

Considerations on Intrusion Software Products

Collin Anderson

ISTAC, October 28, 2015

Litigation Group

Treasury Solicitor's Department
One Kemble Street, London, WC2B 4TS

Bhatt Murphy Solicitors
DX 36626
Finsbury

DX 123242 Kingsway 6
Switchboard: 0207 210 3000
Direct Line: 0207 210 4711
Direct Fax: 020 7210 3001
francesca.debenham@tsol.gsi.gov.uk

AND BY EMAIL: m.scott@bhattmurphy.co.uk

Please Quote: Z1211844/FZD/B5
Your Reference: MPS/FT/002295/0001

8 August 2012

Dear Sirs

EXPORT CONTROLS FOR SURVEILLANCE EQUIPMENT - PROPOSED JR

1. We refer to your letter before claim under the pre-action protocol for judicial review dated 12 July 2012 ("**the PAP Letter**"). This is the response to that letter of the Secretary of State for Business Innovation and Skills ("**the Secretary of State**"). Please address any future correspondence in this matter to Francesca Debenham quoting the reference above.

History of Controls

FinFisher, U.K. and Bahrain

Growing Market


Concerns Over Going Dark

TeleStrategies®

ISS World® America

Intelligence Support Systems for Lawful Interception,
NSA Data Retention, Cyber Threat Detection and Information Sharing

SEPTEMBER 29 – OCTOBER 1, 2015 • WASHINGTON DC



**Where Law Enforcement,
Public Safety, Telecoms and
the Intelligence Community turn for
Technical Training and Product Selection**

Lead Sponsor

SS8®

Associate Lead Sponsors

AQSACOM
Innovating Intelligence

AREA

FIBERBLAZE

]HackingTeam[

Exhibitors and Sponsors

Cambridge Intelligence

MYRICOM
Products by CSPI

FINFISHER®
INTELLIGENCE IN
IT INVESTIGATION

Geofeedia

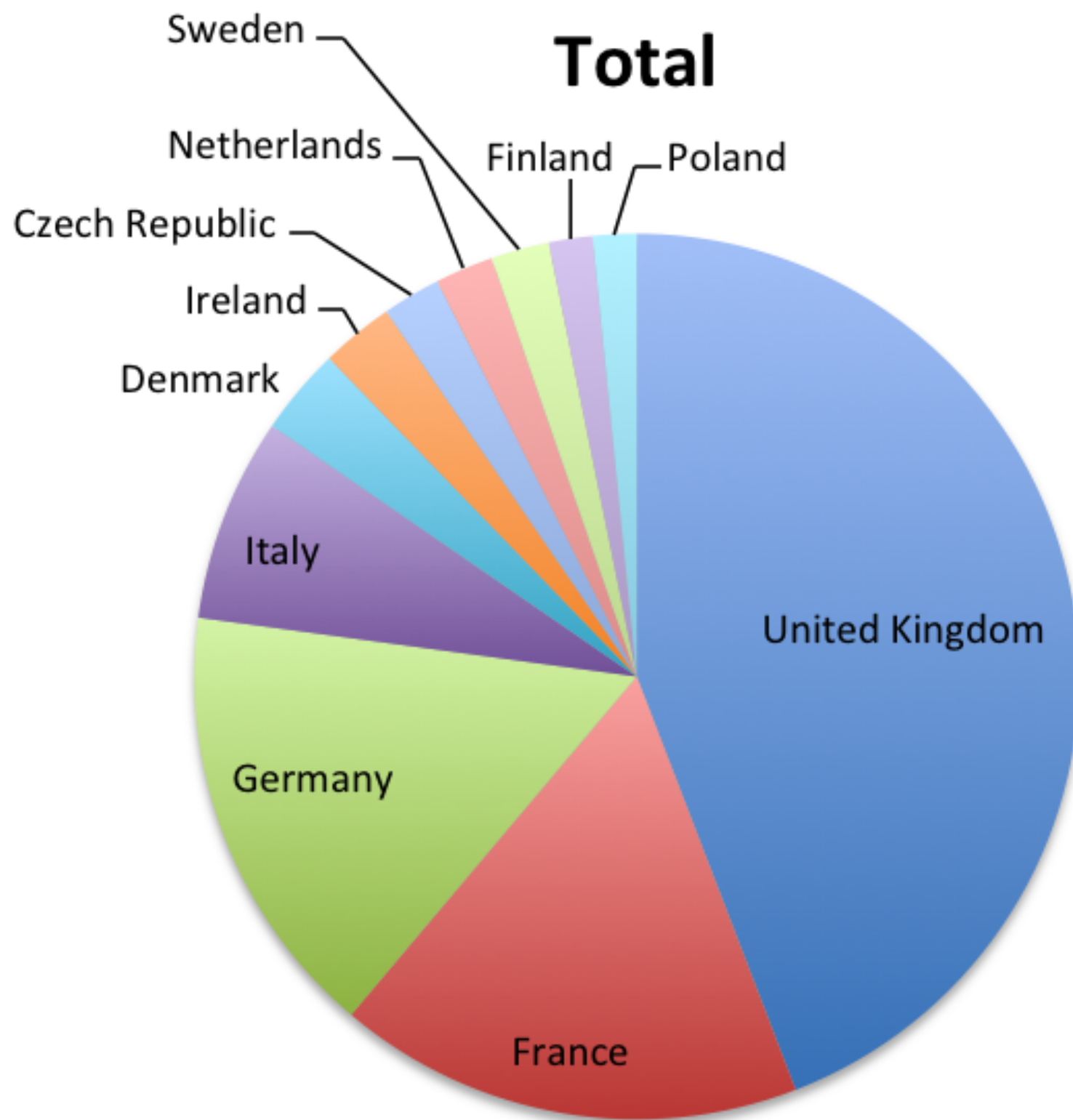
Glimmerglass
Optical Cyber Solutions

NetQuest
Monitoring Access Solutions

octasic

S.E.

