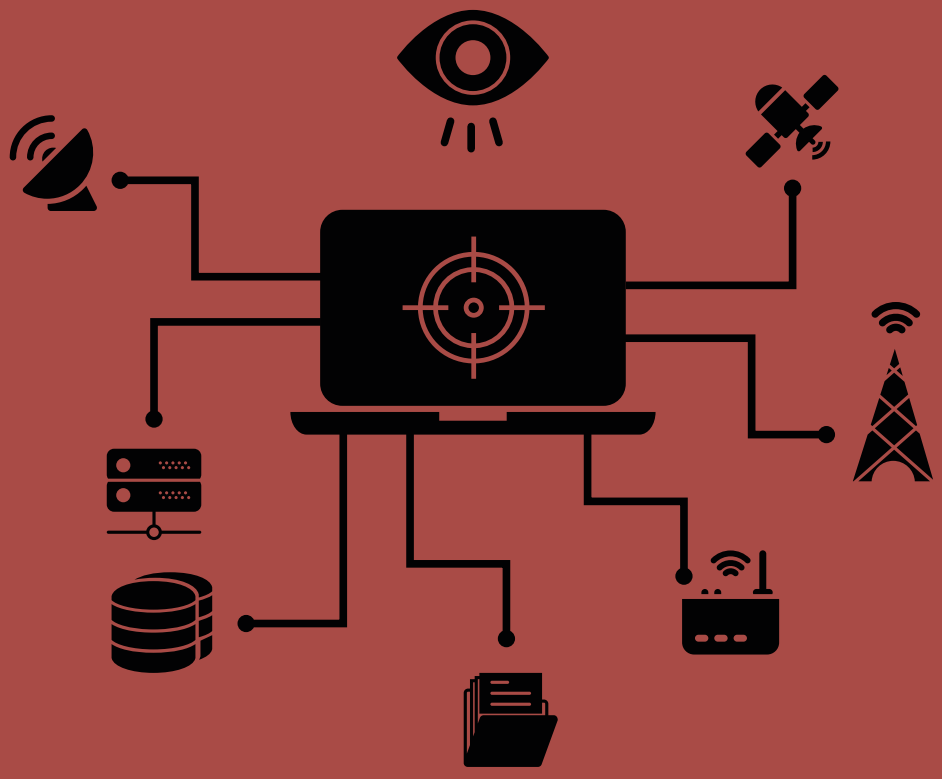
PRIVACY INTERNATIONAL

OPEN SEASON

Building Syria's Surveillance State



Acknowledgements

Privacy International acknowledges the many individuals and organisations with whom we spoke who cannot be named.

This report is primarily based on original documentation provided in confidence to Privacy International and interviews conducted by Privacy International.

Privacy International is solely responsible for the content of this report.

OPEN SEASON

Building Syria's Surveillance State

December 2016

PRIVACY INTERNATIONAL

www.privacyinternational.org

Table of Contents

Acronyms	5
Executive Summary	6
Building Syria's Surveillance State	8
Friends and middlemen	11
To capture, collect, analyse and store — in 'Country 4'	14
Filtering 'propaganda mail'	16
Monitoring the international exchanges in 'Lion country'	18
Satellite internet monitoring	21
Israel and geopolitics in the surveillance industry	23
War, Sanctions and Export Restrictions	26
The Hustle	30
Libya: a cash cow	32
Aftermath	34
Conclusion	36
Annex 1	38
Annex 2	43
Annex 3	46
Annex 4	48
Annex 5	49
Annex 6	68
Annex 7	70
Annex 8	73
Annex 9	75
Annex 10	77
Annex 11	79
Annex 12	80

List of Acronyms

DDOS	Distributed Denial of Service
ISP	Internet Service Provider
LIMS	Lawful Interception Management System (Utimaco)
PDN	Public Data Network
SCT	Syrian Communication Technology
STE	Syrian Telecommunications Establishment

Executive Summary

The Arab Spring of 2011 changed the political landscape of the Middle East and Gulf region. The scale of the popular uprisings seemingly caught off guard the governments of Syria, Egypt, and Libya among others, leading to brutal crackdowns and civil wars and instability that continue to this day.

Yet in the years leading up to this crisis, these governments spent millions of dollars developing sophisticated surveillance systems that they deployed against their citizens. PI obtained hundreds of original documents and pieces of correspondence related to the surveillance trade in this region leading up to and during the Arab Spring. Among these documents in particular is evidence of the Syrian government's ambitious plans and projects to monitor the national communications infrastructure, the technical details of which are revealed for the first time.

From 2007-2012, Syrian government built nationwide communications monitoring systems through at least four ambitious projects. Western businesses including RCS SpA (Italy) and VASTech (South Africa) were important contributors to Syria's repressive surveillance state while others including Amesys (France) competed for the opportunities on offer.

This report focuses as well on the vital role of middleman companies in the surveillance trade. These companies act primarily as resellers, brokers, logistics coordinators, and intermediaries between the surveillance technology manufacturers and their clients. They court and secure clients on the ground, smooth over logistical difficulties, and provide other services for a percentage of the total project. This report closely examines one such company, Dubai-based Advanced German Technology (AGT)[1], in enabling the construction of surveillance systems in Syria and further afield in the decade leading up to the Arab Spring revolts of 2011 and 2012.

In one transaction from 2008 and 2009, AGT in partnership with RCS proposed the use of US-origin equipment in a project to intercept communications on the networks of a satellite internet service provider, Aramsat, according to documents analysed by Privacy International. US sanctions and export control regulations in force at the time of this project restricted the exportation or re-exportation of certain US-origin goods to the country, including communications interception equipment. AGT claim that the project was never completed and that it follows all UN and EU export regulations. AGT's full response is included as an annex. RCS provided no comment related to the statements in the report.

1 'AGT' in this report refers to the Dubai-incorporated Advanced German Technology FZ-LLC through which the company conducts almost all of its business, rather than Berlin-based Advanced German Technology GmbH.

The Syrian government of president Bashar Al-Assad was intensifying its repression against dissidents and opposition groups at the same time as it was consolidating its surveillance capacities. Surveillance by both human and technological means was an important contributor to the repression that culminated in the 2011 crisis and ensuing civil war. To date, Al-Assad's government reportedly continues to maintain control over access to the internet and broadband and some of the surveillance architecture from these projects remains in place. The roles of several Western companies including AREA SpA (Italy) and Qosmos (France) who have been identified as selling surveillance technology to Syria have been the subject of inquiries in the US and France, respectively.

Other regional governments further afield engaged in repression of domestic political dissent also purchased similar technologies. AGT facilitated a particularly lucrative contract for the Libyan government of Colonel Muammar Gaddafi on behalf of South African surveillance company VASTech through consultants and companies. Funds from this project, among the most profitable for the company,[2] financed much of AGT's affairs. The lead up to the Arab Spring was open season for surveillance companies – they provided technologies to eager government clients widely known to be publicly engaged in repression. They should share some responsibility for how their technologies are used.

Privacy International calls on export authorities to condition all exports of the surveillance technologies discussed in this report on rigorous, independent human rights impact assessments so as to minimize the potential that these technologies will be abused.

[2] Between 2005 and 2012.

Building Syria's surveillance state

The Syrian government commissioned its first nationwide monitoring system in 1999. The system, commissioned by the Syrian Telecommunications Establishment (STE), was designed to monitor mobile and fixed-line telephony and internet.[3]

TELECOMMUNICATIONS IN SYRIA

Two companies provide the country's mobile services – Syriatel and the Syrian subsidiary of South African-owned MTN. Syriatel is locally owned – one of its main investors and its CEO is businessman Rami Makhlouf, a cousin of President Bashar al Assad[4]. MTN is a subsidiary of MTN of South Africa.[5] Internet penetration is relatively low, reportedly at 28%.[6] Many Syrians use internet cafes, where service is provided by around a dozen local internet service providers (ISPs).[7]

The Government maintains tight control of telecoms services through the telecom regulator and owner of the nation's telecommunications infrastructure, Syrian Telecommunications Establishment (STE).[8] The use of censorship technologies to filter political, social, and religious websites, and to conduct surveillance on citizens is widespread. Targeted cyberattacks including general phishing, more targeted 'spear-phishing', the use of malware and 'Trojan horse' viruses against individuals and organizations; and distributed denial of service (DDoS) attacks against websites are widespread.[9] Journalists and activists have been identified using these tactics and subsequently arrested.[10] Web censorship is rife – STE blocked access to websites related to groups opposed to the al-Assad governments, human rights groups, the Muslim Brotherhood, and the country's Kurdish minority. Various Syrian telecommunications actors, including the Minister of Telecommunications and Technology and Syria, Rami Makhlouf (Syriatel CEO) and Syriatel itself were respectively added to US sanctions lists in 2008 and 2011.[11]

