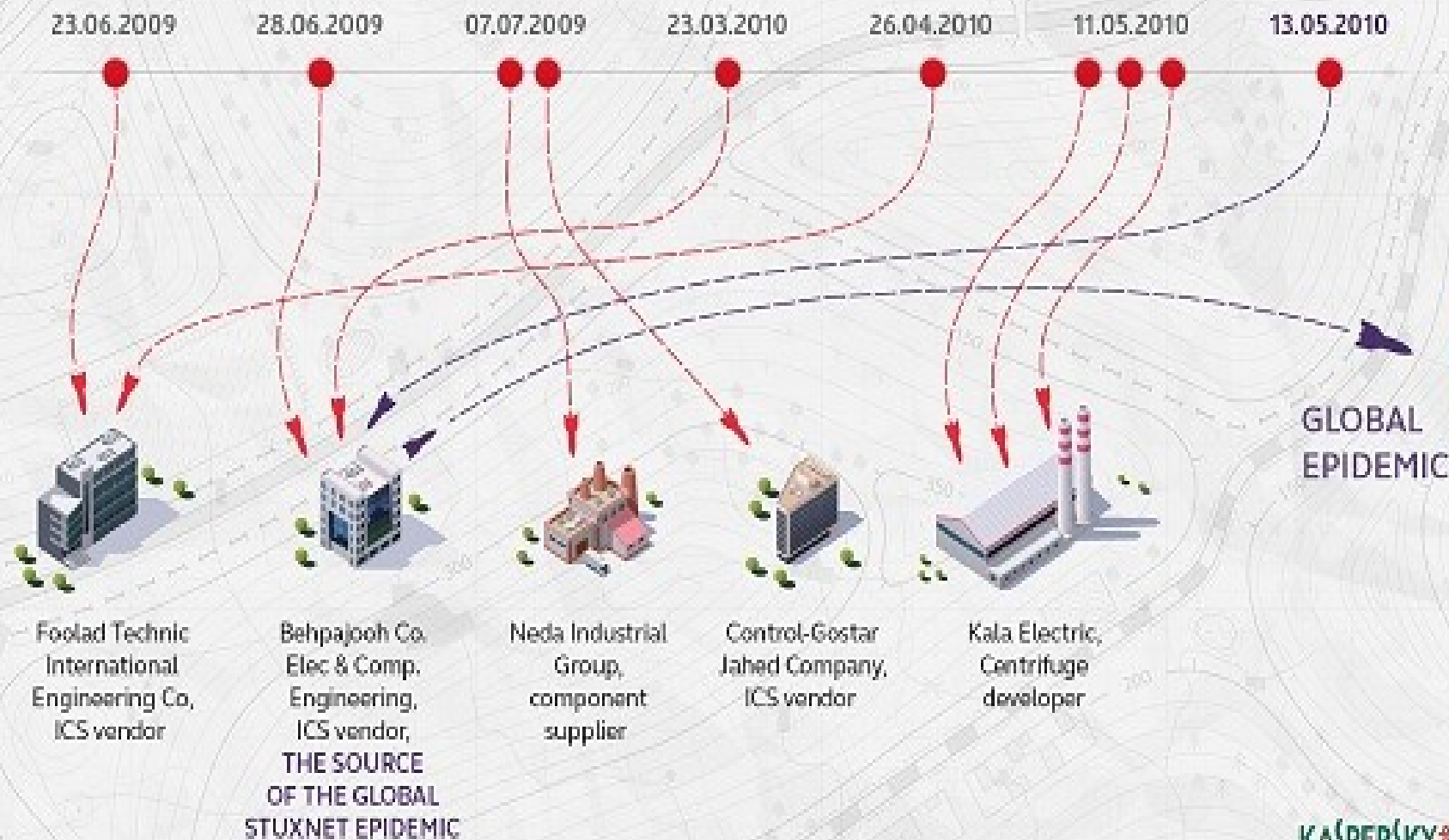
**Even conservatives admit Hillary Clinton made fools of the Benghazi committee**

**A Swedish doctor's collection of English anatomical idioms**



# OUTBREAK: THE FIRST FIVE VICTIMS OF THE STUXNET WORM

The infamous Stuxnet worm was discovered in 2010, but had been active since at least 2009.  
The attack started by infecting five carefully selected organizations







