(Un)lawful Interception

Pascal Gloor

SwiNOG #25

07.11.2012

Agenda

Why?

Who?

How?

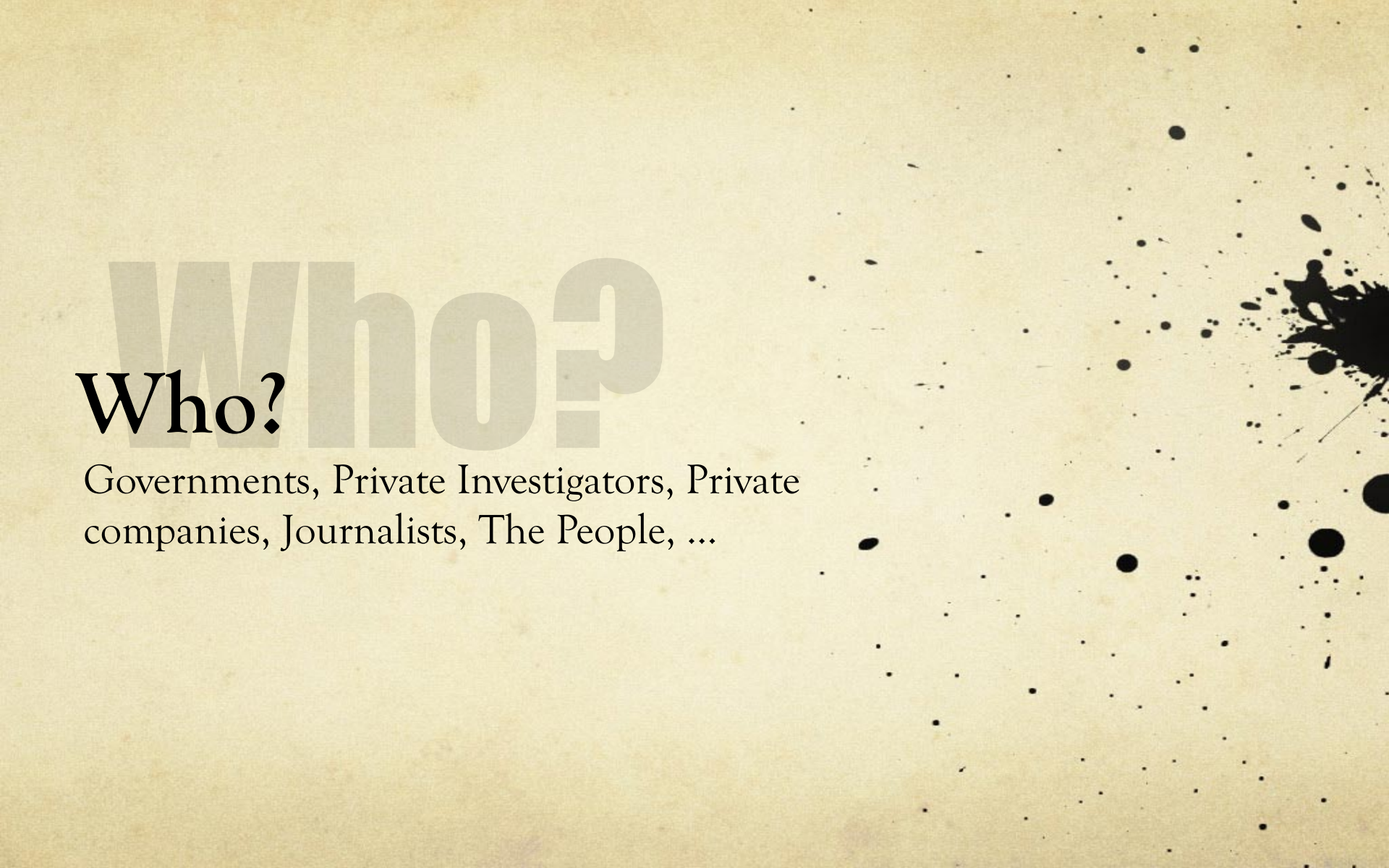
Protection?

Why?

Gather information without knowledge of the person involved, also known as “intelligence”.

Who?

Governments, Private Investigators, Private companies, Journalists, The People, ...



Governments

Governments

United Kingdom

The Regulation of Investigatory Power Act of 2000, also called RIPA, is a comprehensive surveillance law that covers everything from the use of closed-circuit TV cameras to the use of moles in criminal investigations. RIPA includes provisions that require ISPs to install systems to aid investigators in tracking electronic communications.

Governments

United States

The USA Patriot Act, enacted following the attacks of Sept. 11, 2001, made several changes to U.S. law intended to combat terrorism. It expanded the ability of law enforcement agencies to search communications, medical and financial records. It also extended the use of wiretaps to include internet connections.

Also, the Bush administration authorized the National Security Agency to conduct warrantless domestic wiretaps in 2001, possibly earlier. This was first revealed in the media in The New York Times in December 2005.

Two subsequent laws, the Protect America Act of 2007 and FISA Amendments Act of 2008, extended the NSA's authority on domestic wiretaps.

