Systematic Threat Assessment
How to Adapt Security Measures Based on the Research on Latest Threats

Florian Schmid

Project Manager Systematic Threat Assessment

Montreal, October 21, 2014

CASRA

Center for Adaptive Security Research and Applications

- › Founded in 2008

- › Emerged from the Visual Cognition Research Group (VICOREG) at the University of Zurich (founded 1999)

- › About 30 employees (mainly psychologists, computer scientists and engineers)

- › **Main aim: Increase security and facilitation at airports and other environments involving people and technology.**

- › CASRA members are from the following organizations:

APSS Software & Services Ltd.

n|w University of Applied Sciences and Arts Northwestern Switzerland

University of Zurich UZH

Project ICU
Intelligence, Competence and Unpredictability

Goal	Increase threat detection performance by combining intelligence with competence of security officers and unpredictable changes of screening level
Funding	Swiss Federal Office of Civil Aviation (FOCA)
Scope	All Swiss airports and security screening providers
Collaborations	Swiss airports, police authorities, federal competence centers and screening providers
Duration	01.01.2013 – 31.12.2015

Challenge: Training Content

Which threat objects should be trained?

Online News

Information about **3D-printed guns**

BBC online: May 06, 2013

Open Online Forum
3D-files of gun parts available

- 380 Barrel (Threaded).stl
- 380 Barrel (Unthreaded).stl
- Bottom Cover.stl
- Firing Pin Bushing.stl
- Frame Pins (x3).stl
- -Frame.stl
- Grip Pin.stl
- Grip.stl
- Hammer Body.stl
- Hammer Pin.stl
- Hammer.stl
- Spring (x2).stl
- Spring Connecting Rod Bushing.stl
- Spring Connecting Rod.stl
- Trigger Spring.stl
- Trigger.stl
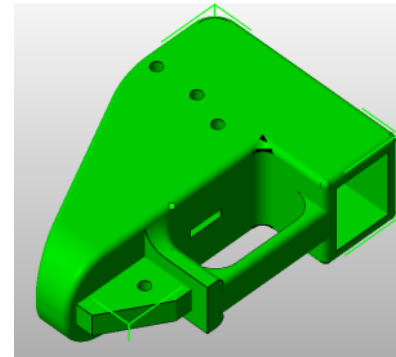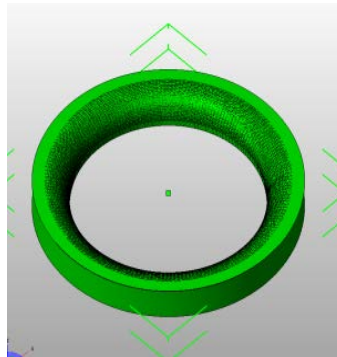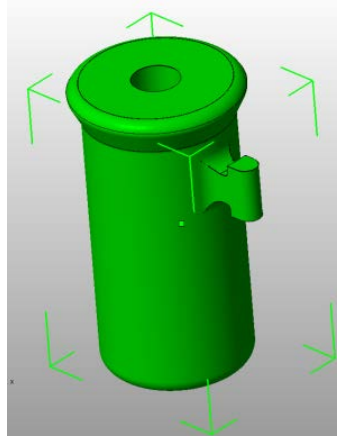
Defcad Forum: May 2013

Deep Web (aka Darknet)

Printed guns available

Deep Web research, April 22, 2014

Consequence

Implementation of new objects in X-ray training software?