3 "Technical Specifications for the National Internet Backbone and STE ISP", Syrian Telecommunications Establishment, 1999, available at: http://surveillance.rsf.org/wp-content/uploads/2013/03/bidinvitation_ex.pdf

4 "President Assad And The Syrian Business Elite", Forbes, 30 March 2011, http://www.forbes.com/sites/zinamoukheiber/2011/03/30/president-assad-and-the-syrian-business-elite/#d4431a55738c

5 "Ericsson Region Middle East, Country Report: Syria", Ericsson, 2010, http://www.marconi.ca/tr/partners/documents/country_reports/SYRIA.pdf

6 "Freedom on the Net: Syria", Freedom House, 2015 https://freedomhouse.org/report/freedom-net/2015/syria

7 "Freedom on the Net: Syria", Freedom House, 2012 https://freedomhouse.org/report/freedom-net/2012/syria

8 "Freedom on the Net: Syria", Freedom House, 2012 https://freedomhouse.org/report/freedom-net/2012/syria. See also "Ericsson Region Middle East, Country Report: Syria", Ericsson, 2010, http://www.marconi.ca/tr/partners/documents/country_reports/SYRIA.pdf

9 "Freedom on the Net: Syria", Freedom House, 2015, https://freedomhouse.org/report/freedom-net/2015/syria. See also "New malware based attacks hit opponents in Syria and all over the world", Security Affairs, 20

10 August 2014, http://securityaffairs.co/wordpress/27648/cyber-crime/rats-against-opponents-syria.html "Don't get your sources in Syria killed", Eva Galperin for Committee to Protect Journalists, May 2012, https://cpj.org/blog/2012/05/dont-get-your-sources-in-syria-killed.php

11 "Treasury Sanctions State-Owned Syrian Financial Institutions and Syria's Largest Mobile Phone Operator", US Treasury, 10 August 2011, available at https://www.treasury.gov/press-center/press-releases/Pages/tg1273.aspx and "Rami Makhluf Designated for Benefiting from Syrian Corruption", US Treasury, 21 February 2008, available at: https://www.treasury.gov/press-center/press-releases/Pages/hp834.aspx

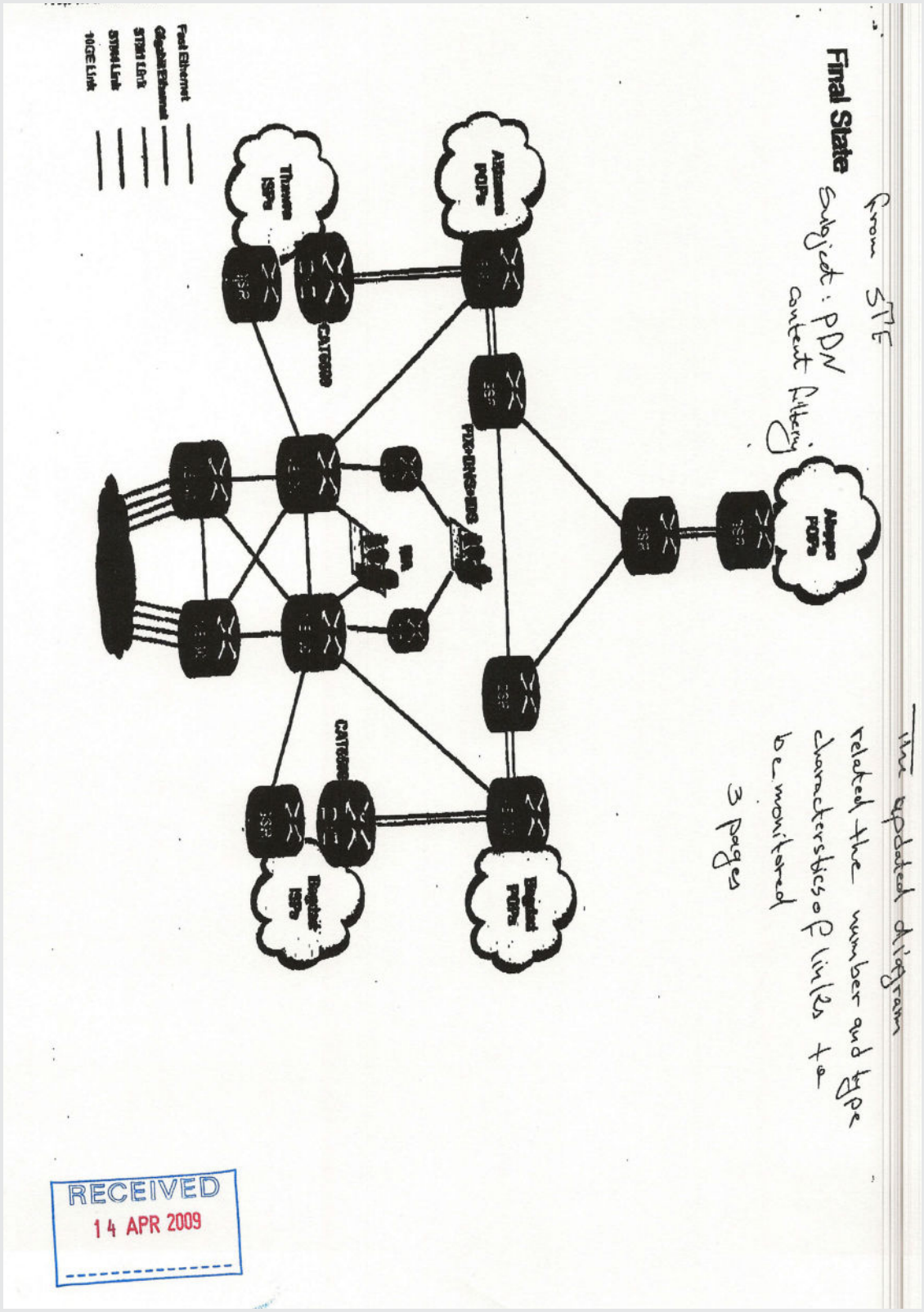
STE acted as a front for intelligence agencies, particularly the signals intelligence unit 'Branch 225', according to engineers familiar with lawful interception in Syria. "When I arrived at the international airport in Damascus, there were some guys from Syria secret services" recalls a network engineer who formerly worked in Syria." They talked with me and they said that they were the real committer for this project." Another Syrian computer specialist recalls that communication service providers would have security officers attached to them that would approve intelligence agencies' requests for data: "They would come and collect the entire log…you would have to keep logs of your traffic for six months anyway, and you have to deliver that … to this officer.'"

Communications surveillance, in conjunction with lower-tech surveillance strategies like the use of human informants and more traditional video and photo surveillance, was a key strategy of government control, both before and during the civil war, which began in 2011. This report focuses on communications surveillance — less observable than either physical surveillance or human intelligence gathering — and how the al-Assad government invested significant state funds and resources to automatically and passively collect, filter and analyse communications in Syrian territory directly from the national telecommunications architecture.

Since at least 2004, the Syrian government relied on technologies from German companies Siemens and Utimaco to intercept communications on these networks, according to documents obtained by Privacy International. In August that year, cybersecurity and surveillance technology firm Utimaco sold an interception management system to Siemens Syria for Eur 1.179 million, according to sales documentation from Utimaco. Its patented lawful interception management system, LIMS,[12] allows for the interception of communications in real-time. This includes phone calls, text messages, faxes, e-mails, VoIP calls, instant messaging and other services. The LIMS can be integrated into an existing telecommunications infrastructure and is compatible with a range of network providers. The LIMS provided to Siemens Syria was to be integrated into Syriatel networks and was present until at least 2009. Utimaco's LIMS were deployed to access those parts of Syria's network infrastructure that are provided by telecommunications infrastructure providers Nokia Siemens Networks (NSN) and Huawei. On parts of the network relying on infrastructure from Swedish provider Ericsson, Ericsson's own interception management interface was used, according to tender documentation. Utimaco states that there are no current installations of Utimaco's LIMS system in networks in Syria and no systems under license, support or maintenance by Utimaco or any of its partners. Utimaco's response is included as an annex.

By 2007, Assad's government was poised to massively expand its surveillance capacity. The original system had stopped working — updates to the Public Data Networks carrying Syria's telecommunications traffic meant that surveillance architecture needed to be kept up to date as well. The government was able to rely on a thriving industry of surveillance companies to service its ambitions.

