UNODC
United Nations Office on Drugs and Crime

HONLEA 2017: Cybercrime, drugs and the darknet

Neil J. Walsh
Chief
UNODC Global Programme on Cybercrime

@neil_w_unodc
https://www.linkedin.com/in/neiljwalsh

UNODC
United Nations Office on Drugs and Crime

Cybercrime as a Service

UNODC
United Nations Office on Drugs and Crime

Multiple thefts…and rediscovery.. of empty containers

- The Port of Antwerp handles over 10million containers per year – that's over 40 crane movements per hour
- One specialised container handling company had a number of thefts from containers – containers that contained zinc and iron
- A simple theft?
- Not quite

UNODC
United Nations Office on Drugs and Crime

How to collect a container at Antwerp

- The receiving company contacts the Antwerp shipping agent to arrange to collect their container
- The shipping agent creates and issues a PIN number to the receiver by email. This is then given to the lorry driver
- The lorry driver arrives at the Port and gives the PIN to the shipping office

- Once verified, the driver gives the PIN to the crane driver and the container is loaded
- Fast, efficient…and secure?

UNODC
United Nations Office on Drugs and Crime

The crimes continued

- Empty containers were recovered – at the Port – with no evidence of a break-in
- Two shipping agents had losses from containers

- Each loss was recorded as a theft and investigated individually as a “simple” theft
- Then one of the shipping agents reported a burglary at their office (also at the Port)…but nothing was stolen

UNODC
United Nations Office on Drugs and Crime

- CCTV showed two men, dressed in suits, entering the offices late at night

- Federal Investigators attended after a local police officer realised the *modus operandi* was strange (why was nothing stolen?)

UNODC
United Nations Office on Drugs and Crime

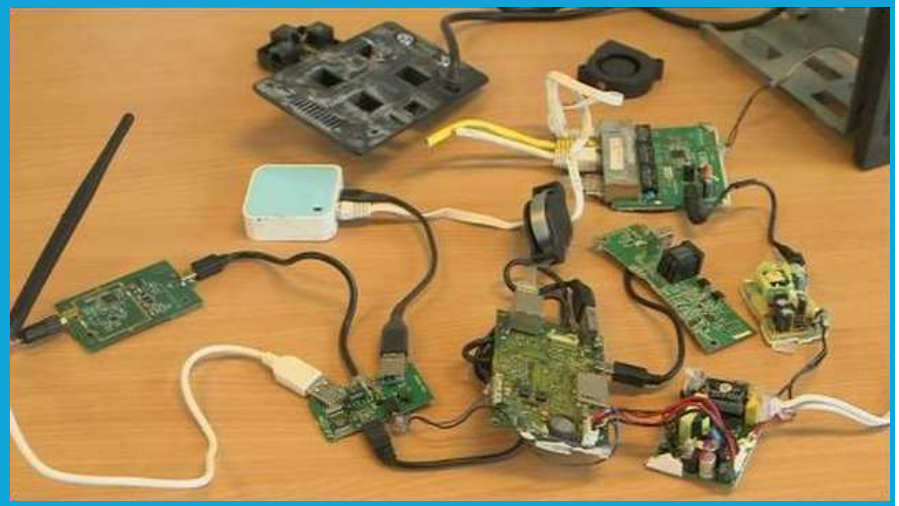
Breakthrough

- Errant WiFi signals throughout the office

- Cyber-team deployed and searched (evidence preservation)