Social Media

Manuals of Radio-Controlled IEDs (RCIEDs)
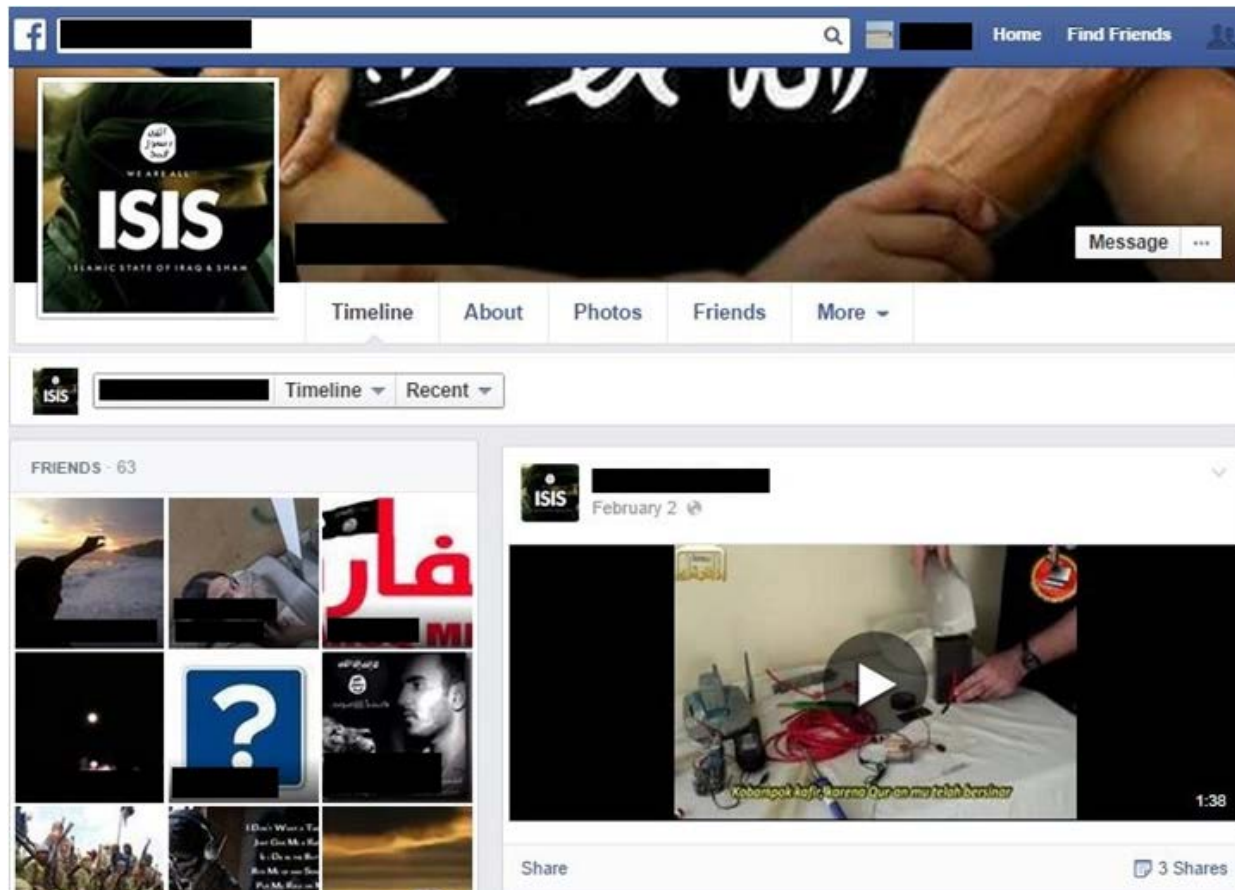
Facebook, February 02, 2014