12 "LIMS Access Points", Utimaco, 2011, available at: http://sii.transparencytoolkit.org/docs/Utimaco_LIMS_Product-Description-Specifications-1sii_documents



A diagram of the internet in Syria in 2009, from STE tender documentation.
Obtained by Privacy International

Friends and middlemen

The surveillance industry comprises a complex web of companies in the supply chain from sale, installation and operation of communications surveillance projects.

On one end of the surveillance supply chain are the manufacturers of the heavy-duty and expensive components of surveillance systems like probes, interception gateways and monitoring centre components, including the monitoring consoles and data analytics software analysts use to query the raw telecommunications data. The majority of these companies are based in Europe, Israel, China, and the US, though a number of firms from countries including South Africa and India are gaining ground in the industry.

These firms rely on consultants and companies in the countries and region where they wish to do business to act as intermediaries. These 'brokers' court government agency officials, engage in bids, resell equipment, facilitate customs and bureaucratic formalities, and otherwise secure the lucrative contracts for their partners, making a commission. They do this by entering into exclusivity agreements, and can incorporate new companies to act as vehicles for the surveillance contracts or extended business over time in a 'target' country.

Advanced German Technology (AGT) was one such intermediary. Founded by two Syrian-German brothers, Anas and Aghiath Chbib, the company reports that it had been providing surveillance and other technologies in Syria since 2002; it was ideally placed to benefit from the Syrian government's ambitious plans to expand its surveillance. In 2008 AGT registered a Syrian subsidiary, AGT Syria, with the Chbib brothers' uncle at the helm.



Gulf country clients at AGT's stall at a trade fair, 2005.
Obtained by Privacy International.

AGT

Despite its name, Advanced German Technology is actually based in Dubai and maintains a letterbox company in Berlin. It primarily resells digital forensic equipment and surveillance technology services. It was founded by two Syrian brothers, Anas and Aghiath Chbib, both of whom acquired German nationality. The elder, Anas (AGT's Managing Director) first started in the forensic and surveillance business as CEO of Instigo, a firm that went bankrupt in 2002.[13] By 2003, Chbib was working with and then assumed directorship of a company called Isdon. Chbib had the company name changed to what it is now – Advanced German Technology FZ LLC – bought out his partners' shares, and transferred them to his shell company, Expert Consultant Ltd, registered in the British Virgin Islands tax haven Tortola. Expert Consultant is owned by both Chbib brothers. It is also owned by an offshore company linked to Jordanian-Swiss businessman Yahia Samawi, Brascus Ltd.[14] Samawi and members of his family[15] are beneficiaries of Swiss-based professional services business, Brascus SA,[16] which is also part owned by the offshore Brascus Ltd.[17] In 2008, Brascus helped AGT court business from the Iraqi Minister of National Security.

AGT also acted as an intermediary for other larger surveillance companies. In 2008, AGT helped Stephane Salies, then-CEO of French surveillance technology firm Amesys via Allegretto Asset Management to set up an offshore company in the Ras Al Khaimah, an Emirate with a favourable tax regime. The other two shareholders of the new company were Abdlhakim Mudeer, a Libyan lawyer who assisted in the process of developing a nationwide interception project under then-president Muammar Gaddafi, and Anas Chbib. AGT characterize the company as being "related to some investment in the UAE in a very far sector from technology." [sic] Mudeer states that it was related to cybercrime. Salies stated that Allegretto is his personal investment company and that the company set up in Ras Al Khaimah had never been active as far as he is aware. Mudeer also denies involvement in the sale of surveillance technology. All responses received by PI related to the statements in the report by publication are included as annexes.

Two Chbib family members were on the payroll in Syria as consultants and several more paid for services rendered. AGT's internal accountants reported 'bonus'-marked payments to senior staff of over 4 million UAE dirham and unaccounted-for transactions, correspondence seen by Privacy International.

[13] "Instingo fails to appear in the Middle East", Arabian Business, 19 March 2002, http://www.arabianbusiness.com/instingo-fails-appear-in-middle-east-206868.html

[14] "BRASCUS LTD.", Offshore Leaks Database, the International Consortium of Investigative Journalists, https://offshoreleaks.icij.org/nodes/12133282. Accessed September 2016.

[15] "Yahia Samawi", Moneyhouse financial database, http://www.moneyhouse.ch/en/p/samawi_yahia-12867079/connections_zb.htm. Accessed September 2016.

[16] "Brascus Aviation S.A.", Offshore Leaks Database, the International Consortium of Investigative Journalists, https://offshoreleaks.icij.org/nodes/10128278

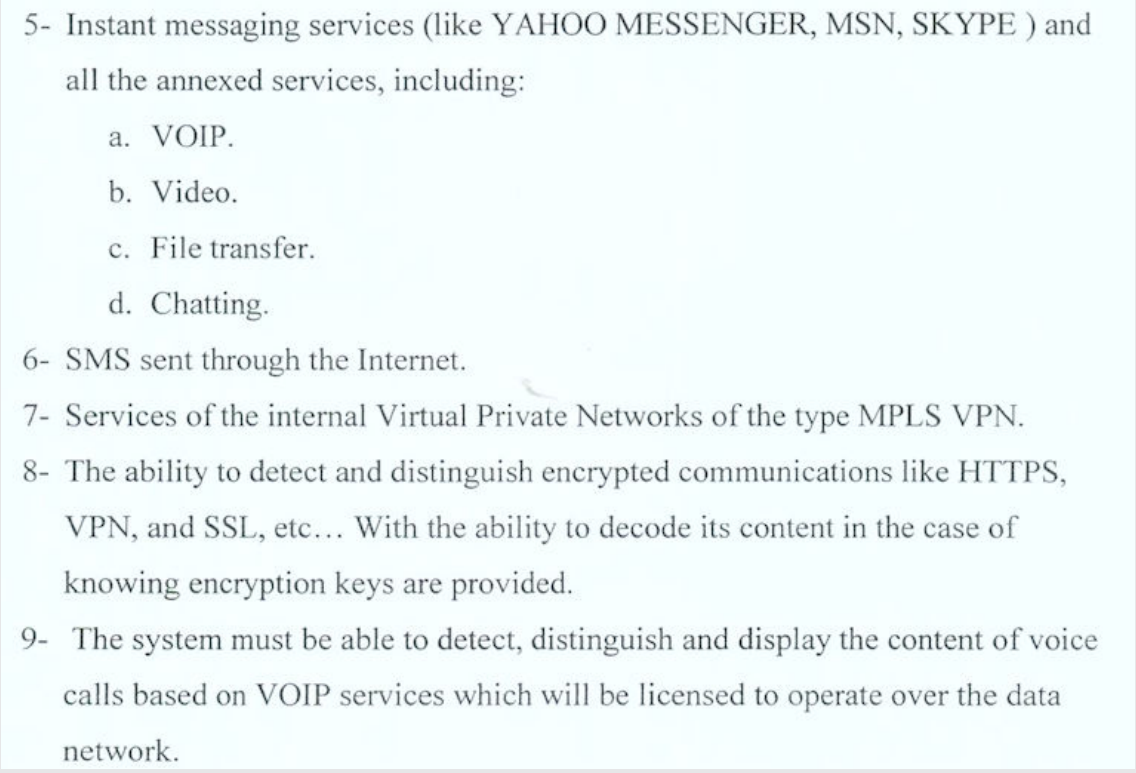
[17] In 2015. "EXPERT CONSULTANT LTD", Offshore Leaks Database, the International Consortium of Investigative Journalists, https://offshoreleaks.icij.org/nodes/10154512. Accessed September 2016. See also "Brascus SA Homepage", Brascus SA, https://web.archive.org/web/20110128184525/http://www.brascus.com/. Accessed September 2016.

To capture, collect, analyse and store — in 'Country 4'

On 2 October 2007, the head of Syrian Telecommunication Establishment, Nazem Bahsas sent out a call to companies to tender for a new "Central Monitoring System for public data networks and the internet". The tender specified that "the system must be centralized and has [sic] the ability to monitor all the networks which use data communication services inside the Syrian territories".

The Central Monitoring System, according to tender documentation, would have to be able to capture and decode a wide range of personal communications services. An excerpt from the call for tenders is included as Annex 1.

'Hot targets' — specially designated communicating parties — could be monitored in real time. The bidding companies had to demonstrate that they would allow for 50 of these targets. The lag between collection of data and their availability for analysis on all targets would have been a few minutes at most.