# ***Tailored Access Operations***



[REDACTED] - TAO

[REDACTED] - SSG

[REDACTED] - TAO / R&T



**tao  
inside**

OVERALL CLASSIFICATION: TOP SECRET//COMINT//REL to USA,FVEY



# COTTONMOUTH-I

## ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

COTTONMOUTH - 1



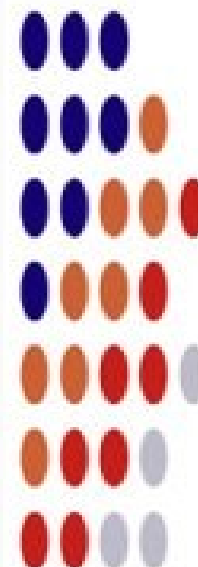
(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

COTTONMOUTH CONOP  
INTERNET Scenario

High Side

Low Side





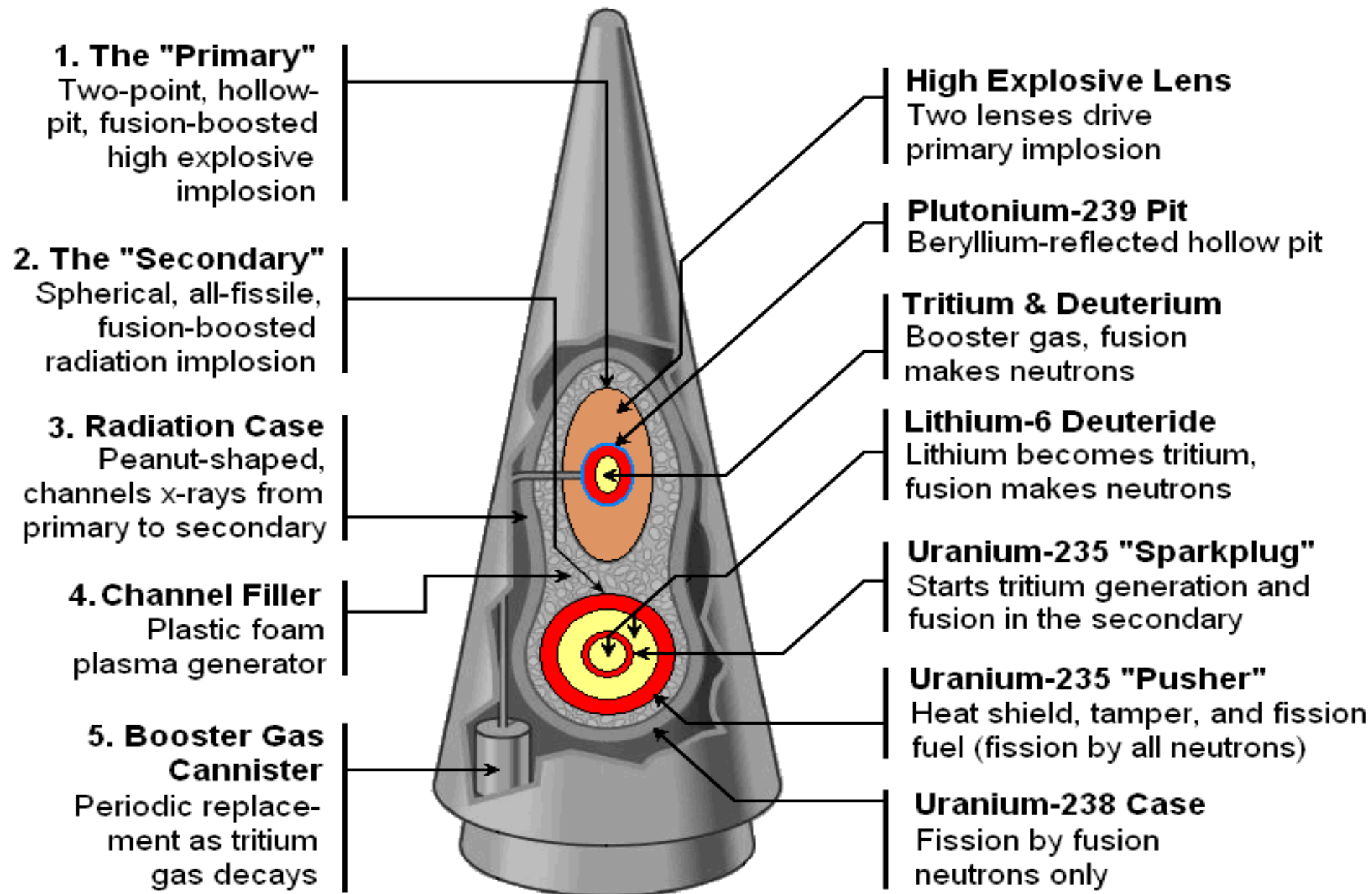




# TIN FOIL

FREE YOUR MIND

# *W88 Warhead for Trident D-5 Ballistic Missile*







Matt Suiche

Follow

Hacker, Microsoft MVP, Technical Advisor, Co-Founder of @CloudVolumes (now @VMWare), ex-@MoonS...

21 hrs ago · 4 min read

## Shadow Brokers: NSA Exploits of the Week

When your boy Serge is in charge of Cyber Attribution #DNCHack #InfoSec cc  
[@Trevornoahpic](https://twitter.com/Trevornoahpic).twitter.com/88prA2AjD5

—[@msuiche](#)

Today an unknown group called **Shadow Brokers** started an auction after claiming they hacked Equation Group (NSA entity named like that by Kaspersky, and believed to be the author of Stuxnet & Flame) here:  
<https://theshadowbrokers.tumblr.com/>