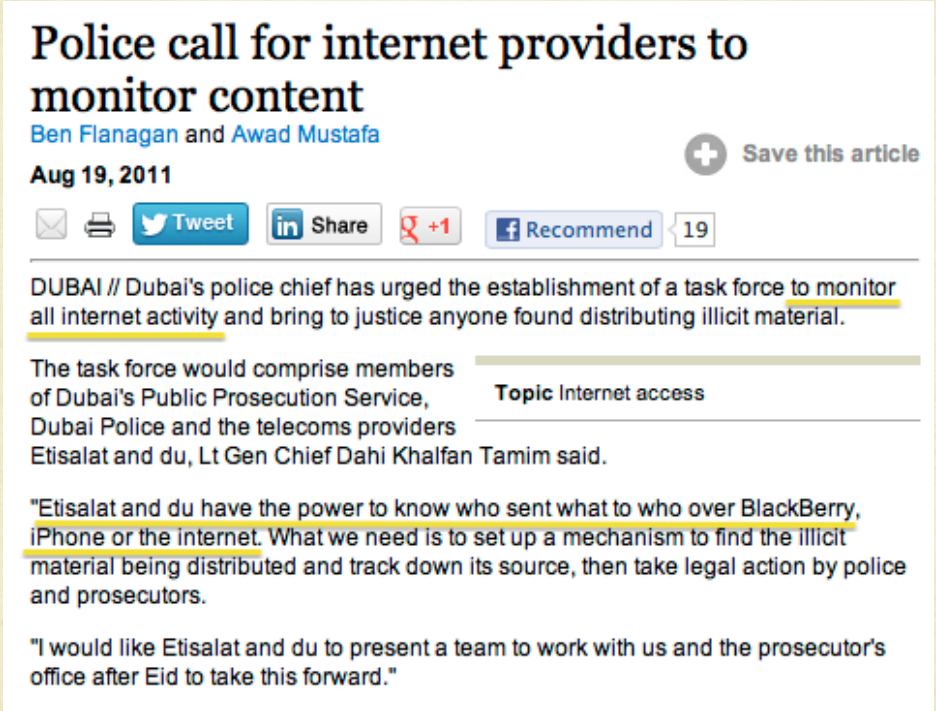
Governments

Germany

In 2006, the western German state of North-Rhine Westphalia adopted a law that gave intelligence agencies broad powers to spy on and hack into the computers of terror suspects, including infecting them with spyware viruses. Germany's highest court overturned that law in 2008, saying: "The law violates the right to privacy and is null and void."

However, the Constitutional Court also ruled that the government is allowed to conduct surveillance on internet communications in cases where it could prevent loss of life or an attack on the country. The court said agencies must get permission from a judge before they can secretly upload spyware to a suspect's computer.

Governments



Police call for internet providers to monitor content

Ben Flanagan and Awad Mustafa

Aug 19, 2011

Save this article

Tweet Share +1 Recommend 19

DUBAI // Dubai's police chief has urged the establishment of a task force to monitor all internet activity and bring to justice anyone found distributing illicit material.

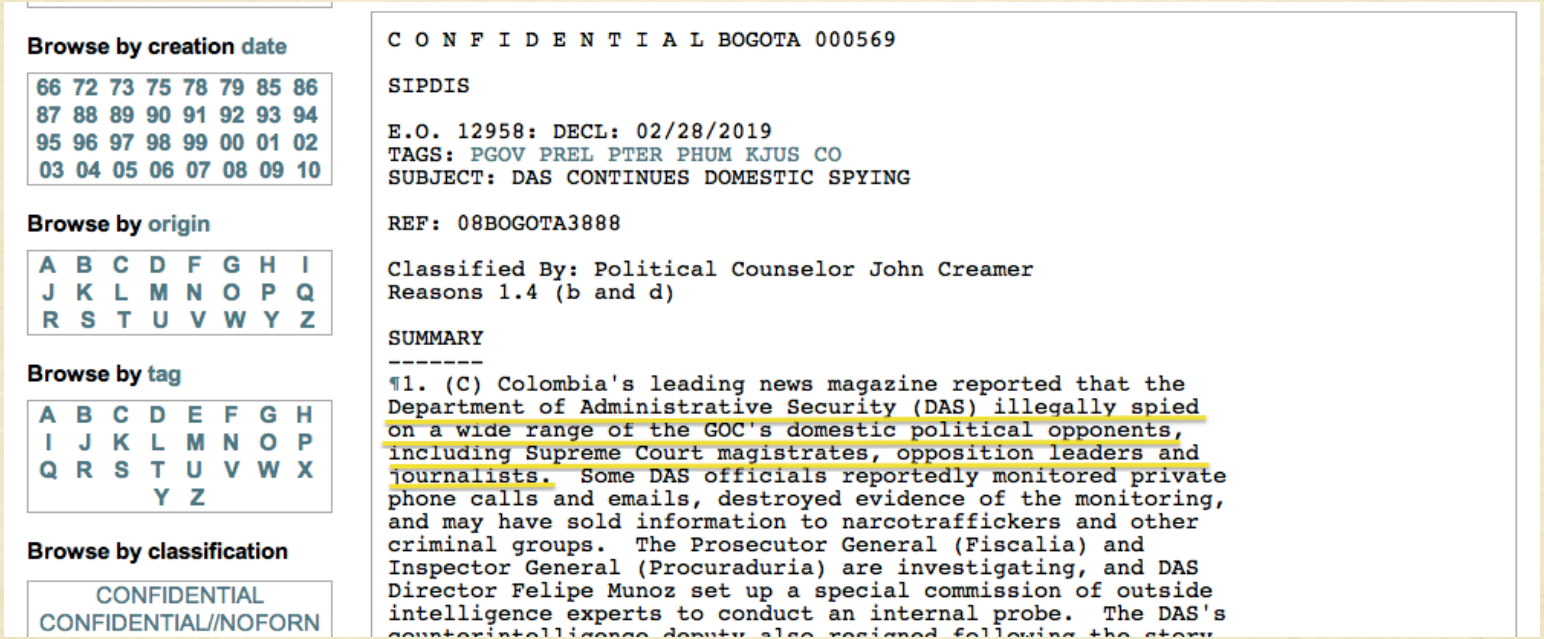
The task force would comprise members of Dubai's Public Prosecution Service, Dubai Police and the telecoms providers Etisalat and du, Lt Gen Chief Dahi Khalfan Tamim said.

Topic Internet access

"Etisalat and du have the power to know who sent what to who over BlackBerry, iPhone or the internet. What we need is to set up a mechanism to find the illicit material being distributed and track down its source, then take legal action by police and prosecutors.

"I would like Etisalat and du to present a team to work with us and the prosecutor's office after Eid to take this forward."