UNODC
United Nations Office on Drugs and Crime

The Compromise



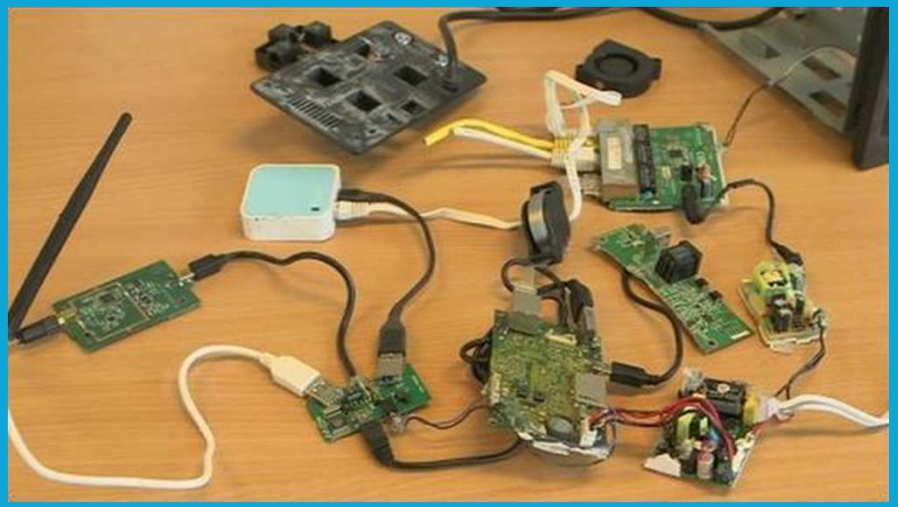
UNODC
United Nations Office on Drugs and Crime

PWNIE plugs

UNODC
United Nations Office on Drugs and Crime

What's under YOUR desk?

A power socket…or a PWNIE plug?



UNODC
United Nations Office on Drugs and Crime

So....

- The Organised Crime Group had TOTAL control of the shipping agent network. But why?
- PIN numbers
- PINs were being issued for containers by two employees.
- Further investigations revealed both women had accepted ADOBE FlashPlayer Updates on their computers by clicking a hyperlink in an email:
- Social Engineering, Spear Phishing and MALWARE deployed

UNODC
United Nations Office on Drugs and Crime

Total Control – multiple vectors

- Technical surveillance team deployed
- WiFi signal…from the car park?
- Key loggers
- Malware
- PWNI
- Brief surveillance of the target
- Geographical and jurisdictional problems near Antwerp

UNODC
United Nations Office on Drugs and Crime

UNODC
United Nations Office on Drugs and Crime

Coordinated International Investigation

- Cross-border surveillance (Belgium and Netherlands)
- Malware traced by IP address to South America
- Research of compromised containers now suggested cocaine trafficking – not metal theft
- IT Security and Penetration Testing

UNODC
United Nations Office on Drugs and Crime

From Colombia to Belgium

- https://www.youtube.com/watch?v=GLyhM8jYzxU

UNODC
United Nations Office on Drugs and Crime

Result

- Large seizures of cocaine
- Multiple arrests
- Significant organisational learning – and excellent first report…from a non-specialist investigator
- Cyber is not just about computers
- Private-sector, Shares and Due Diligence concerns