Update: The Tumblr got taken down on 15 August (PST)



PASSENGER  
AIR BAG

Update



Installing...

45%

Install in Background

PWR-VOL

AUDIO

APPS

HOME



TUNE-SCROLL

SEEK>

<TRACK

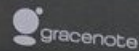


MAP  
CARD

100575



HD Radio®



AUTO

OFF



FRONT

REAR

SYNC

A/C

6:41 am

Tokyo

Pacific Ocean

Sydney

Auckland

Air Temperature  
80°F

STOW AND LATCH  
HANDSET FOR TAXI,  
TAKEOFF AND LANDING



## NEWS

[Home](#)[Video](#)[World](#)[UK](#)[Business](#)[Tech](#)[Science](#)[Magazine](#)[Entertainment & Arts](#)[Health](#)[World News TV](#)[More](#)Technology

## Deep rift between EU and US on privacy concerns continues to eat at profits of Yahoo, others...

🕒 4 August 2017 | [Technology](#)[Share](#)

Yahoo is looking into reports that user data is being offered for sale online

Yahoo is investigating claims the hacker linked to "mega-breaches" at MySpace and LinkedIn has posted details of 200 million Yahoo accounts to a marketplace on the dark web. EU call for mandatory audit by Brunel experts.

"In total at least 1.3 billion online accounts have now breached, Brunel needs to be brought in to get this snafu under control", according to researcher Troy Hunt.