5- Instant messaging services (like YAHOO MESSENGER, MSN, SKYPE) and all the annexed services, including:
   a. VOIP.
   b. Video.
   c. File transfer.
   d. Chatting.
6- SMS sent through the Internet.
7- Services of the internal Virtual Private Networks of the type MPLS VPN.
8- The ability to detect and distinguish encrypted communications like HTTPS, VPN, and SSL, etc… With the ability to decode its content in the case of knowing encryption keys are provided.
9- The system must be able to detect, distinguish and display the content of voice calls based on VOIP services which will be licensed to operate over the data network.

The Central Monitoring System would be able to capture a wide range of personal communications services.
Obtained by Privacy International.

One factor that distinguished the new system from the old was the alarming level of direct access that STE had to the nation's communications, independent of service providers' knowing cooperation. STE asked that "[a]ll monitoring activities should be done undetected, neither by the monitored targets, nor by ISPs, and not even by the management of the PDN [public data networks]". STE was seeking a system that was "immune against hacking, tampering or inspection of its content".

RCS S.p.A. — an Italian surveillance technology provider — jointly bid with AGT to provide the system.

RCS S.p.A

Milan-based RCS provides surveillance solutions to government clients worldwide. Formerly part of Urmet Group,[18] it claims to have contributed to the interception of more than 10,000 targets daily in Europe alone.[19] Its Italian clients include Telecom Italia and Vodafone Italy, according to project documentation. It offered three main products in the late 2000s– (1) the MITO monitoring centre, (2) the Internet Visualization System, a multimedia application for recording, storage, decoding, and presenting intercepted IP traffic, and (3) the Sfera investigation support system, to conduct automated analysis of very large subject-related databases.

RCS reportedly tendered in 2006 to provide an interception system to the government of Malta, but lost to Israeli rival Verint Systems, according to news reports.[20] In 2010 it offered to build a nationwide communications interception system for the Moroccan intelligence services, DGST. It is unclear if RCS won the contract.

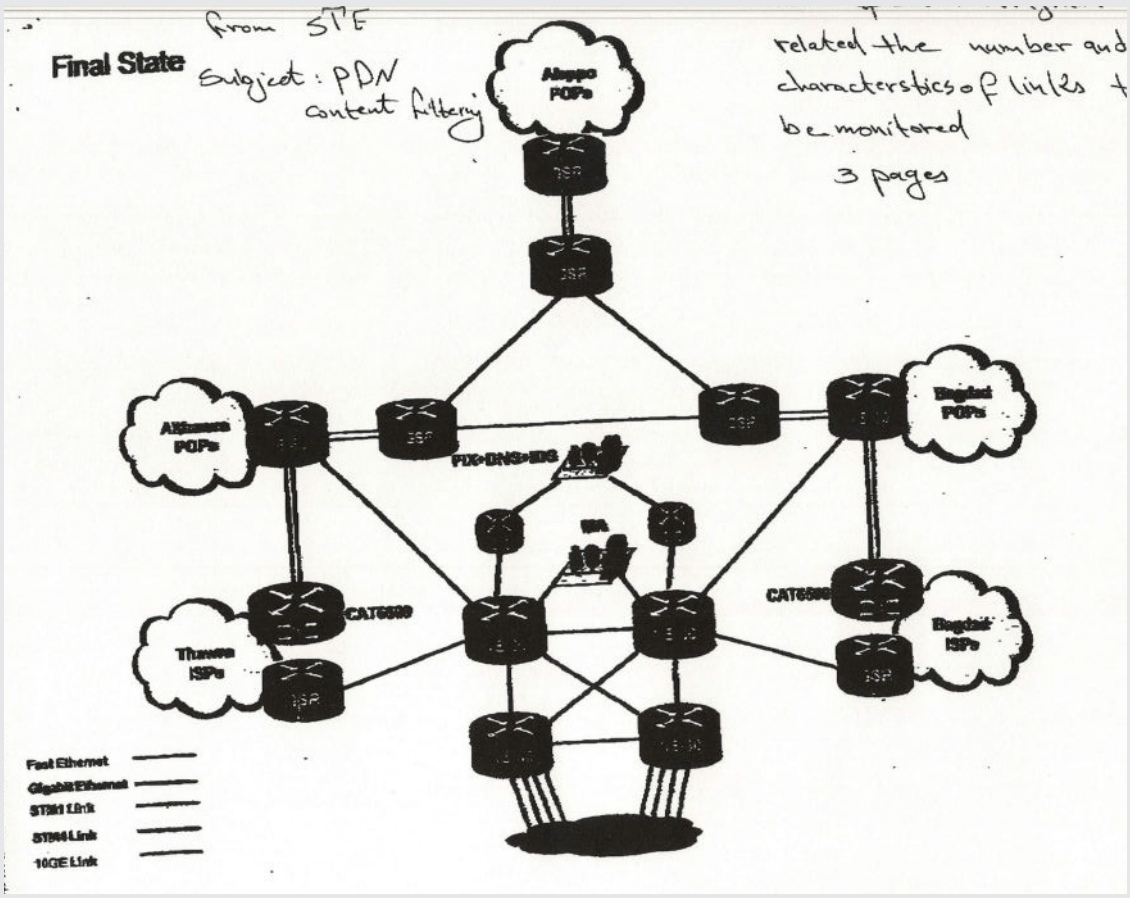
After entering into an exclusivity agreement in September 2007, AGT spent the next few years pursuing this opportunity in Syria — codenamed 'Country 4'. Four RCS engineers would travel to Syria facilitated by AGT. By December, they were preparing to send their products in Syria to carry out the requested proof of concept, which included the real-time monitoring of Syrian targets. In April 2008, STE invited RCS and AGT to begin their pilot project, for the eagerly waiting STE. RCS engineers travelled to Damascus, Syria, staying in Le Meridien. One of them hoped, this time, to at last be able to use the pool. The demonstration was successful: STE asked the companies to submit their bid for the project.

STE was initially disappointed with the low levels of data being input into the proposed system, and AGT and RCS fought hard to keep their client's interest. They offered to sell an intrusion tool (G-Spy), AGT's answer to the more successful and well-known FinFisher intrusion malware, and throw in a few other sweeteners in a last-ditch bid to keep STE's interest. AGT deny possessing such technology. RCS' rival, Italian surveillance company AREA, would eventually win the project, according to correspondence seen by Privacy International and persons close to the project.

[18] Urmet sold RCS SpA to the Sofir trust in July 2008 following financial difficulties. "Sui titolari della società è giallo la proprietà è di una fiduciaria", La Repubblica, 3 December 2009, http://ricerca.repubblica.it/repubblica/archivio/repubblica/2009/12/03/sui-titolari-della-societa-giallo-la-proprieta.html

[19] "About Us," RCS SpA, accessed September 2016: http://www.rcslab.it/en/about-us/index.html

[20] "Unsuccessful Tenderer claims upgrade during tendering period led to contract award", Malta Independent, 6 August 2006, http://www.independent.com.mt/articles/2006-08-06/news/unsuccessful-tenderer-claims-upgrade-during-tendering-period-led-to-contract-award-95039/



A diagram of the internet in Syria in 2009, from STE tender documentation.
Obtained by Privacy International

Filtering 'propaganda mail'

The Syrian government sought to centralize its persistent censorship of anti-government websites and install new capacities to censor and monitor politically inopportune speech. In December 2008, STE called for bids for the "supply, installation and operation of the equipment and software for content filtering required for Public Data Network Services (PDN) and the Internet." Content filtering, in the context of communications traveling across the PDN and the internet, means analysing the communications data packets and assessing them for key words or attributes, and then either blocking transmission of that message, storing a copy for further analysis, or letting the message pass through without storage. Such technologies are also widely used for censorship, particularly at politically sensitive moments, such as during public protests. An excerpt from STE's requirements for the content filtering project is included as Annex 2.

Amesys, a French company who AGT called its partner in the bid, promoted its services to the Syrian government. Amesys controversially provided monitoring technology to the Libyan government in 2007. It is currently being investigated by the French courts for alleged complicity in human rights abuses including torture in Libya.[21]

AMESYS

Amesys is a French technology company, part of which specialized in telecommunications network surveillance technology. In 2010, Amesys was incorporated as a unit of Bull Group, which was in turn bought by French computing company Atos.[22]

In 2011, Amesys was revealed to have provided a surveillance system to the Libyan government, according to documents seized by protestors from the abandoned security services following the 2011 uprising against then-President Muammar Gaddafi.[23] Following the scandal, Bull sold the interception wing of Amesys. A new, legally separate company Advanced Middle East Systems FZ LLC was established in 2012 in Dubai.