Video Sharing

Manuals are distributed on **video sharing websites**

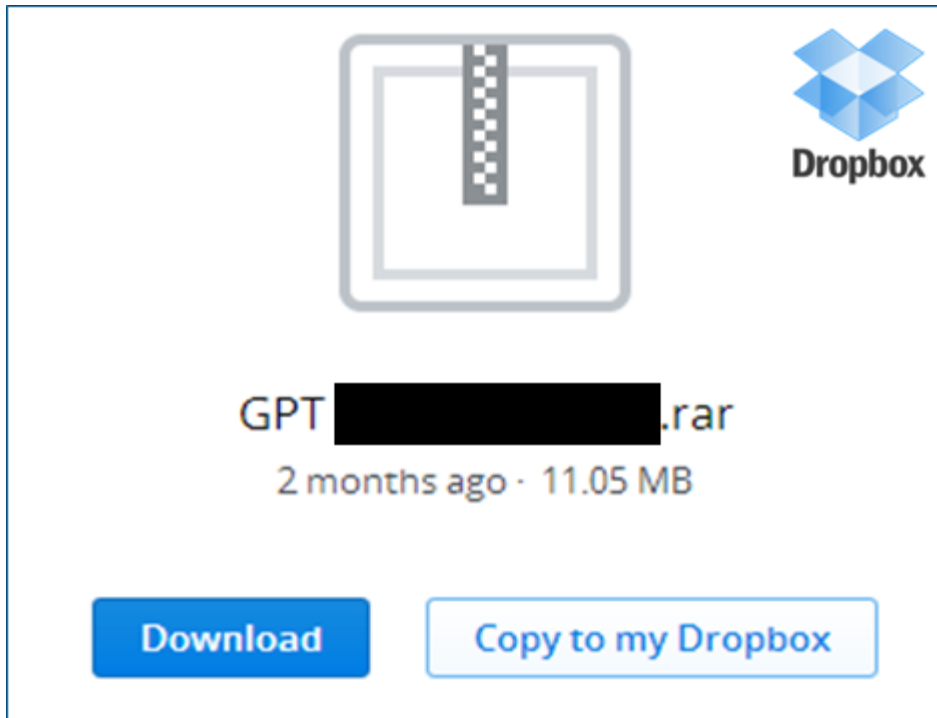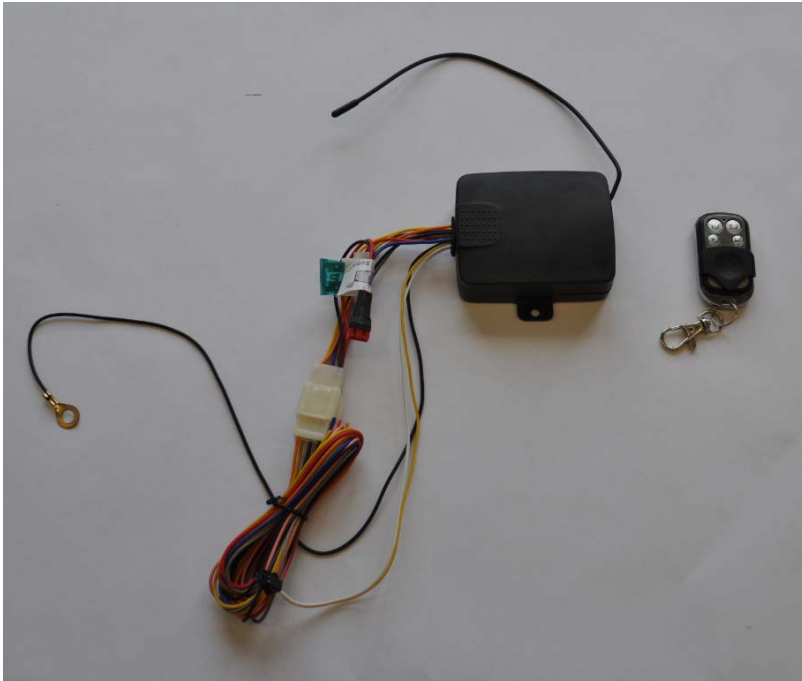Youtube

File Sharing

Manuals are distributed on **file sharing platforms**

Dropbox

Consequence

Implementation of new objects in X-ray training software?

Online News

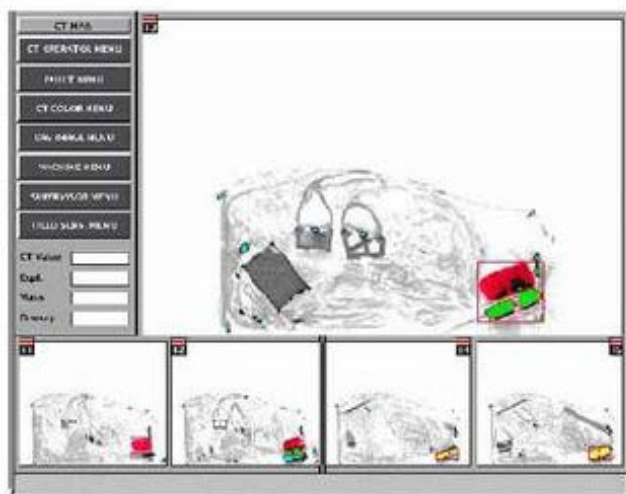Information about **IEDs in electronic devices**

Afghan news site, December 2013

Closed Online Forum

Resurgence of discussion about how to hide explosives

أجهزة الكشف بالأشعة السينية : كانت أجهزة الكشف بأشعة "أكس" الأولية تعتمد على لونين ثم ثلاثة فيما بعد، انتهاءا

إذن كيف نجحنا في تخطي أجهزة الكشف بالأشعة السينية ؟
قمنا باستعمال جهاز يتكون من أجزاء عضوية و غير عضوية و معدنية . تتكون خرطوشة الحبر من الكربون الذي هو مادة
للشكوك إذا ما تم تفتيشها . خلال تواجد الخرطوشة داخل الطابعة تلمس صفيحة معدنية دارة الأسلاك . بهذا الطريقة
صورة لخرطوشة الطابعة المفخخة و هي ممتلئة بمادة PETN و يخرج منها سلكا التفجير