To Review Complete Agenda or To Register, Go To WWW.ISSWORLDTRAINING.COM



Wassenaar Origin Items

Surveillance Items

Wassenaar Origin Items

- FinFisher (formerly Gamma Group)
- HackingTeam
- DigiTask
- AGLAYA
- RCS Lab
- Gr Sistemi (Dark Eagle)
- Clear-Trail Technologies (QuickTrail)
- Stratign (Spy Phone)
- SS8 (Interceptor)
- iPS (ITACA).

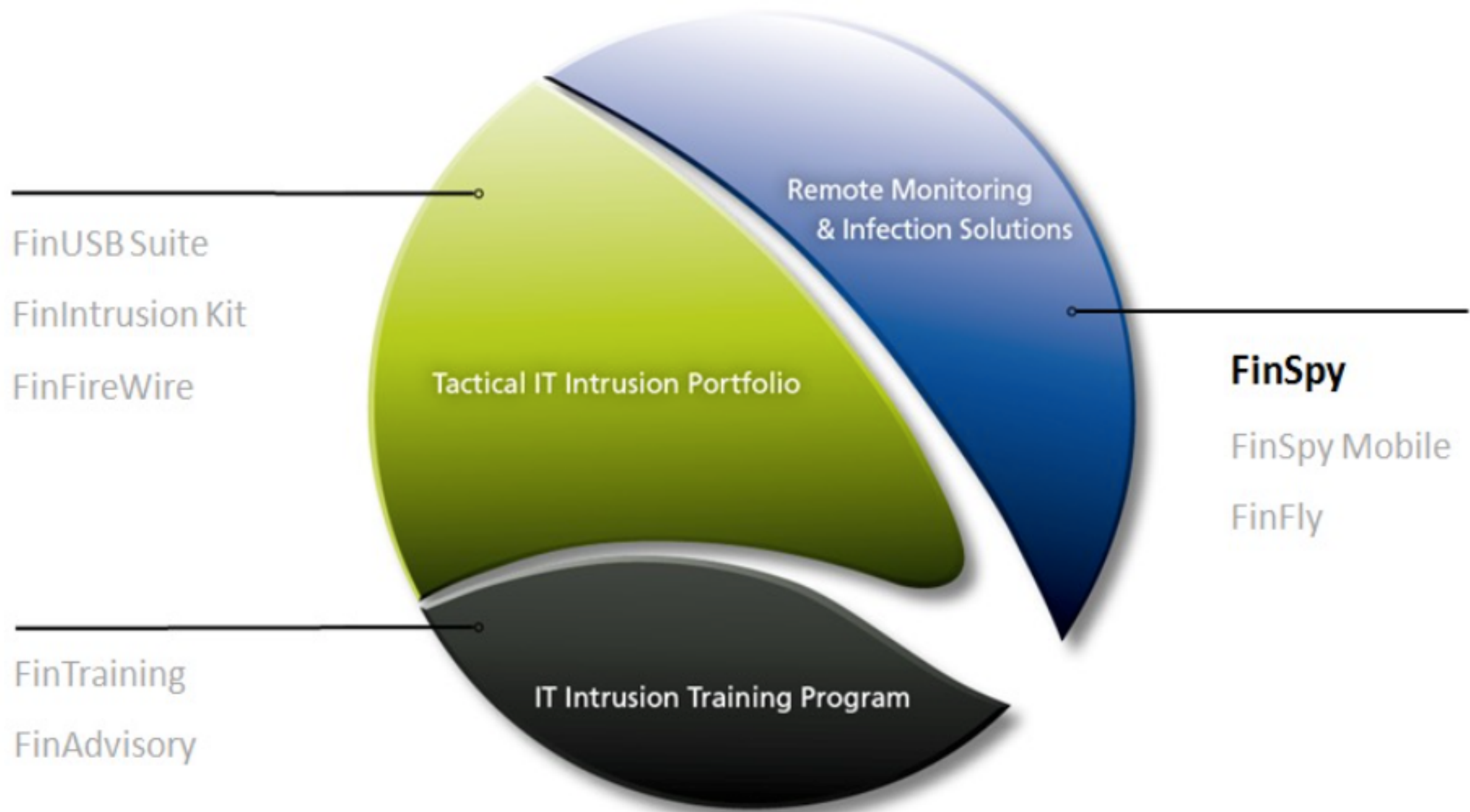
A PRODUCT OF

SS8[®]