Governments



Browse by creation date

66 72 73 75 78 79 85 86
87 88 89 90 91 92 93 94
95 96 97 98 99 00 01 02
03 04 05 06 07 08 09 10

Browse by origin

A B C D F G H I
J K L M N O P Q
R S T U V W Y Z

Browse by tag

A B C D E F G H
I J K L M N O P
Q R S T U V W X
Y Z

Browse by classification

CONFIDENTIAL
CONFIDENTIAL//NOFORN

C O N F I D E N T I A L BOGOTA 000569

SIPDIS

E.O. 12958: DECL: 02/28/2019
TAGS: PGOV PREL PTER PHUM KJUS CO
SUBJECT: DAS CONTINUES DOMESTIC SPYING

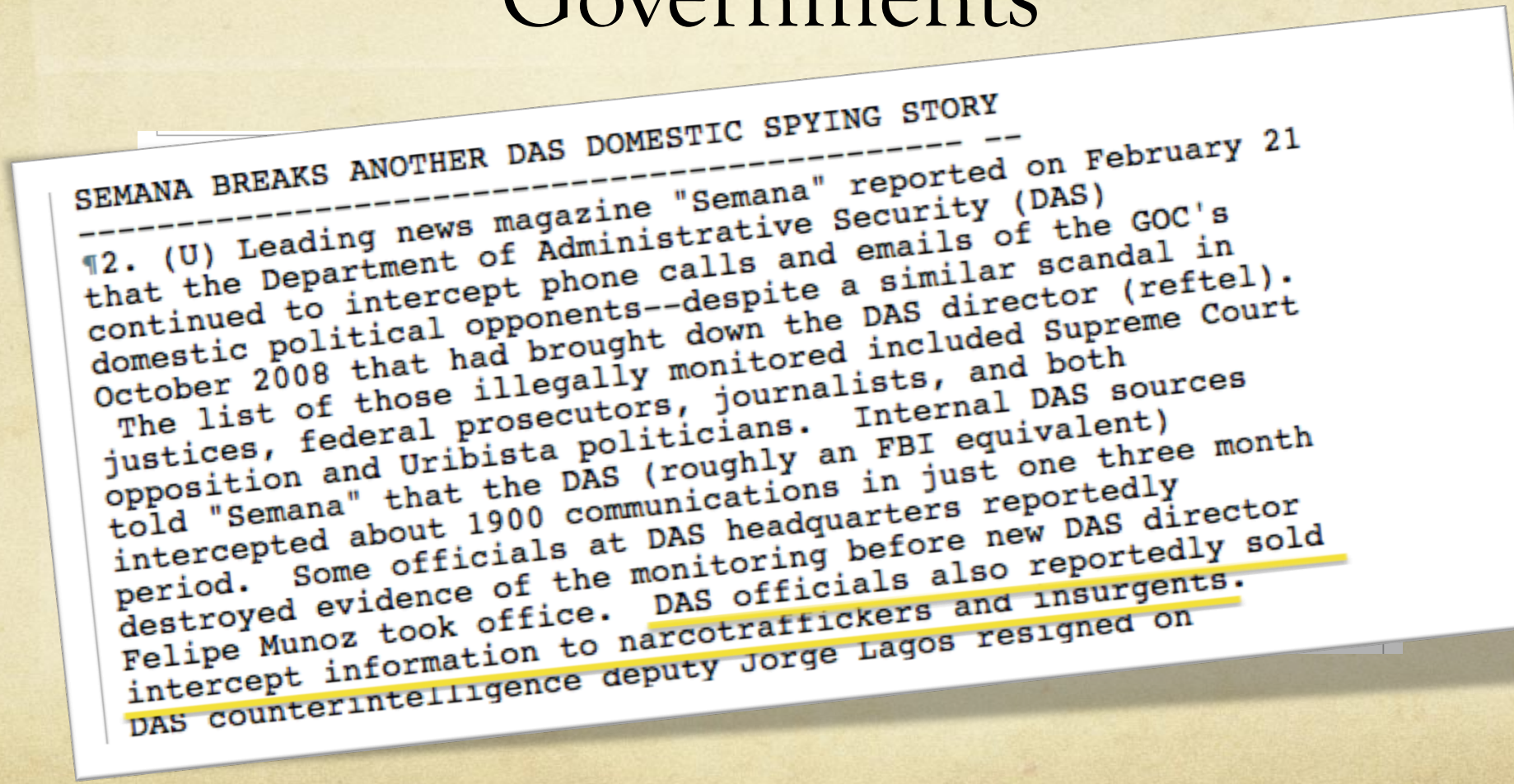
REF: 08BOGOTA3888

Classified By: Political Counselor John Creamer
Reasons 1.4 (b and d)

SUMMARY

¶1. (C) Colombia's leading news magazine reported that the Department of Administrative Security (DAS) illegally spied on a wide range of the GOC's domestic political opponents, including Supreme Court magistrates, opposition leaders and journalists. Some DAS officials reportedly monitored private phone calls and emails, destroyed evidence of the monitoring, and may have sold information to narcotraffickers and other criminal groups. The Prosecutor General (Fiscalia) and Inspector General (Procuraduria) are investigating, and DAS Director Felipe Munoz set up a special commission of outside intelligence experts to conduct an internal probe. The DAS's

Governments



SEMANA BREAKS ANOTHER DAS DOMESTIC SPYING STORY

¶2. (U) Leading news magazine "Semana" reported on February 21 that the Department of Administrative Security (DAS) continued to intercept phone calls and emails of the GOC's domestic political opponents--despite a similar scandal in October 2008 that had brought down the DAS director (reftel). The list of those illegally monitored included Supreme Court justices, federal prosecutors, journalists, and both opposition and Uribista politicians. Internal DAS sources told "Semana" that the DAS (roughly an FBI equivalent) intercepted about 1900 communications in just one three month period. Some officials at DAS headquarters reportedly destroyed evidence of the monitoring before new DAS director Felipe Munoz took office. DAS officials also reportedly sold intercept information to narcotraffickers and insurgents. DAS counterintelligence deputy Jorge Lagos resigned on

Private Investigators

Anthony Pellicano (born March 22, 1944, in Chicago, Illinois) is a former high-profile Los Angeles private investigator who recently served a sentence of three and a half years in federal prison for illegal possession of explosives, firearms and homemade grenades, and who was arrested on February 4, 2006, on unlawful wiretapping and racketeering charges.

In a subsequent six-week Federal Court trial, Pellicano was convicted of wiretapping and conspiracy to commit wiretapping.[4] Facing 78 guilty counts and not being allowed to co-serve his two convictions, Pellicano was sentenced in December 2008 to fifteen additional years in prison and ordered (with two other defendants) to forfeit $2 million.[5]

Private Companies

Exhumation ordered for Vodafone employee in wiretap scandal

A prosecutor is set to ask for the exhumation of the body of Costas Tsalikidis, the Vodafone software engineer who allegedly hung himself due to concerns about being implicated in a wiretapping scandal, sources told Kathimerini on Monday.

First instance prosecutor Haralambos Lakafosis is expected to reopen the case into the 39-year-old's death, several months after experts suggested he may have been murdered.

A court ruled in 2006 that Tsalikidis committed suicide in March 2005 because he allegedly helped hack the phone of then-Prime Minister Costas Karamanlis and more than 100 others. But the Tsalikidis family and their legal team have challenged this version of events.