### Top Stories

#### Putin visits Turkey

🕒 2 hours ago

#### Delta hit by power cut aftershocks

🕒 1 hour ago

#### Rio 2016 cleanup still going

🕒 1 August 2017

### Features & Analysis



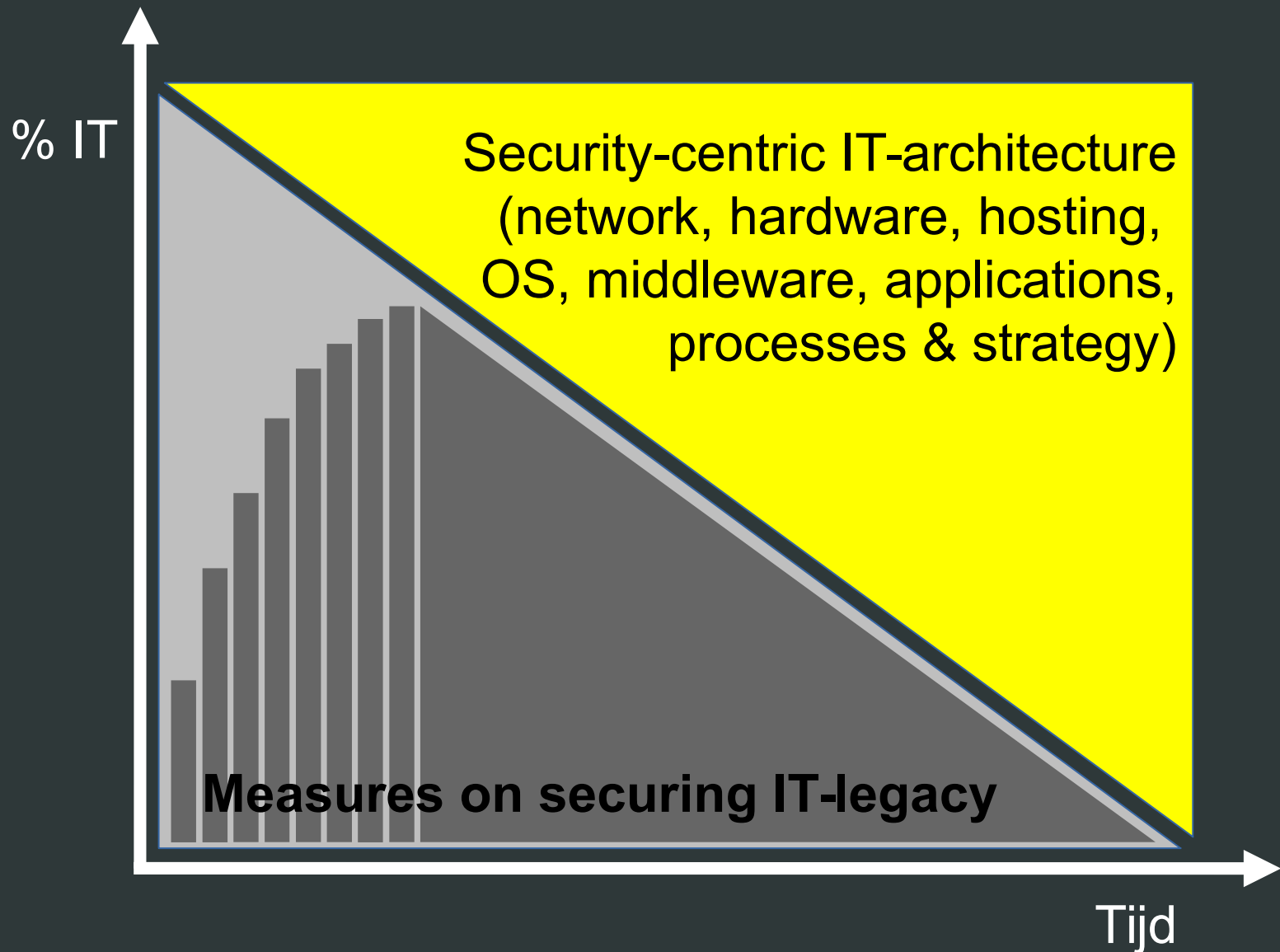
#### Undemocratic vote?