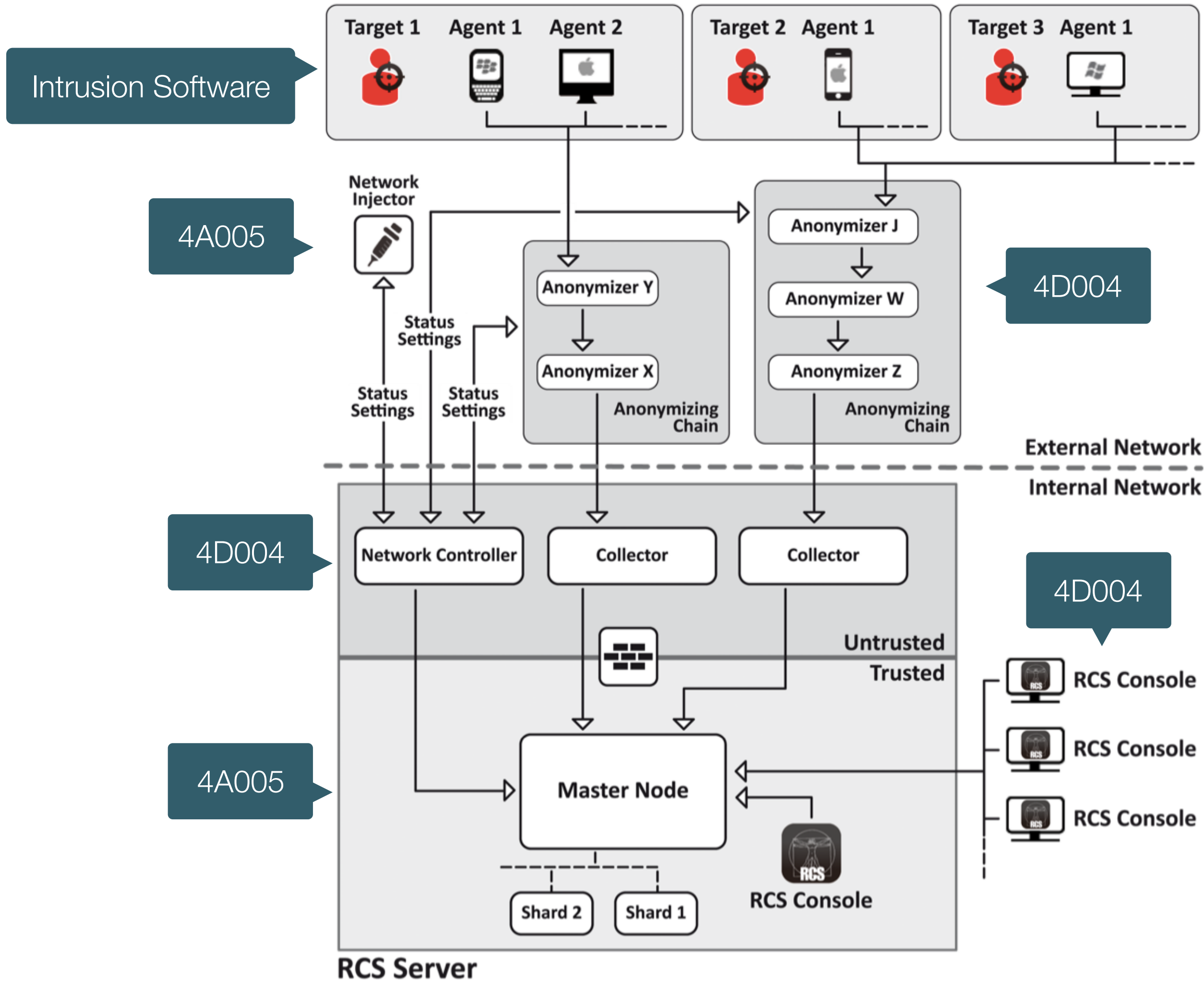
U.S. Origin Items

Intrusion Software

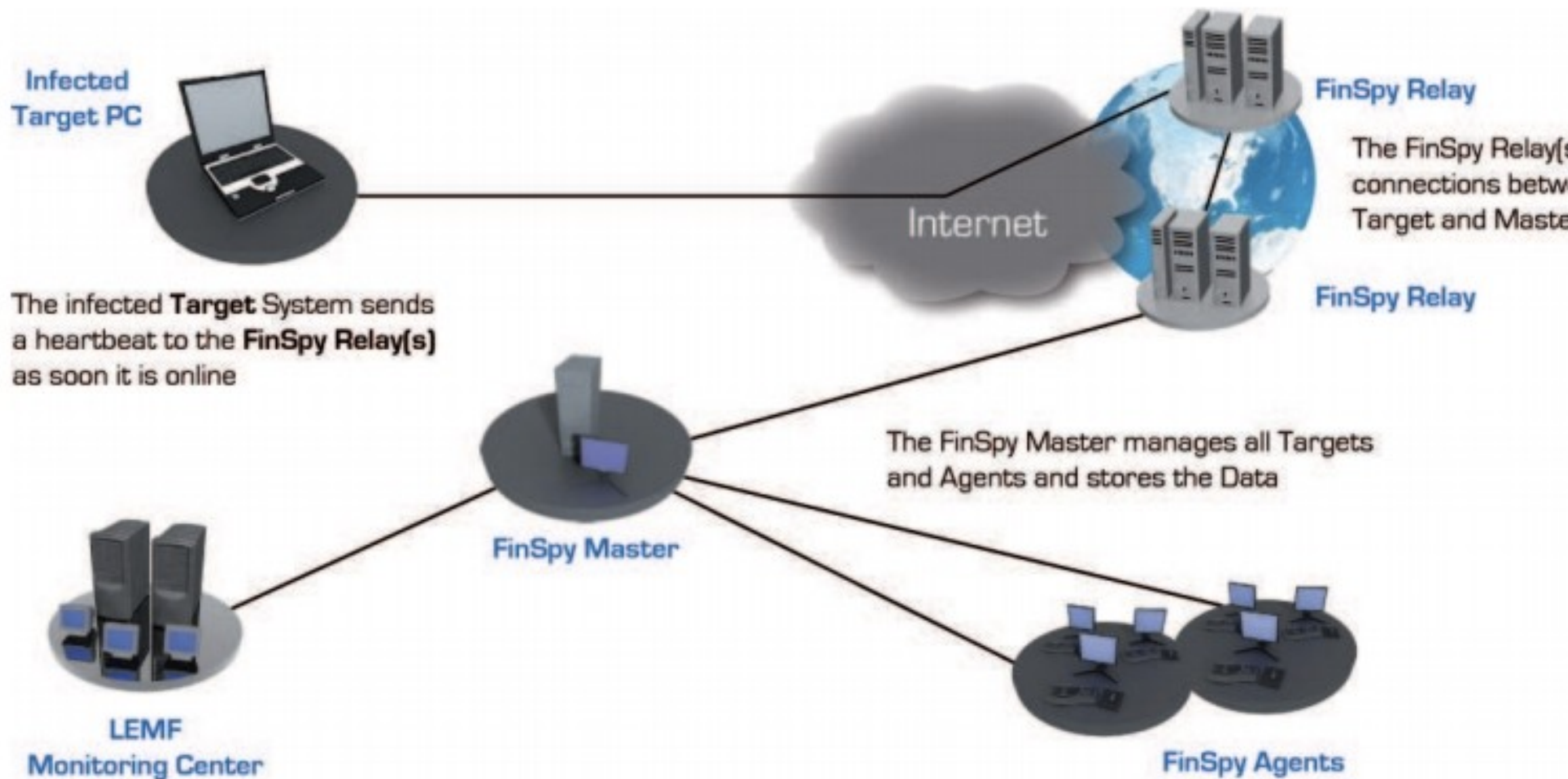


Intrusion Software

Considerations on Surveillance Technologies