Jihadist forum, May 2014

Consequence

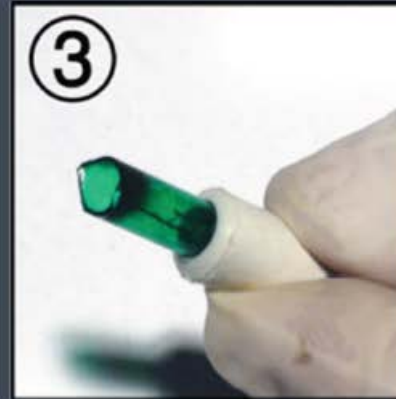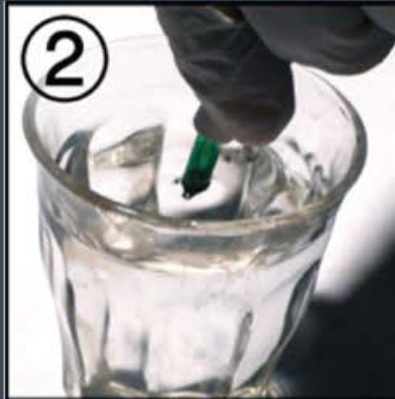Implementation of new objects in X-ray training software?

Radical Propaganda
Manual for **homemade detonators**

Inspire magazine, Summer 2010

Consequence

Implementation of new objects in X-ray training software?