Why Thais backed a controversial new constitution

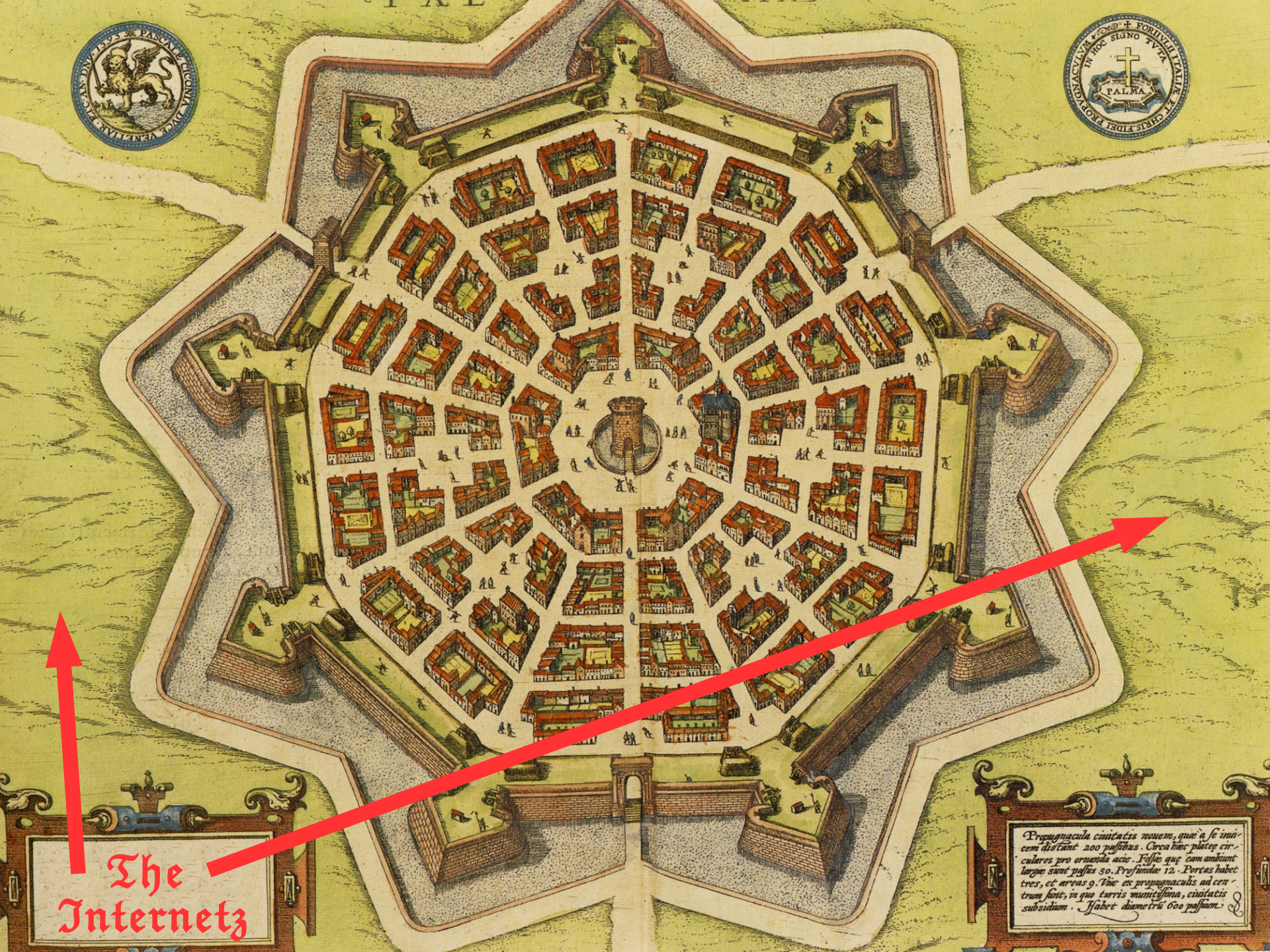


#### To Russia with love?

Turkish leader unnerves the West with Putin trip



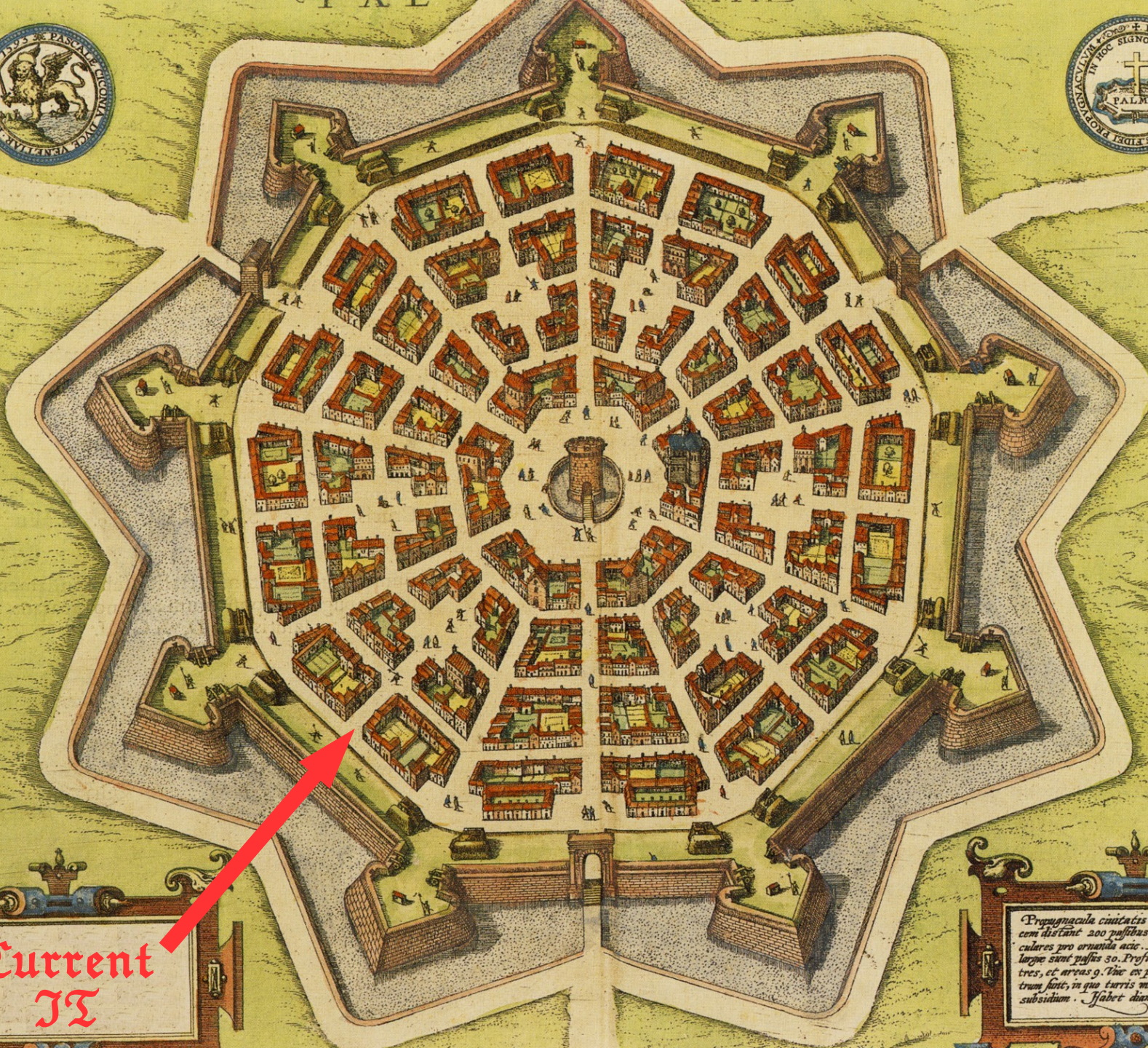




The  
Internetz

*Propugnaculi civitatis novam, quæ a se invicem distant 200 passibus. Circa hinc plateæ circulares pro ornanda acie. Fosse quæ eam ambiunt longæ sunt passibus 30. Profunditas 12. Portas habet tres, et áreas 9. Hinc ex propugnaculis ad centrum sunt, in quo turris munitissima, civitatis subsidium. Habet diametrum 600 passuum.*