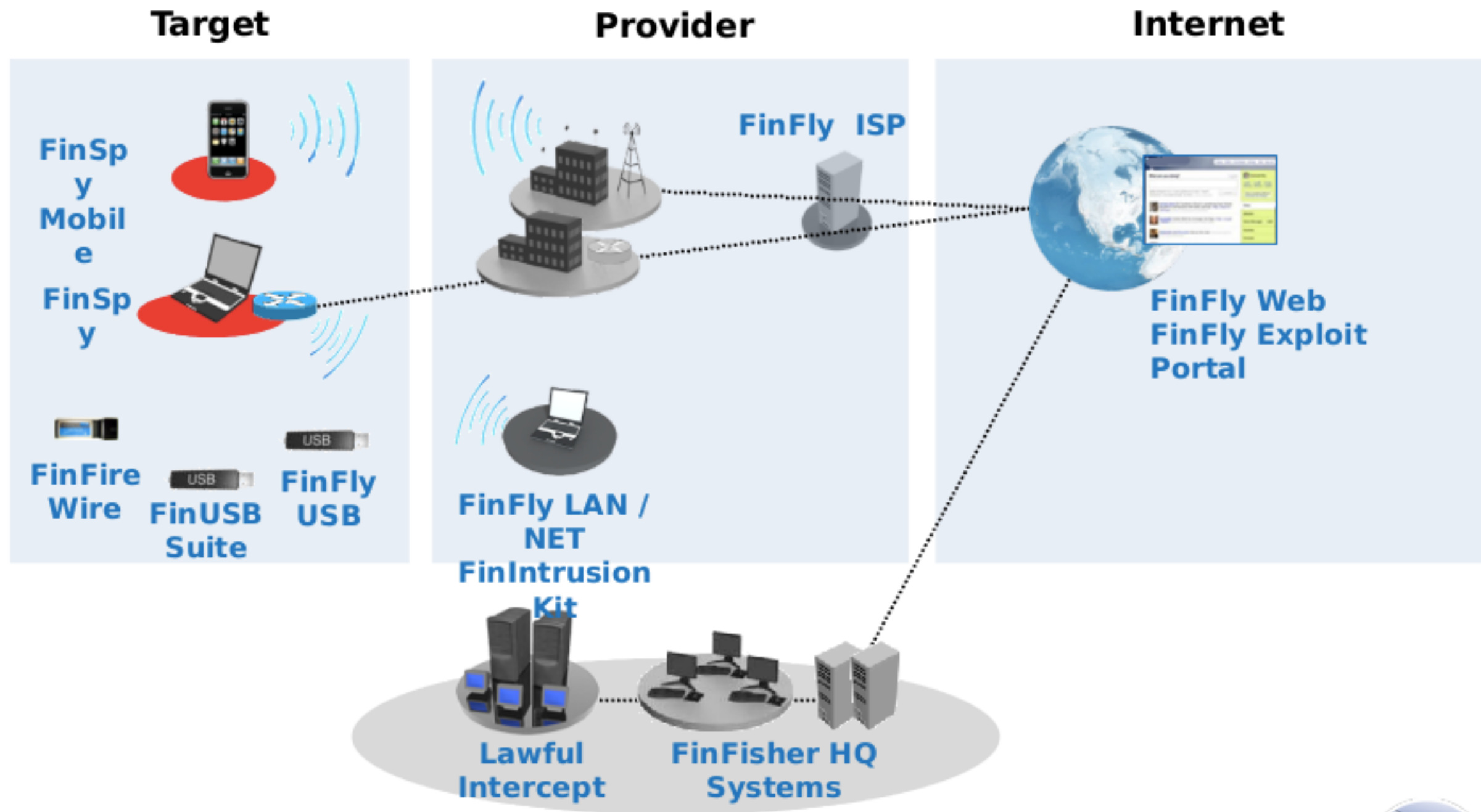


Access Target Computer Systems around the World



Systems, Equipment,
Components (4A005)

Intrusion Software



Systems, Equipment,
Components (4A005)