Standard detonators
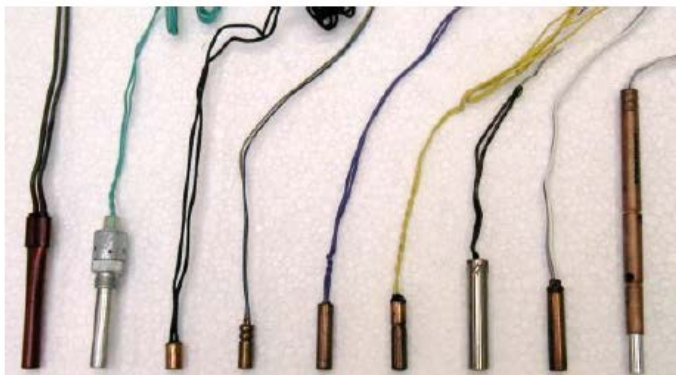
Homemade detonators

Deep Web
How to hide knives

В принципе, в рюкзаке можно провезти даже складные штуки типа мультитулов. Я возил несколько раз, приматывая их к БП ноутбука проводами. На сканере это выглядит как ком электронного барахла с параллелепипедным чем-то в центре. Как правило, не докапываются. Однако, надо быть готовым к тому что рано или поздно дозорные отнимут у вас этот гаджет по причине н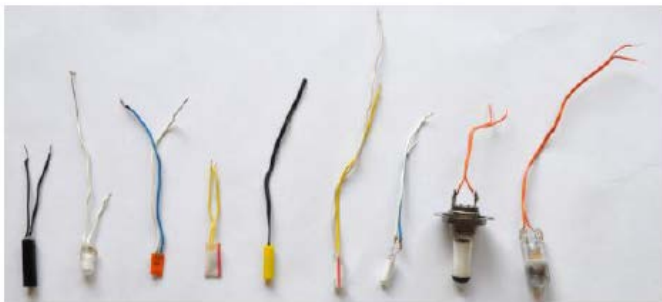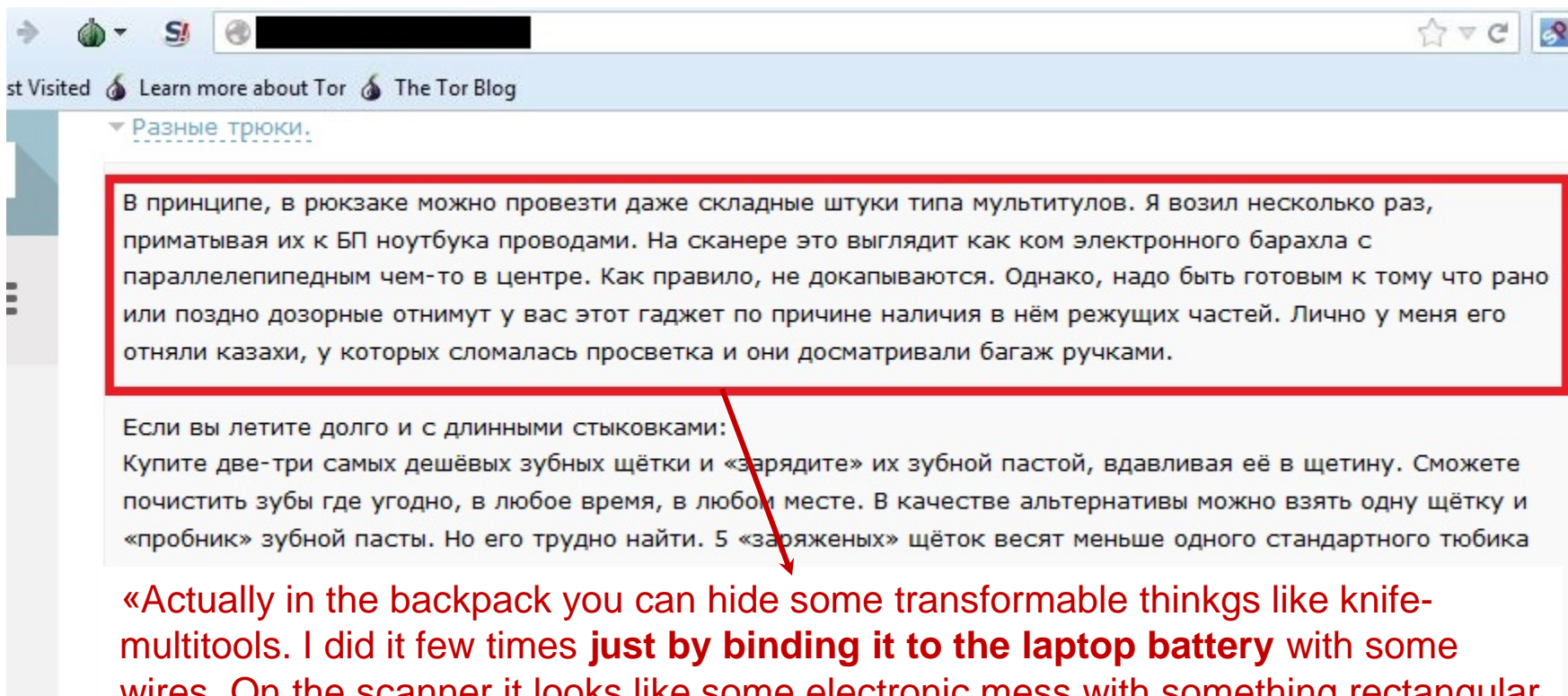аличия в нём режущих частей. Лично у меня его отняли казахи, у которых сломалась просветка и они досматривали багаж ручками.