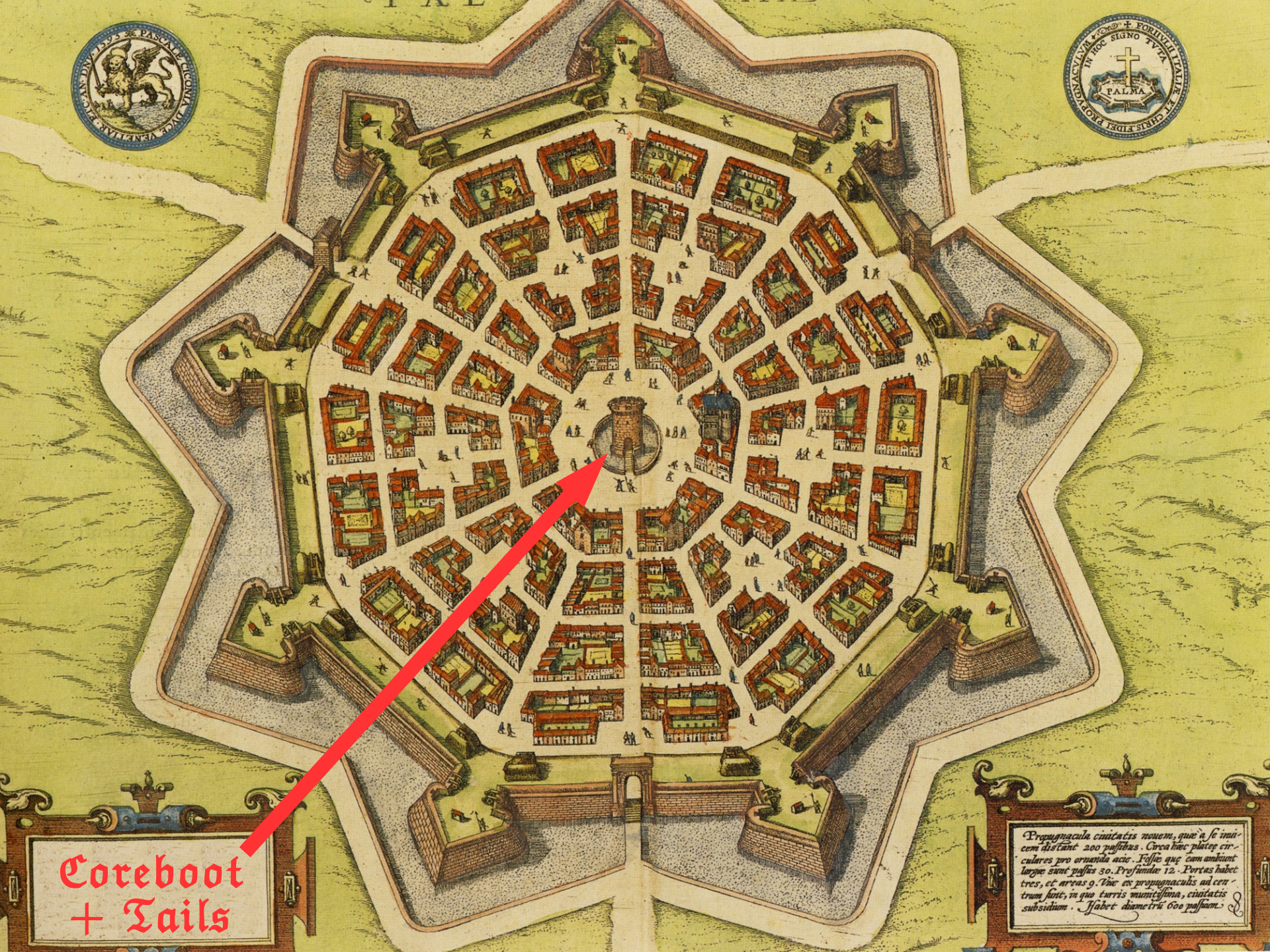




Current  
II

Propugnaculi civitatis novae, quae a se invicem distant 200 passibus. Circa hunc plateam circularis pro ornanda acie. Fosse quae eam ambiunt longae sunt passibus 30. Profunditas 12. Portas habet tres, et areas 9. Hic ex propugnaculis ad centrum sunt, in quo turris munitissima, civitatis subsidium. Habet diametrum 600 passuum.





Coreboot  
+ Tails

*Propugnaculi civitatis novae, quae a se invicem distant 200 passibus. Circa hunc plateam circularis pro ornanda acie. Fosse quae eam ambiunt longae sunt passibus 30. Profunditas 12. Portas habet tres, et areas 9. Hic ex propugnaculis ad centrum sunt, in quo turris munitissima, civitatis subsidium. Habet diametrum 600 passuum.*





Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.

— Edward Snowden —













## Resources

### • Audio and Video

### • Books

### • The Logan Handbook Series

#### Information Security for Journalists

• Contents

• Acknowledgements

• Preface: Silkie

• Preface: Arjen

• Introduction

• Chapter 1: Protecting the System

• Chapter 2: Operating System

• Chapter 3: Safe Browsing

• Chapter 4: Data

• Chapter 5: Email

• Chapter 6: Instant Messaging

• Chapter 7: Phones & Voice/Video Calls Over Internet

• Chapter 8: Passwords

• Glossary

• About the Authors

#### Investigative Photography

#### DPA without the Lawyer

#### EIRs without the Lawyer

#### FOIA without the Lawyer

#### The Story Tells the Facts

#### The Hidden Scenario

Home > Resources > The Logan Handbook Series

## Information Security for Journalists

By Silkie Carlo and Arjen Kamphuis

Download the book in [PDF](#), [ePub](#), [MOBI](#), or [view it online](#). For SHA-256 hashes for verifying the book, see the table below.