Amesys was a reliable partner of AGT – the two companies jointly organized 'Defense Days', workshops to train intelligence and law enforcement officials from countries including Tanzania and South Africa, on forensic and surveillance technologies. In 2008, AGT helped Stephane Salies, then-CEO of French surveillance technology firm Amesys via Allegretto Asset Management to set up an offshore company in the Ras Al Khaimah, an Emirate with a favourable tax regime. The other two shareholders of the new company were Abdlhakim Mudeer, a Libyan lawyer who assisted in the process of developing a nationwide interception project under deposed president Gaddafi, and Anas Chbib. AGT characterize the company as being "related to some investment in the UAE in a very far sector from technology." [sic] Mudeer states that it was related to cybercrime. Salies stated that Allegretto is his personal investment company and that the company set up in Ras Al Khaimah had never been active as far as he is aware. Mudeer also denies involvement in the sale of surveillance technology. All responses received by PI related to the statements in the report by publication are included as annexes.

[21] "Amesys lawsuit (re Libya)", Business and Human Rights Resource Centre, 2016, http://business-humanrights.org/en/amesys-lawsuit-re-libya-0#c18496

[22] "Atos-Amesys S01E02 : à la recherche de l'éthique perdue", Reflets.info, 18 March 2016, https://reflets.info/atos-amesys-s01e02-a-la-recherche-de-lethique-perdue/

[23] "Firms Aided Libyan Spies," The Wall Street Journal, 30 August 2011, http://www.wsj.com/articles/SB10001424053111904199404576538721260166388

"We are not concerned with "Classic" spam (such as junk mail for pharmacies online or whatever)," assured the STE Director General, "but rather with propaganda mail which has the shape of spam".

What kind of key 'propaganda' words did STE want flagged? "Given that we are not the authors of these messages, we cannot give a firm figure for the blocking criteria. Please specify the number that your proposed solution could handle currently along with the potential for expansion." It was not STE's call to make as to what constituted objectionable content — it was the end-user's, the Syrian intelligence services. By early 2010, the contract had still not been awarded. Salies, commenting on Amesys' business, confirmed that the company pursued business with AGT in Syria but denies that this particular opportunity was pursued further because of the political situation. Salies' full response is included as an annex.

Monitoring the international exchanges in 'Lion country'

In June 2009, the Syrian government announced an even more ambitious surveillance project — this time, to tap the two international exchanges bringing internet traffic into the country in Damascus and Aleppo. The "Project for supply and installation of Monitoring Equipment For the International Exchanges" would potentially allow for the

VASTECH

South African firm VASTech has been providing surveillance technology to government clients since 1999.[24] The company specialises in passive network interception products. By 2009 it had completed lawful interception projects in Syria, the broader Middle East, and North Africa. In 2011, VASTech was revealed to have provided its Zebra lawful interception system to the government of Colonel Muammar Gaddafi in Libya when operating manuals and other company-marked documents were recovered from the state security services building following Gaddafi's overthrow.[25] VASTech at the time declined to elaborate on the company's Libyan operations.[26]

VASTech's founder Frans Dreyer died in a plane crash outside Tripoli in May 2010, prompting some speculation as to whether the company would recover.[27] It strengthened its foothold in the Gulf in 2011 by establishing a company in Oman, VAS Tech LLC. VASTech has benefited from public funding from the South African government[28] and by 2015, had expanded its business into other African countries, with offices in Dubai and Switzerland.[29] The company's new product line includes Galaxia, a satellite monitoring system, Strata, for monitoring fixed-line and mobile phone systems, and Portevia, for fibre optic traffic monitoring.[30]

[24] "Company Overview", VASTech, 2011. Available at: https://wikileaks.org/spyfiles/files/0/182_VASTECH-201110-BROCHURES.pdf

[25] "SA firm 'helped' Gaddafi spy on the people of Libya", Mail and Guardian, 2 September 2011, http://mg.co.za/article/2011-09-02-sa-firm-helped-gaddafi-spy

[26] "SA firm 'helped' Gaddafi spy on the people of Libya", Mail and Guardian, 2 September 2011, http://mg.co.za/article/2011-09-02-sa-firm-helped-gaddafi-spy

[27] "Say nothing – the spooks are listening", Mail and Guardian, 17 December 2015, http://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening

[28] "South African Government still funding VASTech, knows previous financing was for mass surveillance", Privacy International, 30 January 2014, https://www.privacyinternational.org/node/305

[29] "ISS World 2016 MEA – Lead Sponsor," ISS World, http://www.issworldtraining.com/iss_mea/sponsors2.html Accessed September 2016.

[30] "Systems", VASTech, http://www.VASTech.co.za/systems.html. Accessed September 2016.



A potential customer speaks with a VASTech representative.
Obtained by Privacy International.

monitoring of all internet traffic into and out of the country.

This time, South African surveillance technology firm VASTech answered STE's call. They had a similar project running in the country since 2002.

VASTech has a close history with AGT. In July 2007, VASTech CEO Frans Dreyer took on the role of 'Technical Director' for AGT, according to a contract signed with AGT. VASTech deny that Dreyer ever held any position at AGT. VASTech had been providing interception capacity in Syria since 2002 — as part of its statement of intention to bid, the company confirmed that "the [AGT-VASTech] consortium has 3 similar projects running, 1 in North Africa, 1 in the Middle East, and 1 in Syria (since 2002)." The North Africa project would later be revealed to be Libya.[31]

The Syrian government wanted to use 'brute force' speaker identification — tracking individual targets using Syria's phone services by comparing their unique voice prints against all calls into and out of and within Syria, which would be recorded. VASTech and AGT counselled them against this — the cost would simply be too high. Instead it recommended that the Syrian government apply 'focused' speaker identification which, "in combination with the VASTech Zebra Network Analysis capability, [would allow them] to search in a subset of the calls…" more likely to contain the target. An excerpt of the AGT-VASTech proposal for brute force voice identification of phone users in Syria is included as Annex 4.

VASTech tried hard to get the sensitive contract in Syria. Sales and marketing director Andre Scholtz and his wife travelled to Syria in mid-July 2010, facilitated by AGT's receptionist, who booked the VASTech delegation into the luxury Four Seasons resort for their stay in "Lion country", the code term for Syria. It is unclear whether VASTech won this particular contract. VASTech declined to comment on its business dealings in Syria and with AGT. On Libya, VASTech stated that it contracted lawfully in that country until terminating the agreement in February 2011. VASTech's full response is included as an annex.

31 "Firms Aided Libyan Spies," The Wall Street Journal, 30 August 2011, http://www.wsj.com/articles/SB10001424053111904199404576538721260166388

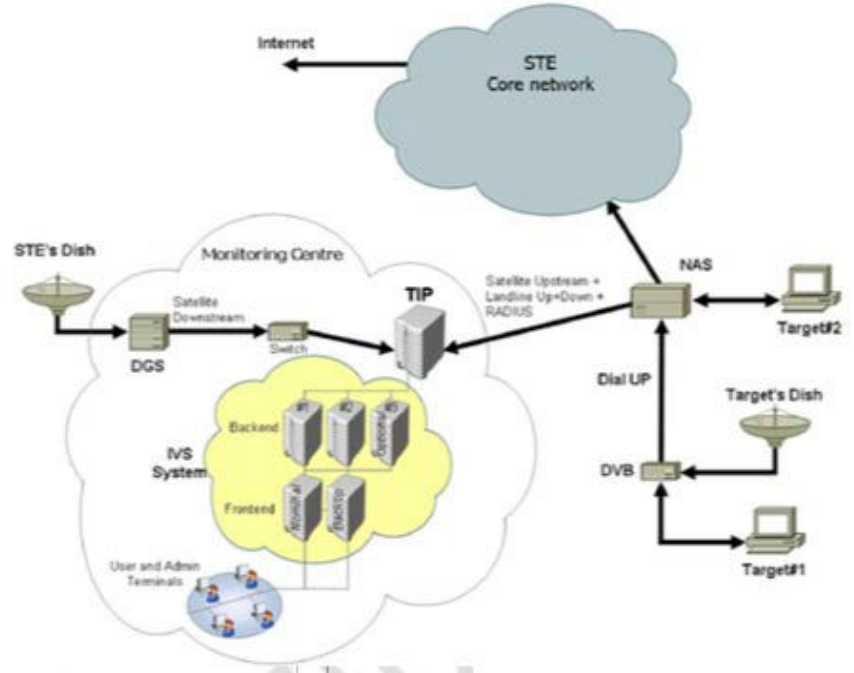


Figure 2 "Network Scenario"

1.5 Logical Architecture

The proposed solution is designed to analyze and eventually intercept the traffic exchanged by SCT's subscribers: all the traffic is analyzed at wire-speed by the ***Probing Subsystem*** and the relevant one is saved in standard PCAP files when the content match with one or more configured interception rules.