Если вы летите долго и с длинными стыковками:
Купите две-три самых дешёвых зубных щётки и «зарядите» их зубной пастой, вдавливая её в щетину. Сможете почистить зубы где угодно, в любое время, в любом месте. В качестве альтернативы можно взять одну щётку и «пробник» зубной пасты. Но его трудно найти. 5 «заряженых» щёток весят меньше одного стандартного тюбика
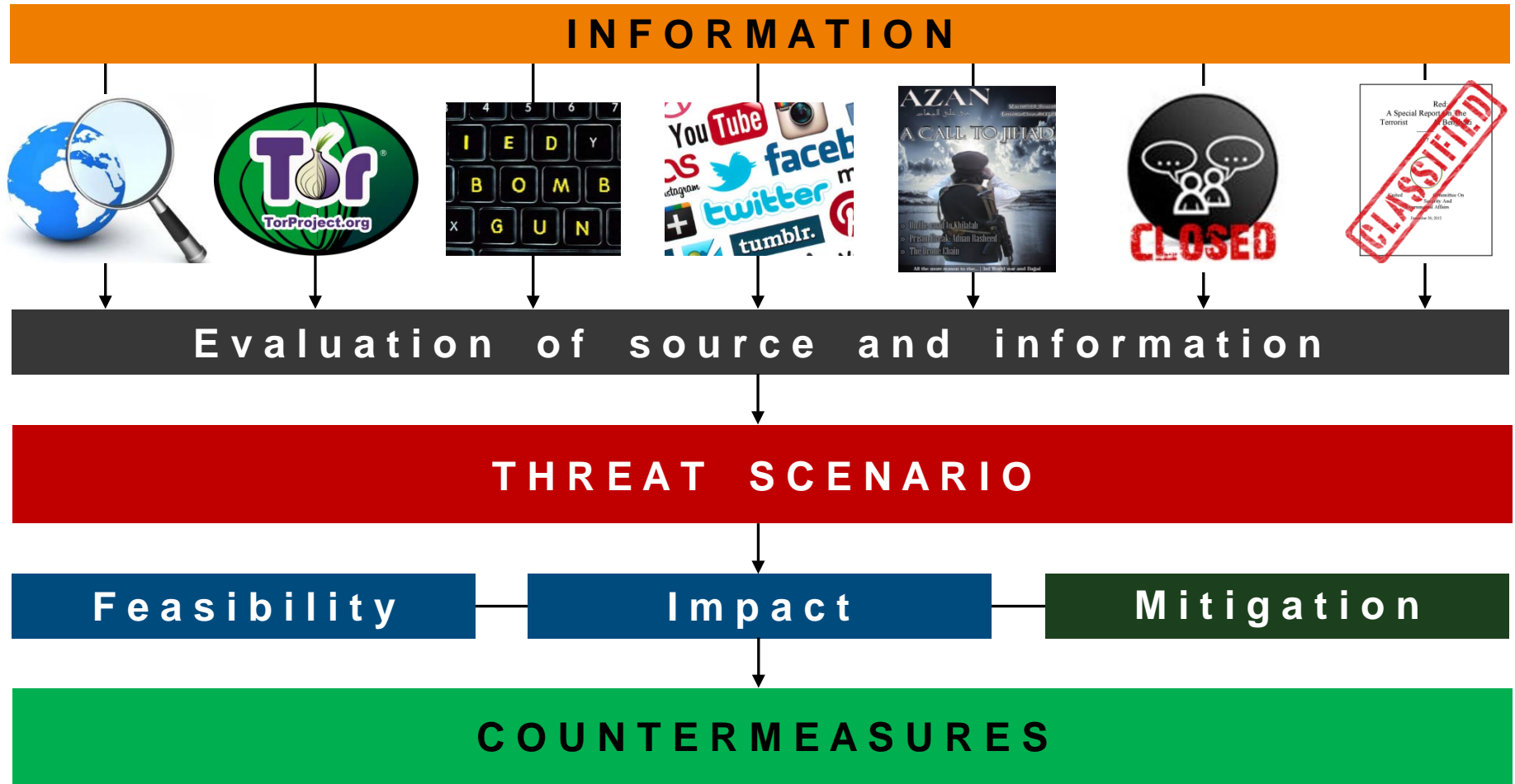
«Actually in the backpack you can hide some transformable thinkgs like knife-multitools. I did it few times **just by binding it to the laptop battery** with some wires. On the scanner it looks like some electronic mess with something rectangular in the center. Usually they *[security personnel]* don't pay attention to this. [...]»

Consequence

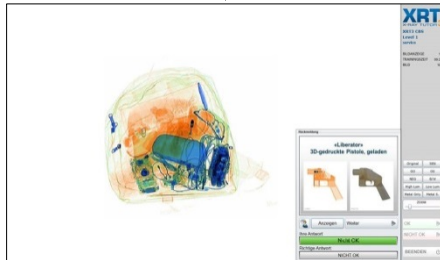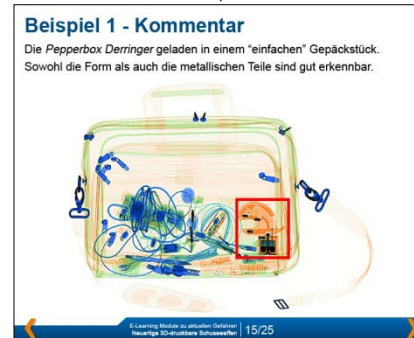Implementation of new objects in X-ray training software?

Systematic Threat Assessment

INFORMATION

Evaluation of source and information

THREAT SCENARIO

Feasibility | **Impact** | **Mitigation**

COUNTERMEASURES

Systematic Threat Assessment

Systematic Threat Assessment

Conclusions

› Keeping up to date

› New types of early stage threats can be found

› Large number of web alerts are constantly generated and have to be evaluated

› Resulting reports serve as support for decision makers

› Processes must be defined in order to ensure know-how transfer to security personnel

Thank you for your attention

Florian Schmid

Project Manager Systematic Threat Assessment

sta@casra.ch