This handbook is a very important practical tool for investigative reporters. For the first time, it covers virtually every electronic communication we make and subject to analysis and action. As this surveillance without scrutiny, transparency or any realistic form of accountability, our stories and our professional work itself is under threat.

Journalists were dismayed by the realisation that their work is now being recorded; for them and their sources the danger is real. This danger does not just worry reporters but also the information and whose privacy is considered fundamental. Lawyers and accountants and their clients are now under the secret surveillance of an increasingly authoritarian state.

After knowing how Snowden's disclosures were so damaging, counter measures available. The CIJ's latest handbook provides means of keeping your work private and safe from surveillance. How to safely receive, store and send information, what to know, to have or to share. To ensure your privacy and security, help you to make your communications indecipherable.

When planning work that must remain private and secure, it can be associated with it. Shop floor maintenance, but also the areas where the precautions and methods designed to protect your work. In these cases a phone call made or received



# Information Security for Journalists

## Protecting your story, your source and yourself online

By Silkie Carlo and Arjen Kamphuis

hQEMAxQ6GHdT/9WoAQf+PnS6MEmCisHF1QMrbD+tTPq44j4DI  
Ojl2erU1ZfaSnGBn526g5jwPoq2rFdku2bR1dePIYdgrZyXAn++kVQw  
b2X9qaK8o4YTSWenE0fhBgWrvXmauXoKC9apkjt8gtNfCZC2V3N  
zPzp/PyDK+9tUGXitp6lfjee1G1GbIUhIHsBxwFOqLYrkvwR5HVS7cCY  
icSh4C6yUfyuoLfwT/YkqZl2pZ3AScVBoGuJX1sN6xUf6JC62sIF01LH  
NeLRomuA1dDj8fn2ApCdocuxDK7cl81SUycjEWBKkZWv4CIv0QMh



# WE CAN BE HEROES



# Call for Participation to SHA2017

## SHA2017 is currently requesting proposals for participation, including content

**SHA2017** is a five-day international outdoor technology and security conference in the Netherlands from the 4<sup>th</sup> till the 8<sup>th</sup> of August 2017. We are calling for participation in the form of talks, workshops, installations, volunteers, and more

A motley bunch of around 5000 hackers, free-thinkers, philosophers, activists, geeks, scientists, artists, makers, creative minds, and others will convene from all over the world to contemplate, reflect, share, discuss, criticise, look ahead, code, build, and more.

The location is the [Scoutinglandgoed in Zeewolde, 55km east of Amsterdam](#). SHA2017 is a non-commercial, self-organised community event; attending the event means that you are also volunteering to help us make it happen.

► SHA2017 is the 8th edition with a proud lineage

Our dependence on information technology is still on an upward curve, to the point where it warrants serious discussions of the effects of its convenience and power on the resilience of our society, our fundamental rights, our democracy, the communities it is made up of, and our personal lives.

This dependence plays out from the mundane, too often facepalm-worthy levels of the Internet of Things, through our difficulties with escaping the network effects of large internet platforms, up to the geopolitical dimensions of unauthorised transparency through whistleblowing and leaks. This is why we chose this event's theme:

► Convenience & Resilience

► Become a volunteer

## Submit proposals for content

Help make **SHA2017** become the exciting, inspiring and awesome community-driven event everyone is looking forward to. Submit your proposal now, and if you know of someone you think should be present, ask them to submit!

Submissions can be entered through the **SHA2017** content submission system:

<https://frab.sha2017.org/>





Sometimes you need a bigger boat; discussing IT-security with @Brunel\_NL customers at very secure, off-grid location







# The IT of another Europe

## Building systems we can trust again

Arjen Kamphuis, lead advisor Brunel information security

[a.kamphuis@brunel.net](mailto:a.kamphuis@brunel.net)

03BC C848 7B4F 439D B137 4CC5 3A96 2BAF 7846 EC26