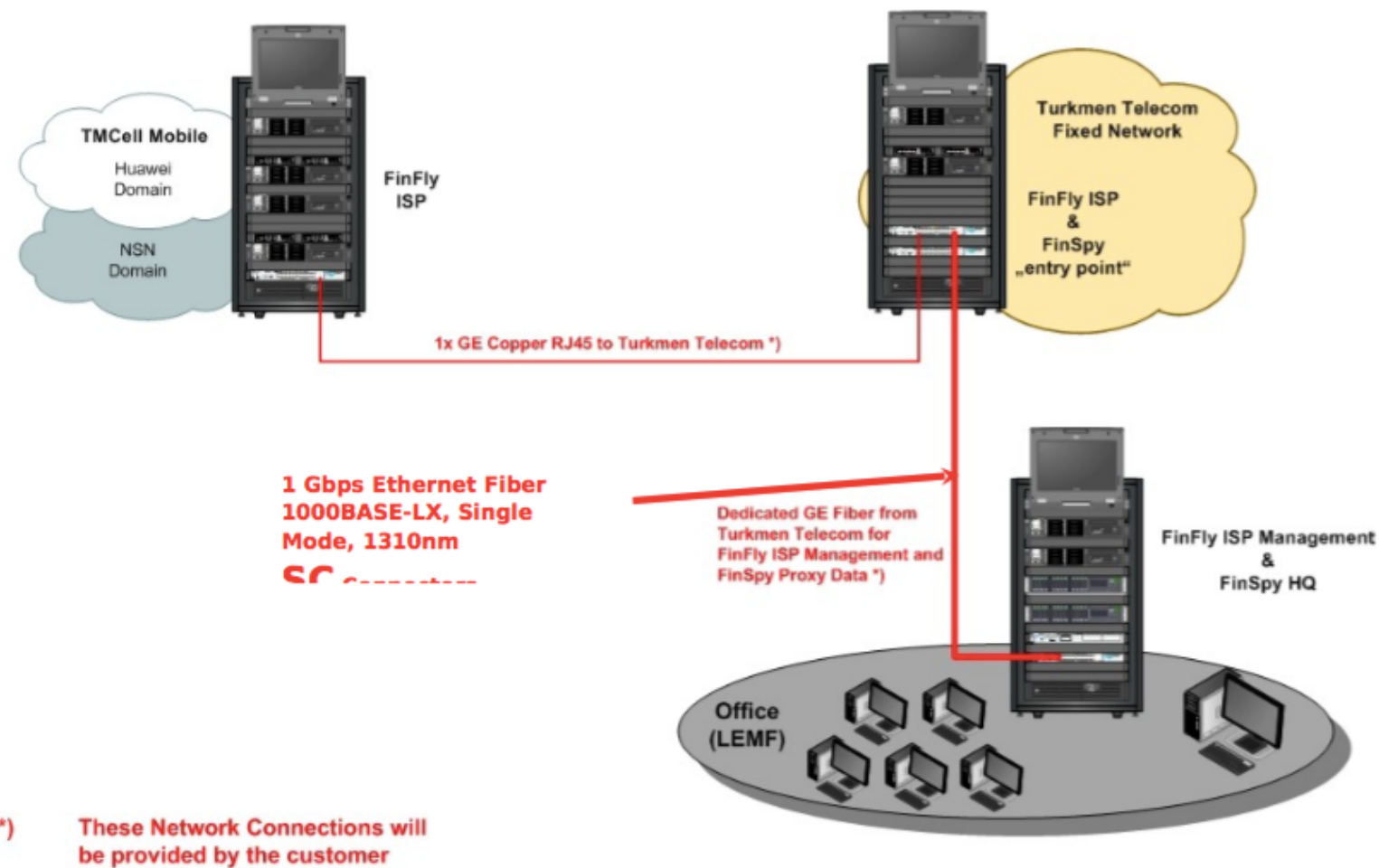
Intrusion Software

3.2 Technical Details

3.2.1 Project Overview

The following graphic shows an overview of the project setup:

FinFly ISP: Turkmenistan Overview



Systems, Equipment,
Components (4A005)

Intrusion Software

The FinFly USB provides an easy-to-use and reliable way of installing Remote Monitoring Solutions on computer systems when physical access is available.

Once the FinFly USB is inserted into a computer, it **automatically installs the configured software** with little or no user-interaction and **does not require IT-trained Agents** when being used in operations. The FinFly USB can be used against **multiple systems** before being returned to Headquarters.

QUICK INFORMATION

Usage:

- Tactical Operations

Capabilities:

- Deploys Remote Monitoring Solution on Target

Content:

- Hardware

Usage Example 1: Technical Surveillance Unit

The FinFly USB was successfully used by **Technical Surveillance Units** in several countries to deploy a Remote Monitoring Solution onto Target Systems that were switched off, by simply **booting the system from the FinFly USB device**.

Usage Example 2: Intelligence Agency

A Source in a domestic terror group was given a FinFly USB that **secretly installed a Remote Monitoring Solution** on several computers of the group when they were using the device to exchange documents between each other. The Target Systems could then be **remotely**

Systems, Equipment,
Components (4A005)

Intrusion Software

Agent

Target

- Data Analysis
- Create Target

Administration

- Configuration
- Show Logfiles
- Agent List
- License Information

LEMF

- Data Management

Help

- About
- Online Help

- Logoff (alex)