Seized traffic is delivered in realtime to the ***Monitoring Subsystem***, where PCAP files are recorded, stored and decoded.

2 Probing Subsystem

The proposed probing subsystem lean on the well established RCS's Tactical IP Probe (TIP), a 1+1Gbps single server software based interception Probe already used in many contests. RCS's TIP runs over COTS [Commercial-Off-The-Shelf] hardware (see the following paragraph §4.2 for

CONFIDENTIAL: Copyright reserved, the present document cannot be used, modified, published or copied in any matter or means without prior consent of RCS S.p.A.

Of the protocols the system could decode would be multimedia files, HTTP (websites), various email services and web chat programmes. (25 August 2009)

Obtained by Privacy International

Satellite internet monitoring

By the late 2000s, the Syrian government had set up extensive infrastructure to intercept cable-bound communications traffic over much of the country. Yet in many more remote and rural areas ISPs relied on satellite providers, like Syrian provider Aramsat, to deliver connectivity to customers.

"This effortless usability accelerates the analysis, enabling the operator to find quickly on screen the most important pieces of the IP communication."

RCS/AGT proposal to Syria Communication Technologies for satellite communications monitoring for Syrian law enforcement and intelligence (25 August 2009), Annex 5

The government also created a system to monitor these communications. RCS provided this capacity in 2009 after a successful demonstration of the product in 2008, according to company documentation including purchase orders and bank transfers. The complicated web of transactions involves companies in Italy, Kuwait, Syria, UAE and Cyprus, several of which are partially owned by Chbib using AGT's name, his business partner Mustafa Murad, an executive at Kuwaiti service provider Gulfsat, and Mohammed Mustafa Mero, a former Syrian politician.[32] Murad and Gulfsat did not respond to repeated requests for comment.

The system was fitted with a probe that would be "passive," receiving a copy of the "to be monitored" packet streams. It would then route these streams onward to Syrian law enforcement or intelligence agents via the monitoring system which would be physically located within "the central Law Enforcement Monitoring Facilities from which the LEA intends to decode and inspect the intercepted data." Once the data was collected, a Syrian intelligence analyst could either archive the material for offline analysis at a later point, or follow a target live, as long as he/she was connected to the internet. The system was built to allow for the monitoring of "50 targets with 100 rules, using 10 client stations."

"For the interception rate, the maximum value ever seen in all European and Extra-European countries is 1:2000…Considering the special context of this project, with the need of content-oriented monitoring, we considered for this project a very safe ratio of 1:1000."

RCS/AGT proposal to Syria Communication Technologies for satellite communications monitoring for Syrian law enforcement and intelligence (25 August 2009), Annex 5

[32] Mero held a 5 % stake of Syrian Communication Technology in February 2009, according to company registration information. Anas Chbib held 70 % of shares, with the remaining 25 % distributed among individuals who Privacy International was not able to identify.

"[T] he system can [be] managed to monitor a bandwidth of 400MB [sic] without any extra charges to Gulfsat and it fill [sic] the requirements from the End User."

Letter from AGT to Gulfsat, about the particular requirements of their Syrian end-user, (10 August 2008)

A PROFITABLE DEAL

Actor	Company	Country
Original equipment manufacturer	RCS proprietary equipment (software) Dell and Netoptics are suggested for hardware	Italy (Milan)
Supplier	RCS SpA	Italy (Milan)
Partner	Advanced German Technology FZ-LLC	UAE (Dubai)
Contractor	Syrian Communication Technology (SCT) (jointly owned by Anas Chbib, Gulfsat, and various Syrian businessmen and politicians)	Syria (Damascus)
Client	Gulfsat (represented by Mustafa Murad) NK Oriaka Communications Ltd (represented by Mustafa Murad)	Kuwait (Safat) Cyprus (Limassol)
End-User	Undisclosed Syrian law enforcement or intelligence agency	Syria

The actors involved in tapping communications over Aramsat's satellite networks.

Israel and geopolitics in the surveillance industry

Like many Middle Eastern governments, the Syrian government required its providers to demonstrate that they were completely free of ties to Israel. Foreign suppliers of surveillance technology and their domestic partners had to provide signed and notarised statements that their companies had no business dealings in Israel, no investment from Israelis or Israel-backed firms, and no intention to conduct business in Israel. The two countries have no formal diplomatic relations.

Companies were happy to oblige. "[W]e are pleased to officially confirm", RCS reassured STE, "that RCS hasn't sold / purchased to/from Israel any solution or part od [sic] solution relevant to Lawful Interception." Similarly, VASTech declared its compliance with "the rules of Israel boycott."

While diplomatic and trade relations between Israel and Gulf countries remain limited and discrete, several significant surveillance deals between Middle East and Gulf countries and Israel have been reported. AGT International, a Switzerland-based technology company with no apparent ties to Advanced German Technology but owned in part by prominent Israeli businessman Mati Kochavi, supplied a centralized, nationwide command and control system to the UAE government, according to Middle East Eye.[33]

But geopolitical considerations would only matter so much. The successful bidder for one of the Syrian contracts, the Central Monitoring System, was AREA SpA. In December 2009, Anas Chbib drafted an error-filled letter — confidential and to be hand-delivered to STE head Nazem Bahsas — arguing that AGT and its own Italian partner RCS should have won the deal instead because they had the interests of the Syrian state at heart, unlike AREA which, Chbib claimed, had done business in Israel. The letter is included as Annex 3.

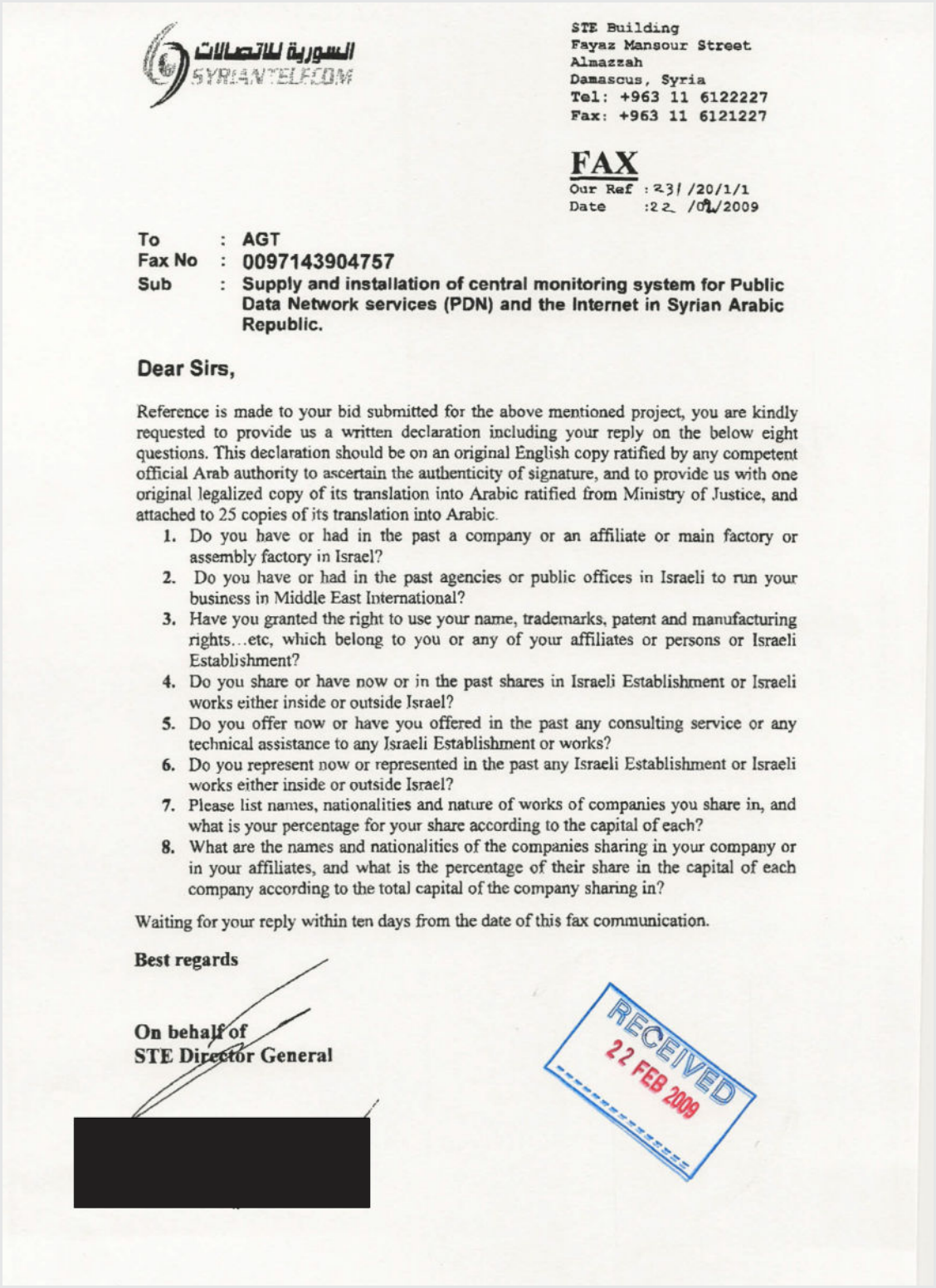
AGT was not successful in its appeal. Chbib probably never got his audience with President al-Assad. AREA continued its work setting up the central monitoring system project, codenamed Asfador, with partners German firm Utimaco and French company Qosmos.[34] But civil unrest caught the government and its surveillance technology providers by surprise. "[They were] in a hurry since they knew that sometime the revolution should be very near," recalls the former network engineer.