UNODC
United Nations Office on Drugs and Crime

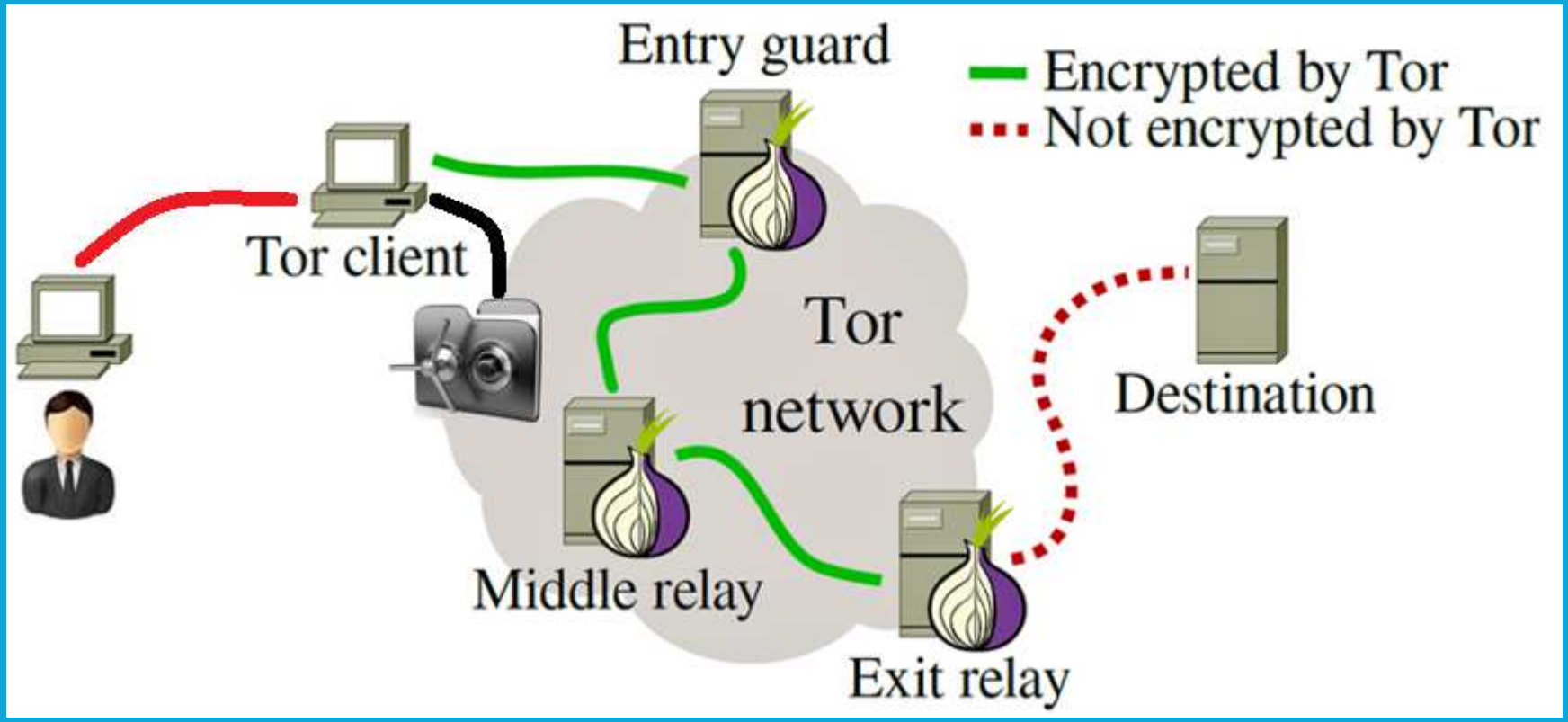
UNODC
United Nations Office on Drugs and Crime

The Darknet

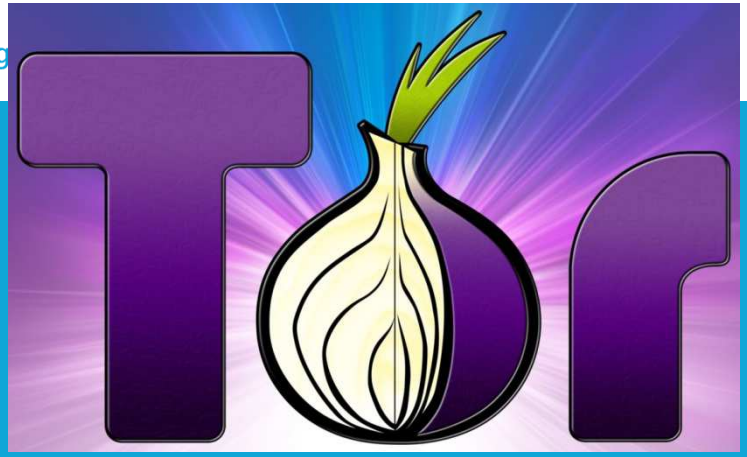
- The **Darknet** is a collection of thousands of websites that use anonymity tools like TOR to hide their IP addresses.
- It's most known use is for black-market drug and weapon sales and child abuse.
- It can't be accessed from a regular internet browser like IE, Firefox or Chrome.
- TOR, The Onion Router, is the most popular way to access the Dark Web.