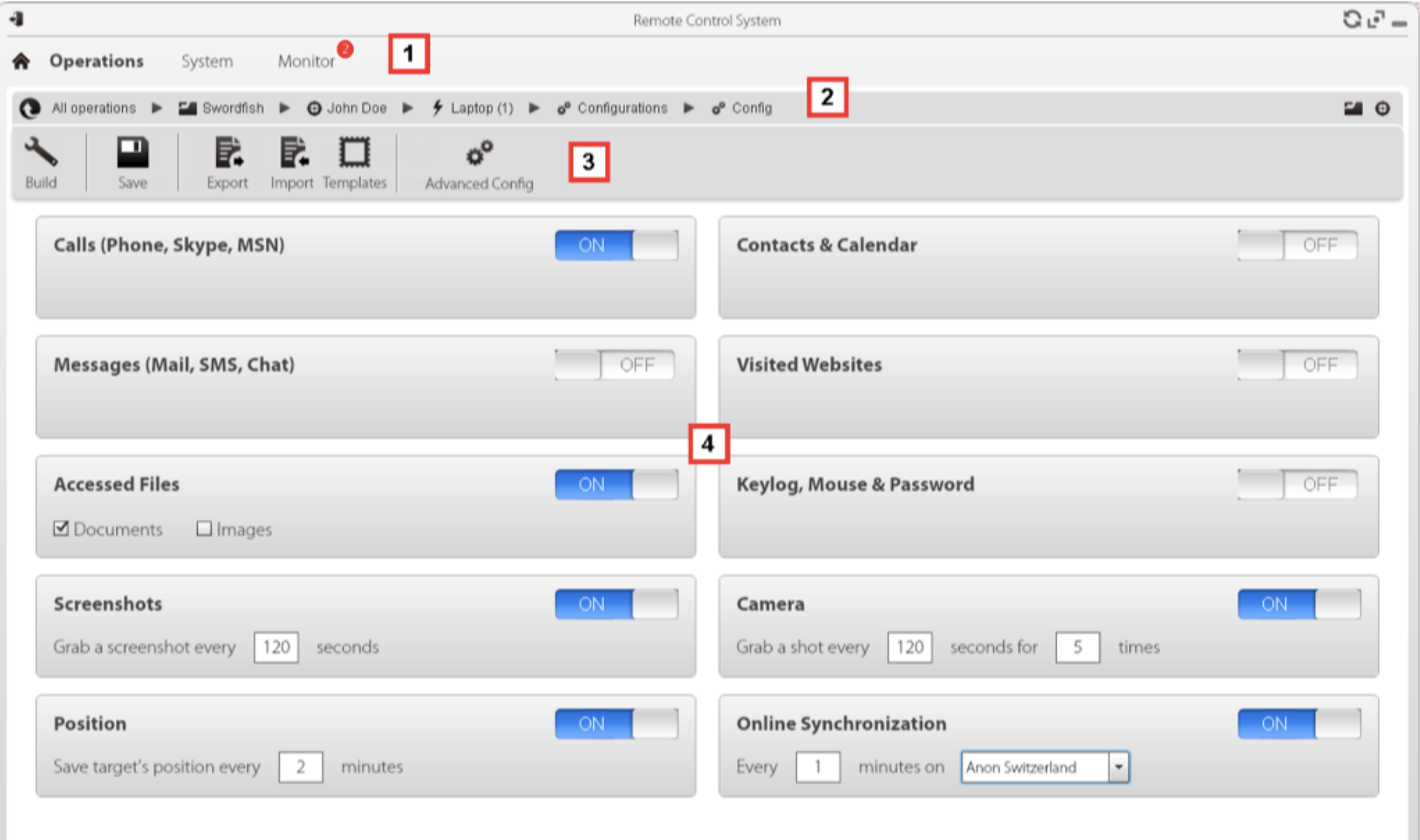
Agent Version 3.0

Target List

Name	M	T	Computer	User	Country	City	Global IP	OS	Target Time
<i>Online</i>									
demo MUC	☆	◦	FINSPYDEVEL1119	SYSTEM	Germany	Munich	87.148.207.133	Windows	2011-07-18 10
<i>Offline</i>									
TESTE DPF DF	☆	◦	WS83765	SYSTEM	Brazil	N/A	186.254.49.192	Windows	2011-06-14 20
ISS-Prague-Linux	☆	◦	ubuntu	test	Germany	Munich	87.148.218.108	Linux	2011-06-17 04
test lh	☆	◦	lh tests-MacBook.local	lh testlh test	Germany	N/A	62.153.225.34	Mac OS	2011-03-10 17
J	☆	◦	lh ubuntu	lh	Germany	N/A	62.153.225.34	Linux	0001-01-01 00
gamma-jakarta	☆	◦	GAMMA-DELL	n/a	Indonesia	Jakarta	118.99.66.72	Windows	2011-04-30 09
BigToe	☆	◦	WS12TGT	SYSTEM	Singapore	Singapore	121.6.105.53	Windows	2011-07-15 17
UK DEMO HOSDB	☆	◦	WS83765	SYSTEM	United Kingdom	N/A	188.66.91.44	Windows	2011-07-05 16
STUART II	☆	◦	STUART-PC	STUART	United Kingdom	N/A	92.6.201.131	Windows	2011-06-15 15
<i>Archived</i>									
teste2	☆	◦	ISABELLA-272349	SYSTEM	France	N/A	91.121.139.153	Windows	2011-05-12 08
Demo_B	☆	◦	FINFISHER12	finfisher	Singapore	Singapore	121.6.105.53	Windows	2011-07-15 17
test2	☆	◦	FIN-TARGET	SYSTEM	United Kingdom	N/A	188.66.91.61	Windows	2011-07-12 11