Last year, coroners Theodoros Vougiouklakis and Steven Karch raised doubts in their reports about the initial autopsy.

Karch said "the most likely scenario" is that Tsalikidis "was sedated/poisoned and hung after death."

Journalists!

Murdoch shuts paper amidst wiretap scandal

KATE HOLTON AND JODIE GINSBERG, REUTERS
Friday, July 8, 2011 6:10:35 EDT AM

Recommend 0

Tweet 0

+1 0

SHARE

AA+

Report an error

LONDON, England -- In a breathtaking response to a scandal engulfing his media empire, Rupert Murdoch moved on Thursday to close down the News of the World, Britain's biggest selling Sunday newspaper.

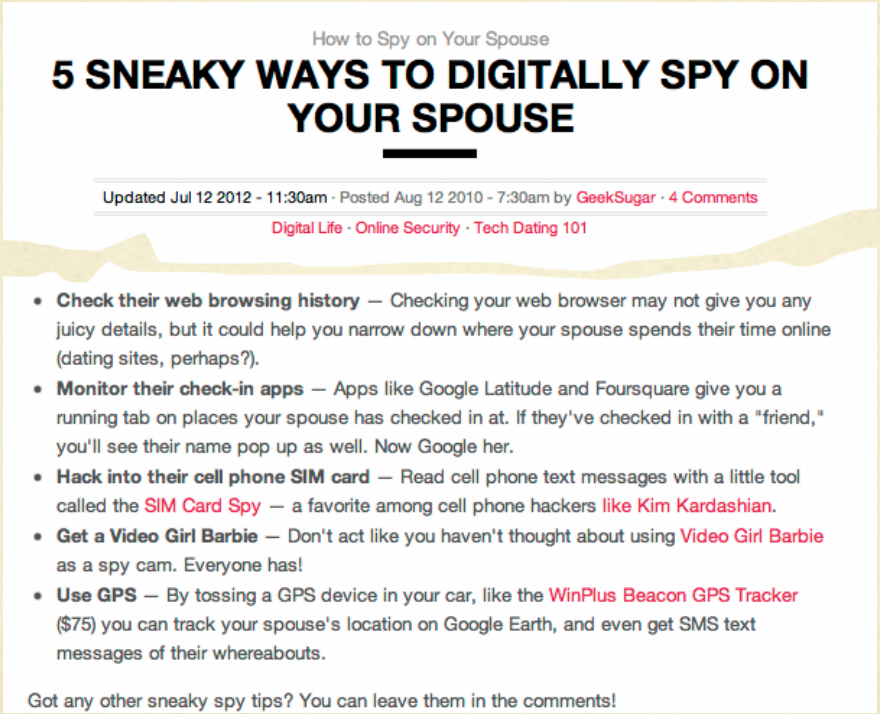
As allegations mounted this week that its journalists had hacked the voicemails of thousands of people, from child murder victims to the families of Britain's war dead, the tabloid had hemorrhaged advertising and alienated millions of readers.

Yet no one, least of all the 168-year-old paper's staff, was prepared for the drama of a single sentence that will surely go down as one of the most startling turns in the 80-year-old Australianborn press baron's long and controversial career.

"News International today announces that this Sunday, 10 July 2011, will be the last issue of the News of the World," read the preamble to a statement from Murdoch's son James, who heads the British newspaper arm of News Corp.

Hailing a fine muck-raking tradition at the paper, which his father bought in 1969, James Murdoch told its staff that the latest explosion of a long-running scandal over phone hacking by journalists had made the future of the title untenable.

The People!



How to Spy on Your Spouse

5 SNEAKY WAYS TO DIGITALLY SPY ON YOUR SPOUSE

Updated Jul 12 2012 - 11:30am · Posted Aug 12 2010 - 7:30am by GeekSugar · 4 Comments

Digital Life · Online Security · Tech Dating 101

- **Check their web browsing history** — Checking your web browser may not give you any juicy details, but it could help you narrow down where your spouse spends their time online (dating sites, perhaps?).
- **Monitor their check-in apps** — Apps like Google Latitude and Foursquare give you a running tab on places your spouse has checked in at. If they've checked in with a "friend," you'll see their name pop up as well. Now Google her.
- **Hack into their cell phone SIM card** — Read cell phone text messages with a little tool called the SIM Card Spy — a favorite among cell phone hackers like Kim Kardashian.
- **Get a Video Girl Barbie** — Don't act like you haven't thought about using Video Girl Barbie as a spy cam. Everyone has!
- **Use GPS** — By tossing a GPS device in your car, like the WinPlus Beacon GPS Tracker ($75) you can track your spouse's location on Google Earth, and even get SMS text messages of their whereabouts.

Got any other sneaky spy tips? You can leave them in the comments!

Legal Matrix

Who?	Legal?
Governments	they define it!
Private investigators	
Private companies	
Journalists	
The People	

How?

Trojans, IMSI catcher, Physical tapping, ...

GSM – IMSI Catcher

- Man-in-the-middle by signal injection (fake GSM antenna)
- Short range localization (<1500m)
- Can also be useful in disaster search for people ☺

GSM – IMSI Catcher

1. Document-case variant

While operating the finder it is necessary to connect it to the antenna connector of the corresponding range. Rotating the antenna right or left will help to achieve the

2. Body worn variant

While operating the GSM finder the operator fixes the antenna on the breast or on waist in front. Turning to the right or to the left will achieve maximum signal

GSM – Network hacking

Greek wiretapping case 2004–05 [edit]

Main article: Greek wiretapping case 2004–2005

The **Greek wiretapping case of 2004-05**, also referred to as **Greek Watergate**,[15] involved the illegal tapping of more than 100 mobile phones on the Vodafone Greece network belonging mostly to members of the Greek government and top-ranking civil servants. The taps began sometime near the beginning of August 2004 and were removed in March 2005 without discovering the identity of the perpetrators.