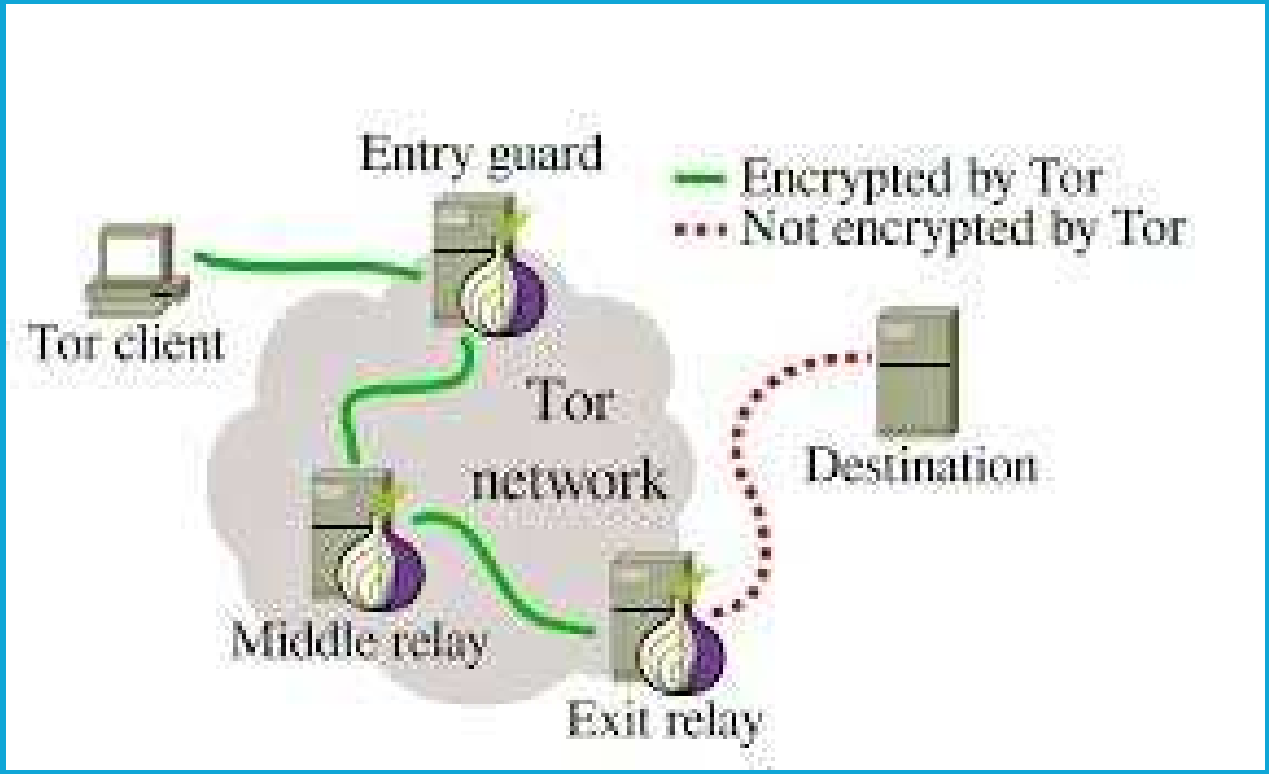
UNODC
United Nations Office on Drugs and Crime

Live Demonstration (hopefully)