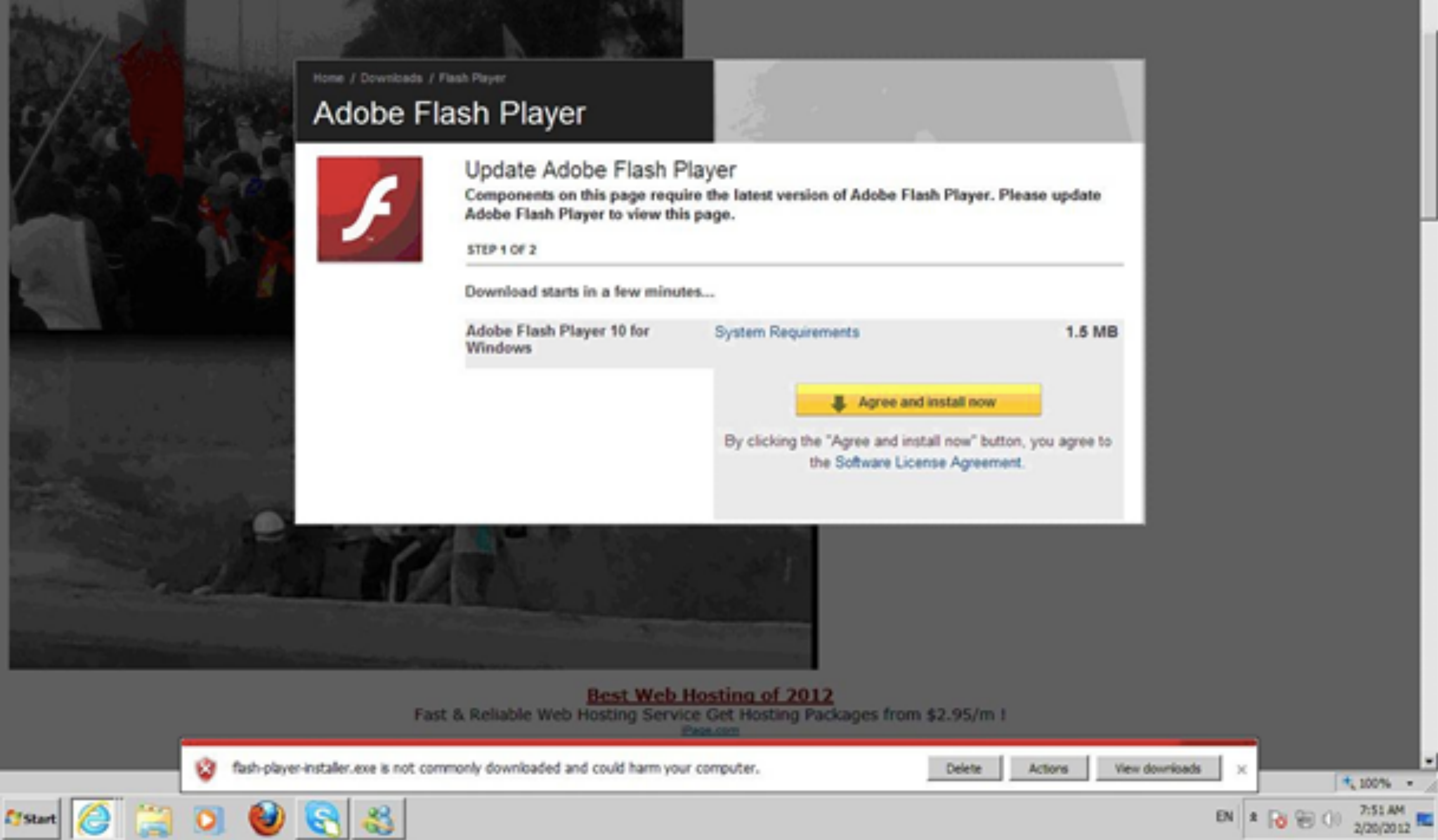
Software (4D0004)

Intrusion Software



Software (4D0004)

Intrusion Software



Software (4D0004)

Intrusion Software

VUPEN Exploits for Law Enforcement Agencies

“ Law enforcement agencies need the most advanced IT intrusion research and the most reliable attack tools to covertly and remotely gain access to computer systems. Using previously unknown software vulnerabilities and exploits which bypass Antivirus products and modern operating system protections such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) could help investigators to successfully achieve this task. ”

Chaouki Bekrar, VUPEN Security CEO

While social engineering or physical access is often used by law enforcement agencies and investigators to gain access to computer systems and install monitoring and interception tools on target PCs or mobile devices, using 0-day exploits taking advantage of previously unknown software vulnerabilities can help investigators in speeding up the process while covertly and remotely installing payloads on PCs and mobiles.

To respond to this challenge, VUPEN Exploits for Law Enforcement Agencies aim to deliver exclusive exploit codes for undisclosed vulnerabilities discovered in-house by VUPEN security researchers. This is a reliable and secure approach to help LEAs and investigators in covertly attacking and gaining access to remote computer systems.

Access to this program is restricted to Intelligence and Law Enforcement Agencies under NDA (Non-Disclosure Agreement) in countries members or partners of NATO, ANZUS and ASEAN.

Technology for
Development (4E001.c)

Intrusion Software

FINFLY EXPLOIT PORTAL

Standard Deployment methods for Remote Monitoring Solutions can **often not be applied** when dealing with **well-trained and extremely careful Targets** as they are familiar with common Deployment techniques and tools.

In most scenarios, **0-Day Exploits** provide an extremely powerful and **reliable way to deploy Remote Monitoring Solutions** by exploiting **unpatched vulnerabilities** in Software the Target is using.

The FinFly Exploit Portal offers access to **a large library** of 0-Day and 1-Day Exploits for popular software like **Microsoft® Office, Internet Explorer, Adobe Acrobat Reader, and many more.**

Usage Example 1: High-Tech Crime Unit

A High-Tech Crime Unit was **investigating a Cyber-Crime** and needed to deploy a Remote Monitoring Solution on

QUICK INFORMATION	
Usage:	· Strategic Operations
Capabilities:	· Deploys Remote Monitoring Solution on Target System through Files and Server
Content:	· Web Portal

Usage Example 2: Intelligence Agency

A Target was identified **within a Discussion Board** but no direct or Email contact was possible. The Agency created a

Technology for
Development (4E001.c)

Intrusion Software

[Home](#) › [Customer Policy](#)

Customer Policy

Since we founded Hacking Team, we have understood the power of our software in law enforcement and intelligence investigations. We also understand the potential for abuse of the surveillance technologies that we produce, and so we take a number of precautions to limit the potential for that abuse. We provide our software only to governments or government agencies. We do not sell products to individuals or private businesses. We do not sell products to governments or to countries blacklisted by the U.S., E.U., U.N., NATO or ASEAN.