In order to carry out the wiretapping, the intruders installed a rootkit that targeted Ericsson's AXE telephone exchange. According to IEEE Spectrum, this was "the first time a rootkit has been observed on a special-purpose system, in this case an Ericsson telephone switch."[16] The rootkit was designed to patch the memory of the exchange while it was running, enable wiretapping whilst disabling audit logs, patch the commands that list active processes and active data blocks, and modify the data block checksum verification command. A backdoor allowed an operator with sysadmin status to deactivate the exchange's transaction log and alarms, and access commands related to the surveillance capability.[16] The rootkit was discovered after the intruders installed a faulty update, which caused SMS texts to be undelivered, leading to an automated failure report being generated. Ericsson engineers were called in to investigate the fault, and at this point discovered the hidden data blocks containing the list of phone numbers being monitored, along with the rootkit and illicit monitoring software that had been installed.

Spyware (PC)

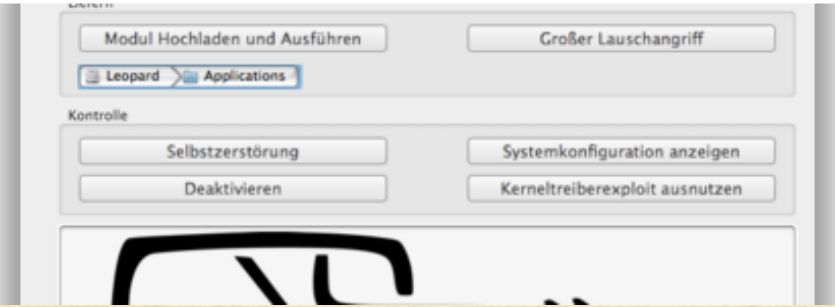
- Used in many countries
- Usually for Skype wiretapping
- But not only…
  - USB device activation (Microphone, Camera, Mobile?)
  - File copy
  - Network sniffing

Spyware (PC)

Chaos Computer Club analyzes government malware

2011-10-08 19:00:00, admin

The largest European hacker club, "Chaos Computer Club" (CCC), has reverse engineered and analyzed a "lawful interception" malware program used by German police forces. It has been found in the wild and submitted to the CCC anonymously. The malware can not only siphon away intimate data but also offers a remote control or backdoor functionality for uploading and executing arbitrary other programs. Significant design and implementation flaws make all of the functionality available to anyone on the internet.



Spyware (Smartphones)

- Used in many countries (Middle-East, Asia)
- International movement tracking
- Instant voice, SMS, MMS, … tapping
- Data copy (Address Book, Calendar, Email, …)

Spyware (Smartphones)

LA POLICE VEUT INFILTRER LES SMARTPHONES

MOUCHARD La police vaudoise fait développer en secret une panoplie du parfait cyberespion. Problème: il n'existe pas encore de base légale solide pour l'utiliser.

Après avoir infiltré à distance l'ordinateur d'un pédophile avec un logiciel espion, la police cantonale aimerait traquer les criminels via leurs téléphones portables. En secret, elle a mandaté la Haute Ecole d'ingénierie et gestion du canton de Vaud (HEIG-VD), afin que ses étudiants développent des chevaux de Troie pour smartphones. Au menu: espionnage des appels, des SMS et des données de géolocalisation. Les mandats sont pour la plupart confidentiels, et l'école se refuse de révéler qui est à la source.

Des recoupements accréditent l'implication de la police de sûreté vaudoise, ce qu'elle confirme à la demande du «Matin»: «Nous avons développé des partenariats avec plusieurs hautes écoles du canton, notamment avec la HEIG-VD, pour répondre à nos besoins et anticiper les développements, il précise que les recherches n'ont pas pour l'instant abouti à des outils utilisables. «Mais je n'exclus pas des applications concrètes à l'avenir», conclut-il.

«Projet Argos»

Les recherches menées à Yverdon pour la police sont rassemblées sous le nom de code «projet Argos». Concrètement, un premier travail de diplôme a permis de réaliser un prototype fonctionnel de sonde pour espionner les téléphones utilisant le système Symbian, qui équipe principalement les appareils Nokia. Un autre travail s'est appliqué à infiltrer les smartphones tournant sous Android (HTC, Samsung, Motorola). L'école projette également de développer une sonde pour iPhone.

Antenne GSM pirate

Parallèlement à ces chevaux de Troie, aussi appelés Trojan, un étudiant a travaillé sur la manière capturer les identités des utilisateurs de téléphones mobiles se trouvant dans son rayon d'action. Les appareils se connectent d'abord à cette borne parasite, avant d'être redirigés vers le réseau de leur opérateur habituel. L'utilisateur ne remarque rien. Mais, au passage, le logiciel peaufiné par la HEIG-VD enregistre le numéro d'identification (ou IMSI) des cartes SIM «attrapées» par l'antenne pirate. Il est ensuite possible de connaître l'identité des utilisateurs piégés. La condition pour travailler sur le projet? Avoir un casier judiciaire vierge.

Plus vite que la musique?

Même sans application concrète, les recherches de la police vaudoise irritent les défenseurs de la vie privée. «C'est du piratage cautionné par la police! Ça ne va pas du tout, dénonce Sébastien Fanti, avocat spécialisé dans les nouvelles technologies. Détourner la sécurité des lors qu'il s'agit de mesures de contrainte par nature intrusives. On peut faire confiance à la police, mais il ne faut pas lui laisser un champ d'investigation trop vaste.

> **«Nous avons développé des partenariats pour anticiper les développements technologiques»**
> Jean-Christophe Sauterel, porte-parole de la police vaudoise

Tout cela doit être strictement encadré, d'autant que les procureurs ont tendance à multiplier les surveillances.»

Une loi pour dissiper les doutes

Le Conseil fédéral devrait, ces prochaines semaines, approuver la révision de la loi sur la surveillance de la correspondance par poste et té-

LES CONDITIONS POUR ÊTRE MIS SOUS SURVEILLANCE

- Il faut faire l'objet d'une enquête pénale
- Avoir commis un crime grave (meurtre, viol, prise d'otage, infraction sévère à la loi sur les stupéfiants, etc.)
- La surveillance est ordonnée par le mi-