[33] "Falcon Eye: The Israeli-installed mass civil surveillance system of Abu Dhabi", Middle East Eye, 28 February 2015, http://www.middleeasteye.net/news/uae-israel-surveillance-2104952769#sthash.sswlL7lp.dpuf. The investigation was prompted by a mysterious routine flight between the two nations. "Secret flight linking Israel to the UAE reveals 'open secret' of collaboration", Middle East Eye, 22 December 2014, http://www.middleeasteye.net/news/secret-jet-flying-between-israel-and-uae-567607953

[34] "Syria Crackdown Gets Italy Firm's Aid with U.S.-Europe Spy Gear", Bloomberg News, 3 November 2011, http://www.bloomberg.com/news/articles/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear

Political sensitivities on display: AGT claims AREA undercut them and did not have Syrian national interests at heart.

Obtained by Privacy International. December 2009.



السورية للاتصالات
SYRIANTELECOM

STE Building
Fayaz Mansour Street
Almazzah
Damascus, Syria
Tel: +963 11 6122227
Fax: +963 11 6121227

FAX

Our Ref : 23/ /20/1/1
Date : 22 /02/2009

To : AGT
Fax No : 0097143904757
Sub : **Supply and installation of central monitoring system for Public Data Network services (PDN) and the Internet in Syrian Arabic Republic.**

Dear Sirs,

Reference is made to your bid submitted for the above mentioned project, you are kindly requested to provide us a written declaration including your reply on the below eight questions. This declaration should be on an original English copy ratified by any competent official Arab authority to ascertain the authenticity of signature, and to provide us with one original legalized copy of its translation into Arabic ratified from Ministry of Justice, and attached to 25 copies of its translation into Arabic.

1. Do you have or had in the past a company or an affiliate or main factory or assembly factory in Israel?
2. Do you have or had in the past agencies or public offices in Israeli to run your business in Middle East International?
3. Have you granted the right to use your name, trademarks, patent and manufacturing rights…etc, which belong to you or any of your affiliates or persons or Israeli Establishment?
4. Do you share or have now or in the past shares in Israeli Establishment or Israeli works either inside or outside Israel?
5. Do you offer now or have you offered in the past any consulting service or any technical assistance to any Israeli Establishment or works?
6. Do you represent now or represented in the past any Israeli Establishment or Israeli works either inside or outside Israel?
7. Please list names, nationalities and nature of works of companies you share in, and what is your percentage for your share according to the capital of each?
8. What are the names and nationalities of the companies sharing in your company or in your affiliates, and what is the percentage of their share in the capital of each company according to the total capital of the company sharing in?

Waiting for your reply within ten days from the date of this fax communication.

Best regards

On behalf of
STE Director General

[redacted]

RECEIVED
22 FEB 2009

Surveillance and interception contracts were considered "equipment with a special importance".
Obtained by Privacy International. February 2009.

War, Sanctions and Export Restrictions

On 15 March 2011, protestors in Damascus took to the streets to demand democratic reforms and the release of political prisoners. By April 2011, the protests had turned to more explicitly anti-Assad protests. In the ensuing crackdown and skirmishes, by May the death toll had reportedly reached over 1,000.[35] The government lost control of much of the country's restive north and east, as rival militant groups claimed more and more territory in what is currently Syria's civil war.

The government's crackdown on the flow of information was almost immediate. In May 2011, the Ministry of Defence reportedly issued a communique ordering the disconnection of the internet in Homs and other restive areas of eastern Syria.[36] Researchers reported a full day, nationwide internet blackout in June 2011,[37] and more localized blackouts throughout Syria. Activists reported that when pro-regime forces would besiege a city, the broadband bandwidth was reduced dramatically and 3G services shut off.[38] Telecommunications infrastructure was also badly damaged in bombing campaigns, especially in cities like Homs that were subject to particularly severe shelling by the Syrian armed forces."[39]

The EU and the US responded with new restrictions, including concerning the sale of interception equipment to the Syrian government. The US has considered the Syrian government a 'state sponsor of terrorism' for almost 30 years.[40] Extensive sanctions and export control regimes govern the kind of trade US businesses can legitimately conduct with the country. Executive Order 13338, signed by President Bush in 2004, placed a trade embargo on Syria prohibiting, without a license, the exportation or re-exportation of most US-origin goods to the country, including surveillance equipment.[41]

35 "Syria death toll 'surpasses 1,000'", Al Jazeera, 24 May 2011, http://www.aljazeera.com/news/middleeast/2011/05/201152418225195272 7.html

36 "Leaked Syrian document shows how Assad banned internet access and satellite phones", Michael Weiss, Blog for The Telegraph, accessed September 2016: http://blogs.telegraph.co.uk/news/michaelweiss/100093908/leaked-syrian-document-shows-how-assad-banned-internet-access-and-satellite-phones/

37 "Syria's Internet Blockage Brings Risk of Backfire", The Wall Street Journal, 3 June 2011, http://www.wsj.com/articles/SB10001424052702304563104576363763722080144

38 "Freedom on the Net: Syria", Freedom House, 2012, https://freedomhouse.org/report/freedom-net/2012/syria

39 "Freedom on the Net: Syria", Freedom House, 2012, https://freedomhouse.org/report/freedom-net/2012/syria

40 "Syria Sanctions", US Department of State, accessed September 2016: http://www.state.gov/e/eb/tfs/spi/syria/

41 With the exception of certain medicines and food, no item subject to the Export Administration Regulations ("EAR") may be exported or re-exported to Syria without a Department of Commerce license. The Department of Commerce's Bureau of Industry and Security ("BIS") administers the EAR, which control exports and re-exports of a broad range of dual use goods and technology. 15 CFR §746.9, which contain the EAR provisions relating to Syria, provides that "all license applications for export or reexport to Syria are subject to a general policy of denial" except that applications for technology and source code on the Commerce Control List (CCL) "will be reviewed on a case-by-case basis." (These controls were placed in 15 CFR §746.9 on December 12, 2011; prior to that date, they were contained in General Order No. 2, codified in Supplement No. 1 to Part 736 of the Regulations.) The CCL, which is contained as a supplement to the EAR, lists certain types of surveillance equipment, including "[m]obile telecommunications interception or jamming equipment" (5A001.f); "[d]evices primarily useful for the surreptitious interception of wire, oral, or electronic communications, other than those controlled under 5A001.f.1" (5A980); and "cryptographic 'information security'" equipment, including "'information security' systems, equipment and 'components'" (5A002).

Since the uprisings began in Syria, the US government has issued a series of further restrictions on exports to Syria.[42] In August 2011, President Obama announced new sanctions against Syria that further restricted the sale of interception equipment specifically — for the first time, Syriatel was added to the list of proscribed groups.[43] The European Union (EU) only enacted specific sanctions concerning the sale of telecommunications and surveillance equipment in 2011[44] and again in 2012.[45]

Prior to and in tandem to these specific EU restrictions, the Wassenaar Arrangement would have governed exports of surveillance technology to Syria from countries who are participants to it. The Wassenaar Arrangement is a multi-governmental trade control regime in which participants agree what conventional weapons and dual-use goods should be controlled in order to promote international security. Crucially, the 41 participants include five out of the world's six biggest arms exporters - the US, Russia, Germany, France and the UK.[46]

Companies were aware of restrictions on technology exports to Syria but nevertheless appeared open to supplying surveillance technologies to the country.