UNODC
United Nations Office on Drug



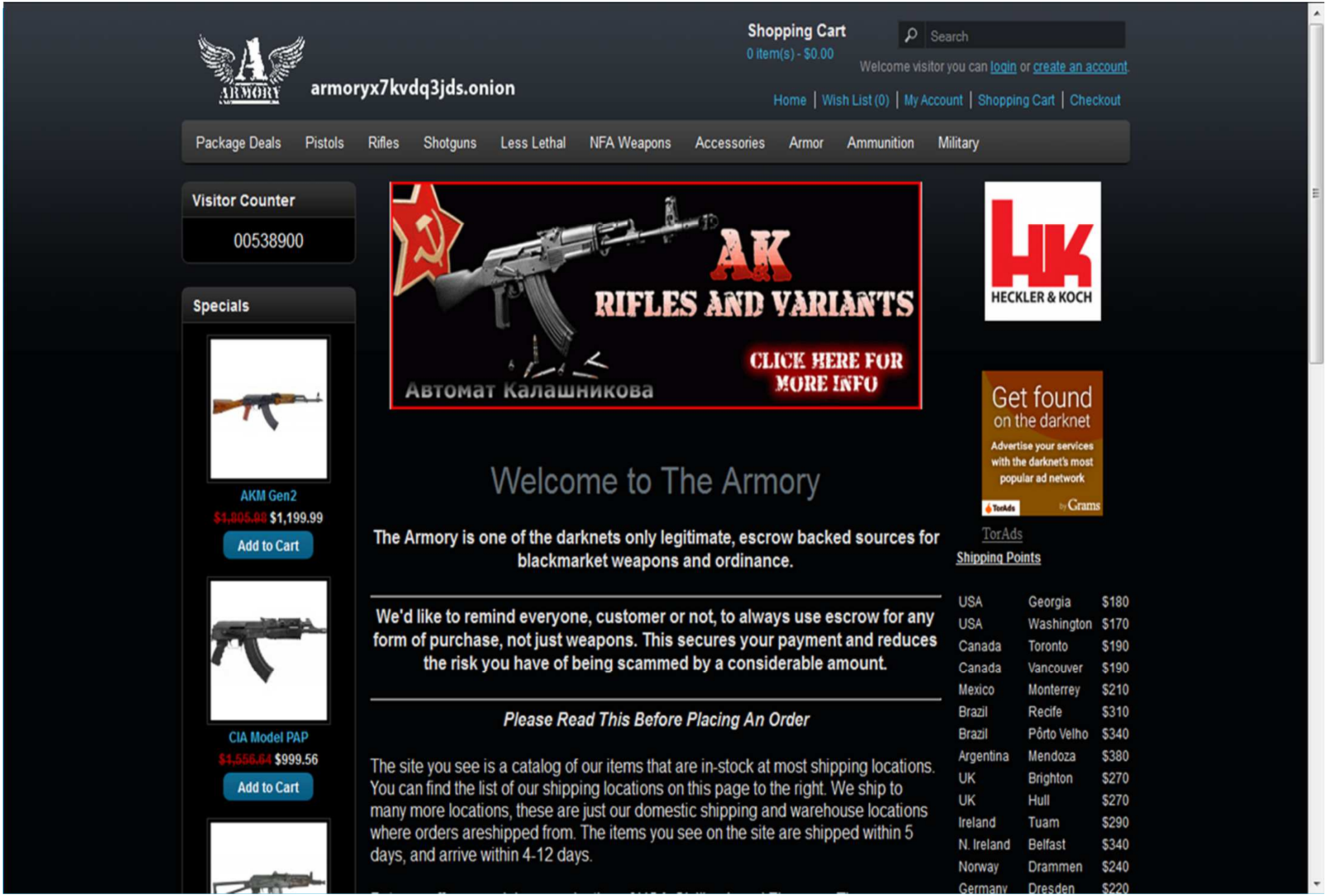



TorBrowser
About Tor
about:tor
Startpage
Tor Browser
3.5.3-Windows
Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Startpage.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
Run a Tor Relay Node »
Volunteer Your Services »
Make a Donation »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »
1:11 AM
3/20/2014

UNODC
United Nations Office on Drugs and Crime

Hidden Services: firearms, drugs and online child sexual exploitation

UNODC
United Nations Office on Drugs and Crime



UNODC
United Nations Office on Drugs and Crime

(more photo)

FLIR FIRST MATE II MS-224B THERMAL NIGHT VISION BLACK (HUNTER GRADE)

Detector Type: 24° x 18° NTSC
Focal Length: 19 mm
Waveband: 7.5 - 13.5 µm
Start-up Time (from Stand-by): < 5 seconds
Focus: Fixed
Image Processing: FLIR Proprietary Digital Detail Enhancement
Power Button: On/Off
Polarity: Toggles White Hot, Black Hot, InstAlert
Brightness: Adjusts Display Brightness
Built-in Display: Color LCD Display
Video Refresh Rate: <9 Hz (NTSC and PAL)
Image Polarity: White Hot, Black Hot, InstAlert
Battery Type: Internal Camera Battery / Li-Ion
Battery Life (Operating): 5 Hours + (typical)
Environmental Rating: IP-67
Operating Temp.: -4°F to 122°F
Weight w/ Lens: 12oz
Size (L x W x H): 6.70" x 2.31" x 2.44"