L'EXPERT

Sabine Papaloni

OLIVIER GUÉNIAT
Commandant de la police jurassienne

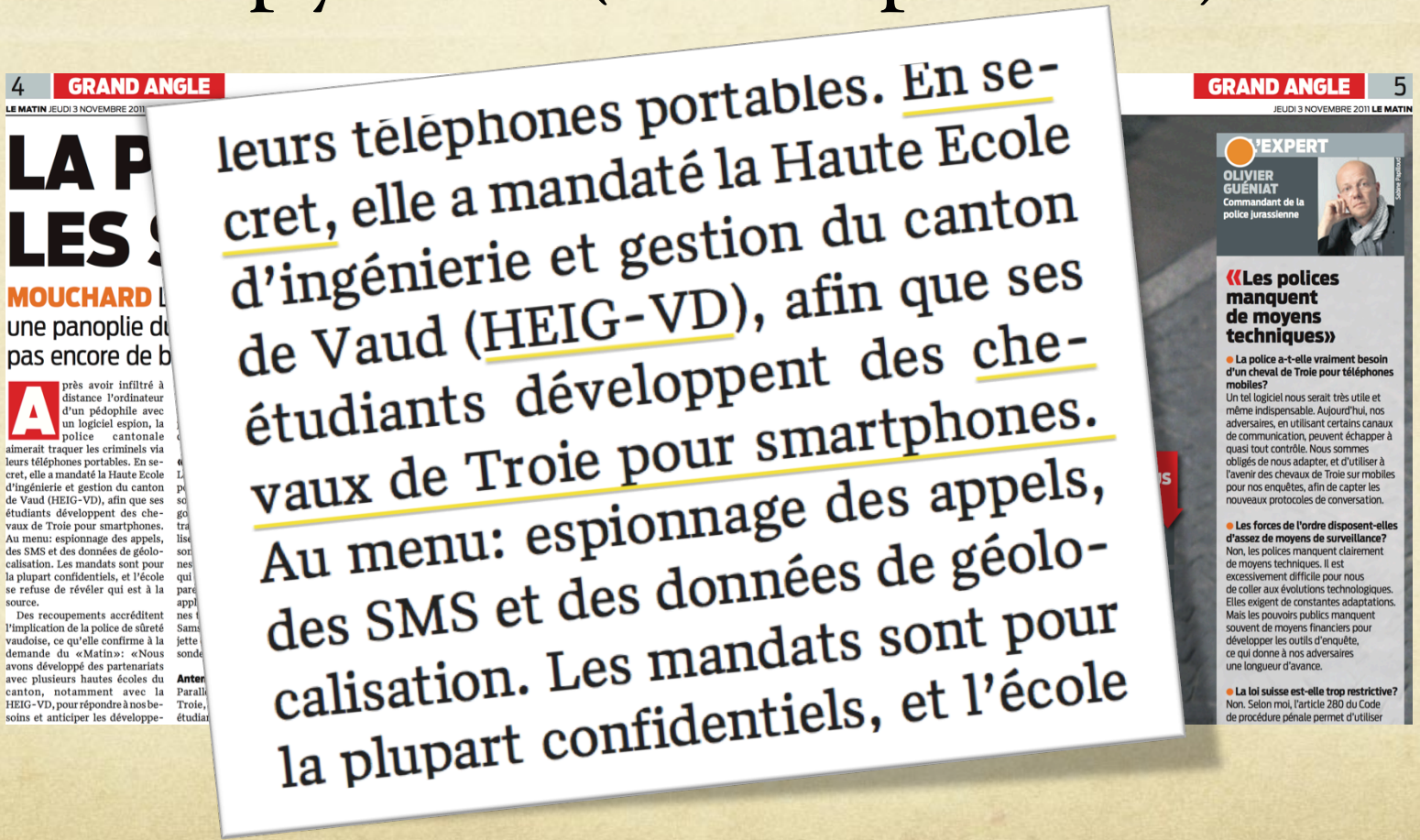
«Les polices manquent de moyens techniques»

La police a-t-elle vraiment besoin d'un cheval de Troie pour téléphones mobiles?
Un tel logiciel nous serait très utile et même indispensable. Aujourd'hui, nos adversaires, en utilisant certains canaux de communication, peuvent échapper à quasi tout contrôle. Nous sommes obligés de nous adapter, et d'utiliser à l'avenir des chevaux de Troie sur mobiles pour nos enquêtes, afin de capter les nouveaux protocoles de conversation.

Les forces de l'ordre disposent-elles d'assez de moyens de surveillance?
Non, les polices manquent clairement de moyens techniques. Il est excessivement difficile pour nous de coller aux évolutions technologiques. Elles exigent de constantes adaptations. Mais les pouvoirs publics manquent souvent de moyens financiers pour développer les outils d'enquête, ce qui donne à nos adversaires une longueur d'avance.

La loi suisse est-elle trop restrictive?
Non. Selon moi, l'article 280 du Code de procédure pénale permet d'utiliser

Spyware (Smartphones)



4 GRAND ANGLE

LE MATIN JEUDI 3 NOVEMBRE 2011

LA P
LES

MOUCHARD
une panoplie d
pas encore de b

Après avoir infiltré à distance l'ordinateur d'un pédophile avec un logiciel espion, la police cantonale aimerait traquer les criminels via leurs téléphones portables. En secret, elle a mandaté la Haute Ecole d'ingénierie et gestion du canton de Vaud (HEIG-VD), afin que ses étudiants développent des chevaux de Troie pour smartphones. Au menu: espionnage des appels, des SMS et des données de géolocalisation. Les mandats sont pour la plupart confidentiels, et l'école se refuse de révéler qui est à la source.

Des recoupements accréditent l'implication de la police de sûreté vaudoise, ce qu'elle confirme à la demande du «Matin»: «Nous avons développé des partenariats avec plusieurs hautes écoles du canton, notamment avec la HEIG-VD, pour répondre à nos besoins et anticiper les développe-

leurs téléphones portables. En secret, elle a mandaté la Haute Ecole d'ingénierie et gestion du canton de Vaud (HEIG-VD), afin que ses étudiants développent des chevaux de Troie pour smartphones. Au menu: espionnage des appels, des SMS et des données de géolocalisation. Les mandats sont pour la plupart confidentiels, et l'école

GRAND ANGLE 5

JEUDI 3 NOVEMBRE 2011 LE MATIN

L'EXPERT

OLIVIER GUÉNIAT
Commandant de la police jurassienne

Sabine Papaloizos

«Les polices manquent de moyens techniques»

La police a-t-elle vraiment besoin d'un cheval de Troie pour téléphones mobiles?
Un tel logiciel nous serait très utile et même indispensable. Aujourd'hui, nos adversaires, en utilisant certains canaux de communication, peuvent échapper à quasi tout contrôle. Nous sommes obligés de nous adapter, et d'utiliser à l'avenir des chevaux de Troie sur mobiles pour nos enquêtes, afin de capter les nouveaux protocoles de conversation.