We review potential customers before a sale to determine whether or not there is objective evidence or credible concerns that Hacking Team technology provided to the customer will be used to facilitate human rights violations. We fully comply with dual use and export controls called for in the nineteenth plenary meeting of the Wassenaar Arrangement. Moreover, in HT contracts, we require customers to abide by applicable law. We reserve the right in our contracts to suspend support for our software if we find terms of our contracts are violated. If we suspend support for HT technology, the product soon becomes useless. We will refuse to provide or we will stop supporting our technologies to governments or government agencies that:

- We believe have used HT technology to facilitate gross human rights abuses;
- Who refuse to agree to or comply with provisions in our contracts that describe intended use of HT software, or who refuse to sign contracts that include requirements that HT software be used lawfully;
- Who refuse to accept auditing features built into HT software that allow administrators to monitor how the system is being used.

HT policies and procedures are consistent with the U.S. Know Your Customer guidelines. We conduct ongoing employee training to assure that employees know and understand the provisions of these guidelines. Should we discover "red flags" described in these guidelines while negotiating a sale, we will conduct a detailed inquiry into the matter and raise the issue with the potential customer. If the "red flags" cannot be reasonably explained or justified, we may suspend the transaction. Our review

End User Limitations

Intrusion Software

Product name

Ahnlab Internet Security 2013
Avast Internet Security 2013
AVG Internet Security 2013
Avira Internet Security 2013
BitDefender Total Security 2013
Comodo Internet Security Pro
ESET Smart Security
F-Secure Internet Security
Kaspersky Antivirus 2013
McAfee Antivirus 2013
Microsoft Security Essential
Norman Antivirus

Invisibility

Cannot upgrade to elite
Cannot upgrade to elite
Cannot upgrade to elite

End Use Requirements

Intrusion Software



SHA256: 4ebf2fa48acb91d540c9b7b69515d5da8bbb345b5738470e026805d0c84ded52

File name: DarkComet.exe

Detection ratio: 42 / 55

Analysis date: 2015-07-19 23:21:54 UTC (3 months, 1 week ago)



[Analysis](#)
[File detail](#)
[Relationships](#)
[Additional information](#)
[Comments 2](#)
[Votes](#)

Antivirus	Result	Update
ALYac	Backdoor.RAT.DarkComet.gen	20150719
AVG	Delf.TKC	20150719
AVware	Trojan.Win32.Generic!BT	20150719
Ad-Aware	Trojan.Generic.7971032	20150719
Agnitum	Trojan.Agent2!P6ger7pkD+M	20150717
AhnLab-V3	Win-Trojan/Agent.6520320	20150719
Antiy-AVL	Trojan/Win32.Agent	20150719
Avast	Win32:Flooder-GR [Trj]	20150719
Avira	BDS/Freeze.A	20150717
Baidu-International	Adware.Win32.Agent.Elnx	20150719
ClamAV	Win.Trojan.Agent.108072	20150717

End Use Requirements

Intrusion Software

[IS !\[\]\(919a2cb85b99741a73c0c31a427236a8_img.jpg\) DETEKT FOR ME?](#)[HOW DOES IT WORK?](#)[DOWNLOAD](#)

Detekt is a free tool that scans your Windows computer for traces of FinFisher and Hacking Team RCS, commercial surveillance spyware that has been identified to be also used to target and monitor human rights defenders and journalists around the world. Read more about our [Intentions & Methods](#). Please also read the [Frequently Asked Questions](#).

In recent years we have witnessed a huge growth in the adoption and trade in communication surveillance technologies. Such spyware provides the ability to read personal emails, listen-in skype conversations or even remotely turn on a computers camera and microphone without its owner knowing about it.

**IT HAS BEEN WELL DOCUMENTED THAT
GOVERNMENTS ARE USING
SURVEILLANCE TECHNOLOGY TO
TARGET HUMAN RIGHTS DEFENDERS**

Continual Updates

Intrusion Software

Lawful Interception vs. Penetration Testing

- the system is specially suited for integration with particular Intrusion Software packages or control systems;
- the exporter maintains partnerships with Intrusion Software vendors;
- pertinent patents or sales material make reference to lawful interception or surveillance use cases;
- the system is sold as a package with Intrusion Software and whether any Intrusion Software product is reliant on the system or operation in question for operation;
- the product is primarily marketed to, or only sold to, law enforcement or intelligence agencies;
- the end recipient is a law enforcement or intelligence agency, or an entity with known relationships to such sectors, and the possible use cases for such customers;
- the primary placement or capabilities of the device would enable its end recipient the ability to tamper with public access networks.

Outside of TSU, these are end use and end user qualifications, not technical definitions.

Proposed Rule Recommendations

- Apply the Technology and Software — Unrestricted (TSU) license exception to cybersecurity software.
- Issue broad license authorizations for transfers of penetration testing software and hardware that does not qualify for license exceptions to non-governmental use and users.
- After adopting license exception TSU and broad license authorizations for non-governmental use and users, tailor the licensing process for remaining items specifically to human rights concerns regarding cybersecurity items.
- Provide guidance on the “generation” component of ECCN 4D004 to decontrol certain classes of development tools.
- Narrow the control on technology for the “development” of Intrusion Software so that it only applies to transfers to government end users or for military or law enforcement purposes.
- Issue clear guidance on key terminology introduced into the text of the rule.

Documents: <http://cda.io/>

Contact: collina@gmail.com