$1500 (1.2694 BTC)
amount 0

(more photo)

FLIR LS32 THERMAL NIGHT VISION BLACK (LAW ENFORCEMENT GRADE)

Detector Type: 336 x 256 VOx Microbolometer
Focal Length: 19 mm Fixed Focus
Field of View (H x W): 17° x 13°
Digital E-Zoom: 2x
Start-up: [illegible] Seconds
USB Port: Charging Software Updates
Image Optimization: Proprietary Digital Detail Enhancement
Refresh Rate: 30 Hz
Polarity: White Hot, Black Hot, InstAlert
Weight (with battery): 12.9 oz (365 g)
Battery Type: Internal Battery/Li-Ion
Battery Recharging: USB Cable for Internal Battery; AC Adapter
Battery Life (Thermal Imager Only): 5+ Hours Typical
Laser Type: Visible Red (Wavelength 630-660nm)
Laser Class: IIIA/3R (US FDA/IEC)
Laser Power: <5mW (3.5mW typical)
Environmental Rating: IP-67
Operating Temp.: -4°F to 122°F (-20°C to +50°C)
RANGE PERFORMANCE - Detect Man-Sized Target (1.8 m A- 0.5 m): ~600 yds (~548 m)

$3800 (3.2159 BTC)
amount 0

(more photo)

AMMUNITION

9mm Ammo 115gr FMJ (50 per box) $23 (0.0195 BTC)
amount 0

.380 ACP FMJ (50 per box) $25 (0.0212 BTC)
amount 0

.40 S&W FMJ (50 per box) $40 (0.0339 BTC
amount 0

12 Gauge 00 Buckshot (10 Boxes of 5 = 5[illegible] rnds) $40 (0.0339 BTC)
amount 0

.22LR Remington (10 Boxes of 50 = 500 rnds) $65 (0.055 BTC)
amount 0

.223 Remington / 5.56 (10 Boxes of 20 = 200 rnds) $70 (0.0592 BTC)
amount 0

.308 Win / 7.62x51 (5 Boxes of 20 = 100 rnds) $70 (0.0592 BTC)
amount 0

7.62x39 (10 Boxes of 20 = 200 rnds) $60 (0.0508 BTC)
amount 0

.45 ACP FMJ(50 per box) $23 (0.0195 BTC

UNODC
United Nations Office on Drugs and Crime

TRUSTED DARKNET MARKETS:

Dream Market

Established: Nov 15, 2013
ltxocqhw4eruf5lu.onion
-Invite (Required)
-Forum
Short Link: **drk.li/Dream**

AlphaBay

Established: Dec 22, 2014
pwoah7oh4jlgdwri.onion
-Invite (Required)
-Forum
Short Link: **drk.li/AB**

Outlaw Market

Established: Dec 29, 2013
outfor6jwcztwbpd.onion

-Forum
Short Link: **drk.li/Outlaw**

East India Company

Established: Apr 28, 2015
g4c35ipwiutqccly.onion

-No Forum
Short Link: **drk.li/EiC**

ALL OTHER DARKNET MARKETS:

These markets are not as well established as the above "Trusted Markets".

Agora Marketplace

Established: Dec 3, 2013
agorahooawayyfoe.onion
-Invite (Required)
-Forum
Short Link: **drk.li/Agora**

Abraxas Market

Established: Dec 13, 2014
abraxasdegupusel.onion
-Invite (Required)
-Forum
Short Link: **drk.li/Abraxas**

Crypto Market

Established: Dec 22, 2014
cryptomktgxdn2zd.onion

-Forum
Short Link: **drk.li/CM**

Middle Earth Marketplace

Established: Jun 22, 2014
mango7u3rivtwxy7.onion

-Forum
Short Link: **drk.li/ME**

UNODC

United Nations Office on Drugs and Crime

HONLEA 2017: Cybercrime, drugs and the DarkNet

@Neil_W_UNODC