Les forces de l'ordre disposent-elles d'assez de moyens de surveillance?
Non, les polices manquent clairement de moyens techniques. Il est excessivement difficile pour nous de coller aux évolutions technologiques. Elles exigent de constantes adaptations. Mais les pouvoirs publics manquent souvent de moyens financiers pour développer les outils d'enquête, ce qui donne à nos adversaires une longueur d'avance.

La loi suisse est-elle trop restrictive?
Non. Selon moi, l'article 280 du Code de procédure pénale permet d'utiliser

Systematic Internet tapping

- Single operator (Monopoly)
- Single carrier (Monopoly but free “access” market)
- Unlikely in free markets
- Technologies / “Features”
  - User activity logging
  - Content blocking
  - Injection proxy

Injection proxy

- Web content injection
  - Javascript injection on login pages
- PC Spyware injection
  - Usually in software updates
    - ~~Microsoft Updates~~ (now signed, hashed)
    - Apple updates
    - Common software updates (Flash, PDF reader, ...)
- Smartphones Spyware injection

Injection WITH SSL

Issuance of fraudulent certificates [edit]

On July 10, 2011, a wildcard certificate was issued by DigiNotar's systems for Google by an attacker with access to their systems. This certificate was subsequently used by unknown persons in Iran to conduct a man-in-the-middle attack against Google services.[12][13] On August 28, 2011, certificate problems were observed on multiple Internet service providers in Iran.[14] The fraudulent certificate was posted on pastebin.[15] According to a subsequent news release by VASCO, DigiNotar had detected an intrusion into its certificate authority infrastructure on July 19, 2011.[16] DigiNotar did not publicly reveal the security breach at the time.

After this certificate was found, DigiNotar belatedly admitted dozens of fraudulent certificates had been created, including certificates for the domains of Yahoo!, Mozilla, WordPress and The Tor Project.[17] DigiNotar could not guarantee all such certificates had been revoked.[18] Google blacklisted 247 certificates in Chromium,[19] but the final known total of misissued certificates is at least 531.[20] Investigation by F-Secure also revealed that DigiNotar's website had been defaced by Turkish and Iranian hackers in 2009.[21]

Injection proxy

In many real-life operations, physical access to in-country Target Systems cannot be achieved and covert **remote installation** of a Remote Monitoring Solution is required to be able to **monitor the Target from within the Headquarters.**

FinFly ISP is a strategic, **countrywide, as well as a tactical** (mobile) solution that can be **integrated into an ISP's Access and/or Core Network** to remotely install the Remote Monitoring Solution on selected Target Systems.

FinFly ISP appliances are based on **carrier grade server technology,** providing the maximum **reliability and scalability** to meet almost every challenge related to network topologies. A wide-range of Network Interfaces – all **secured with bypass functions** – are available for the required active network connectivity.

Several passive and active methods of Target Identification – from **online monitoring** via passive tapping to **interactive communications** between FinFly ISP and the AAA-Servers – ensure that the Targets are identified and their appropriate traffic is provided for the infection process.

FinFly ISP is able to **infect Files** that are downloaded by the Target **on-the-fly** or infect the Target by **sending fake Software Updates** for popular Software. The new release now integrates Gamma's powerful remote infection application **FinFly Web** to infect Targets on-the-fly by just **visiting any website.**

QUICK INFORMATION	
Usage:	- Strategic Operations
Capabilities:	- Deploys Remote Monitoring Solution on Target System through ISP Network
Content:	- Hardware/Software

Usage Example: Intelligence Agency

FinFly ISP was deployed in the main Internet Service Provider networks of the country and was actively used to remotely deploy a Remote Monitoring Solution on Target Systems. As the Targets have Dynamic IP DSL Accounts, they are identified with their Radius Logon Name.

[redacted]

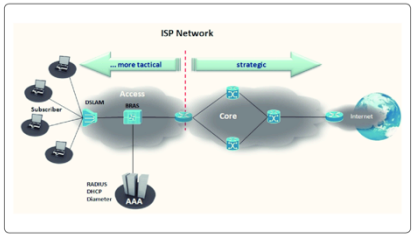
WWW.GAMMAGROUP.COM

FINFISHER™
IT INTRUSION

Remote Monitoring & Infection Solutions
FINFLY ISP

Different Location Possibilities

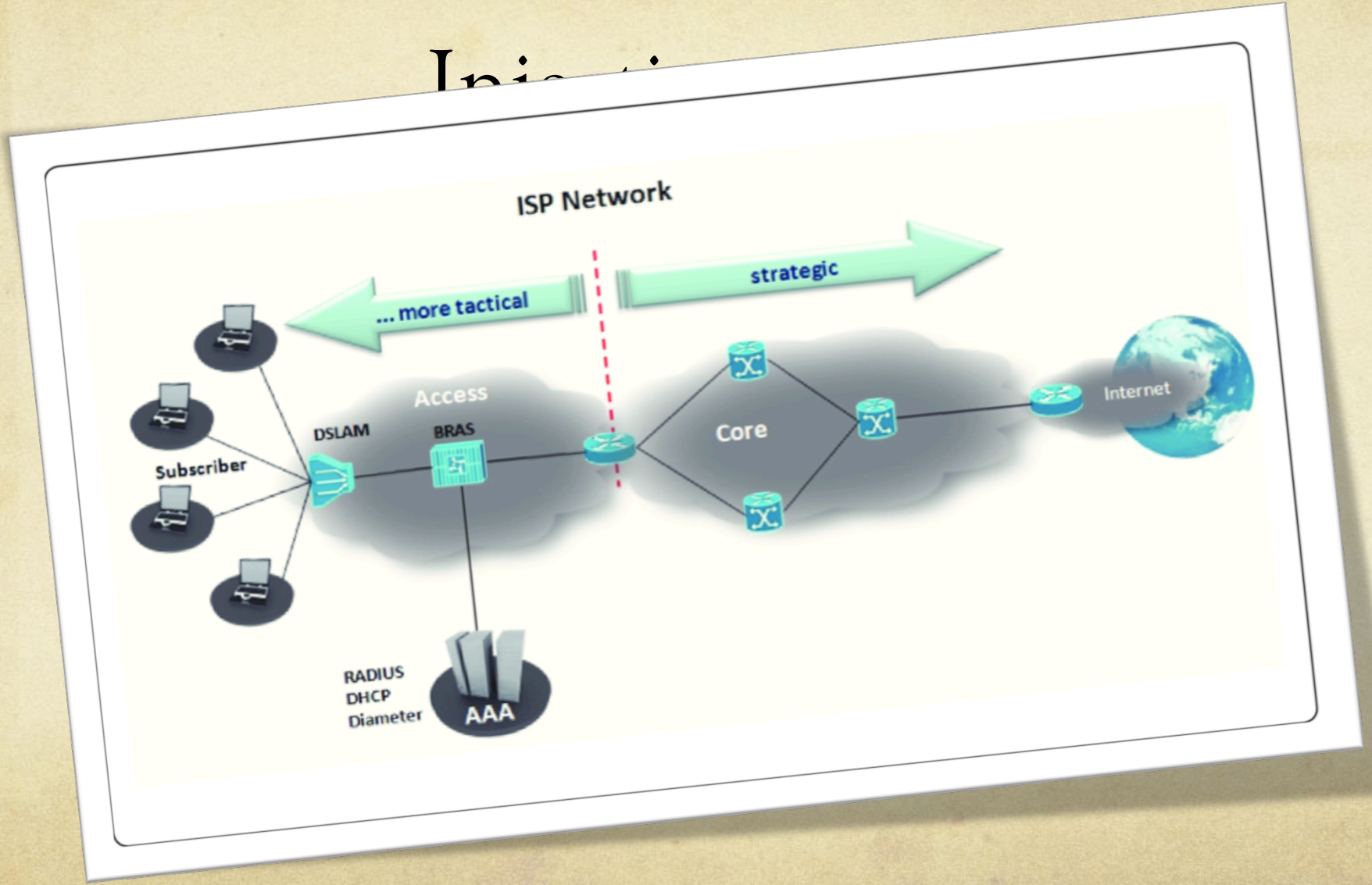
- FinFly ISP can be used as a tactical or strategic solution within ISP networks



A tactical solution is mobile and the hardware is dedicated to the infection tasks inside the access network close to the targets' access points. It can be deployed on a short-term basis to meet tactical requirements focused on either a specific target or a small number of targets in an area.

A strategic solution would be a permanent ISP/countrywide installation of FinFly ISP to select and infect any target from the remote headquarters without the need for the LEA to be on location.

Of course, it is possible to combine tactical and strategic solutions to reach a maximum of flexibility for the infection operations.

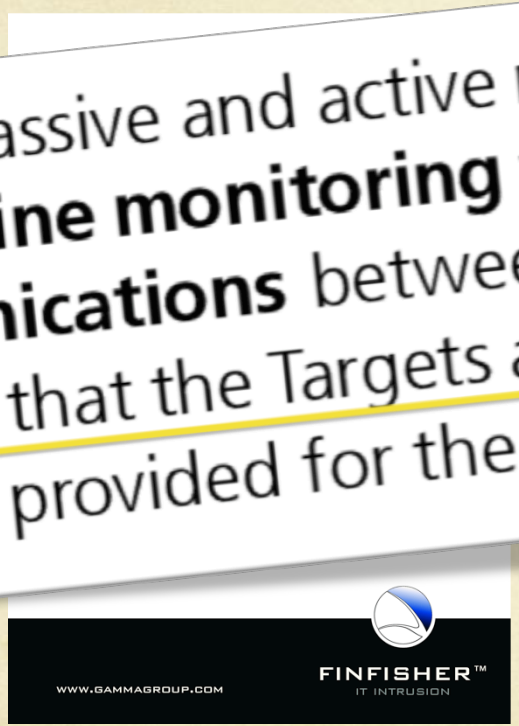

ISP Network
... more tactical
strategic
Access
DSLAM
BRAS
Subscriber
Core
Internet
RADIUS
DHCP
Diameter
AAA

Injection proxy

FinFly ISP appliances are based on **carrier grade server technology,** providing the maximum **reliability and scalability** to meet almost every challenge related to network topologies. A wide-range of Network Interfaces – all **secured with bypass functions** – are available for the required active network connectivity.

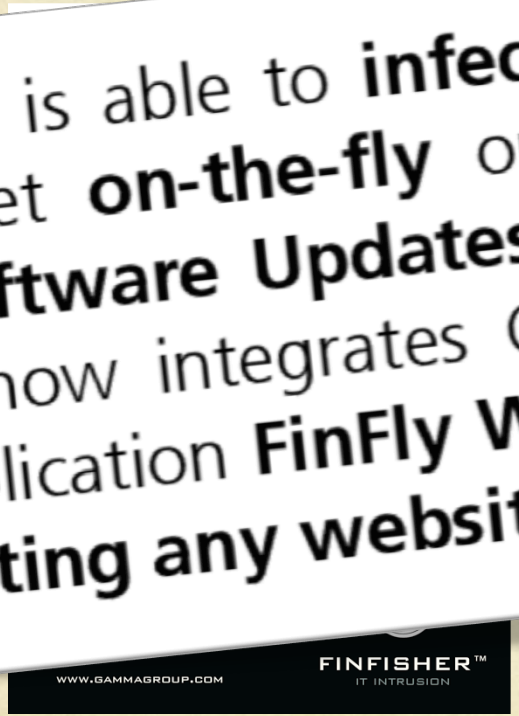
Injection proxy

Several passive and active methods of Target Identification – from **online monitoring** via passive tapping to **interactive communications** between FinFly ISP and the AAA-Servers – ensure that the Targets are identified and their appropriate traffic is provided for the infection process.



Injection proxy

FinFly ISP is able to **infect Files** that are downloaded by the Target **on-the-fly** or infect the Target by **sending fake Software Updates** for popular Software. The new release now integrates Gamma's powerful remote infection application **FinFly Web** to infect Targets on-the-fly by just **visiting any website.**



Physical “injection”

- Spyware might be injected manually while you’re busy…
  - … being interrogated for no valid reason
  - …

Protection?

Should I protect myself?

Personal protection

- During business travel or vacations to “some” countries you should…
  - “Clean” the devices you bring with you;
  - Use a strong encrypted VPN to a trusted place;
  - Use WDE on your laptop;

Business protection

- If you MUST implement LI solutions…
  - … choose CAREFULLY your partner
  - … don’t give any third party full control
  - … limit strictly access to LI systems
  - … inspect the systems regulary

WARNING !!!

Sneaky Marketing Slide!!!!

The End

Questions?