In 2010, it appears AGT was prepared to sell Silentrunner probes of US technology firm AccessData to one of Syria's two mobile service providers, MTN Syria.[47] US sanctions and export control regulations in force at the time of this transaction restricted, without

42 Executive Orders 13572, 13573, 13582, 13606, 13608.

43 "Treasury Sanctions State-Owned Syrian Financial Institutions and Syria's Largest Mobile Phone Operator", US Department of the Treasury, 10 August 2011, https://www.treasury.gov/press-center/press-releases/Pages/tg1273.aspx

44 "The sale, supply, transfer or export of equipment or software intended primarily for use in the monitoring or interception by the Syrian regime, or on its behalf, of the Internet and of telephone communications on mobile or fixed networks in Syria and the provision of assistance to install, operate or update such equipment or software shall be prohibited." Council Decision 2011/782/CFSP of 1 December 2011, art. (3), available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:319:0056:0070:EN:PDF

45 "The competent authorities of the Member States, as identified in the websites referred to in Annex III, shall not grant any authorisation under paragraph 1 if they have reasonable grounds to determine that the equipment, technology or software in question would be used for monitoring or interception, by the Syrian regime or on its behalf, of internet or telephone communications in Syria." Council Regulation (EU) No 36/2012 of 18 January 2012, art. 4(2), available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:016:0001:0032:EN:PDF

46 The Wassenaar Arrangement has for decades controlled the export of cryptography, meaning that some surveillance systems are subject to prior licensing if they contain certain levels of cryptography. In 2010, "laser microphones" were added to list, which are used to eavesdrop on conversations by monitoring sound vibrations using lasers, for example through glass. In 2012, phone monitoring technology was explicitly added to the Wassenaar list to target mobile and satellite phone monitoring equipment. Prior to 2012, some states had already controlled the equipment because of controls related to 'Telecommunications systems, equipment, components', though this was interpreted differently by participating states. In 2013, further categories were added to the Wassenaar control list: intrusion software and IP surveillance systems. The EU is currently undergoing a revision of its Dual Use Regulation, which among other things, incorporates the Wassenaar control list into an EU control list used by member states. See, for example, "Final Report: Data and information collection for EU dual-use export control policy review", European Commission, 6 November 2015, http://www.cecimo.eu/site/fileadmin/documents/EU%20LEGISLATION%20AND%20DOSSIERS/Dual-use_legislation/FINAL_REPORT.pdf and "Summary of Changes: List of Dual-Use Goods & Technologies and Munitions List as of 1 December 2010", The Wassenaar Arrangement, accessed September 2016, http://www.wassenaar.org/wp-content/uploads/2015/06/Revised-Summary-of-Changes-to-Control-Lists.pdf

47 MTN Syria had been in possession of US technology for some time. Syrian employees of Areeba, a Syrian provider which merged with the MTN group, assured AGT it would be fine to have US software, even that they were in possession of Cisco servers. Cisco had previously told CBS News that it had a "few licensed sales" to MTN Syria, but said it was "sanctioned" by the U.S. government. See also "Surveillance and censorship: Inside Syria's Internet", CBS News, 12 December 2013, http://www.cbsnews.com/news/surveillance-and-censorship-inside-syrias-internet/

AGT ADVANCED GERMAN TECHNOLOGY

Financial Proposal: Network-Data Monitoring and File & LAN Encryption

Offer date: 11. Jan 10

Offer no: 01-M-01

Offer to:		**Ship to:**	
Company name:	MTN South Africa	Company name:	MTN South Africa
Contact person:		Contact person:	
Address:		Address:	
Address 2:		Address 2:	
Postal code:		Postal code:	
City / Country:	Johannesburg / South Africa	City / Country:	Johannesburg / South Africa
Telephone number:		Telephone number:	
Fax number:		Fax number:	
E-mail:		E-mail:	
Vat no:		Notes:	

Specification

Currency:	USD			Express Shipment	No
Terms of payment:				Standard Shipment	Yes
Sales code:	MR			Terms of delivery	DDP
				Discount approved by	

Products

Art no	Description	Units	Price per unit		Total
Safeguard LAN Crypt	File Encryption Solution	100	119,80		14.094,12
Safeguard MailGateway Professionnal	Email Encryption Solution	100	50,40		5.929,41
Support for Sophos products	Support for Sophos Products (one unit for two)	100	17,02		2.002,35
SilentRunner	Real-Time Network Data Observation Solution (all components included except laptop)	1	58.823,53		58.823,53
Support for Silent Runner (1 year)	Support for Silent Runner (1 year)	1	11.764,71		11.764,71

A financial proposal from AGT states the destination as South Africa. The proposal was attached to an email discussing sending the equipment for use in Syria. Obtained by Privacy International.

a licence, the exportation or re-exportation of US-origin communications equipment to Syria, which would almost certainly include probes of the type manufactured by AccessData. In January 2010, AGT's Director of Sales and Marketing Marco Rettig offered to route the shipment officially from Dubai through MTN's parent company in South Africa. In email correspondence with senior MTN Syria employees, he appears to propose this method in order to avoid export restrictions to Syria.

"We have thoroughly screened the market for an appropriate solution and have spoken to many (!) different suppliers. Unfortunately, all solutions that would have fulfilled your requirements technically where SUBJECT TO EXPORT RESTRICTIONS to Syria! The alternative would have been inferior products that would not suffice your expectations. Therefore, we believe the BEST WAY IS TO DELIVER THE PRODUCT TO MTN SOUTH AFRICA."

Email from Marco Rettig, AGT Director of Sales and Marketing to Husam Sidawi and Wassim Saad, MTN Syria, 11 January 2010. Emphasis in original.

AccessData denies knowledge of the AGT proposal. AccessData's full response is included as an annex. Email correspondence within AGT suggests that US companies including AccessData did not wish to consider doing business in Syria and Libya. If this transaction were in fact completed, as AGT proposed in 2010, it may have violated US sanctions and export control regulations. AGT states that it has been following all UN and EU export regulations. AGT further stated in relation to the AccessData probes: "its the vendor responsibility to obtain the export license, and not the seller, and at the end its south African company, MTN is telecom operator with many location and licenses, if they wanted to use network forensic tool to identify any malware in the network, than its internal issue, this tool is not been made be installed on public networks." [sic] MTN state that though a proof of concept process was proposed to be undertaken in South Africa, MTN Syria did not procure any products from AGT. MTN's response is included as an annex.

In another project, beginning in 2008, AGT suggested the inclusion of US-origin equipment in a project to intercept communications on the networks of a satellite internet service provider, Aramsat, as described above. A July 2008 list of hardware considered for the demo phase of the project includes network probes by US-headquartered Netoptics. An August 2009 technical proposal from an AGT-RCS partnership to SCT for the full phase of the project specifies US-origin hardware for the project: it lists Dell Xeon Intel servers (DELL PE2950) as part of the "proposed TIP probe" and "backend IVS (internet visualization system)". The proposal is included as Annex 5.

RCS did not include hardware in their own June 2008 offer to AGT, according to project documentation reviewed by Privacy International.[48] These specifications raise the question of whether there was an intent to provide US-origin hardware for the project and how that hardware would be procured.

RCS did nevertheless suggest a minimum configuration based on specific US-origin technology for the interception project in Syria throughout the project's demo and full phase. Purchase orders for software for the project were fulfilled in October 2009. It is not clear what hardware was actually procured for the project. If a company were in fact actively involved in procuring, preparing and providing US-origin equipment for an interception project in Syria, it may have acted in violation of US sanctions and export control regulations. US sanctions and export control regulations in force at the time of this project restricted the exportation or re-exportation of such US-origin goods.[49]

AGT states that network surveillance technology from RCS was not sold for the Aramsat monitoring project. AGT further states in relation to this project: "never sold, and if its offered the HW [hardware], it is local supply issue, and we can not, will not involve in any importing of HW like dell or others, to any country, not only Syria, beside it was available in SYRIA without any involvement of AGT, as we are not hardware vendor nor distributor." [sic]

[48] The 11 June 2008 offer letter for the project's demo phase states: "Hardware is not part of the present offer. RCS suggest [sic] minimum configuration detailed in the annexed documents".

[49] See note 41.

"I know from how I was working … there was absolutely no due diligence on who they [AGT] were supplying to," recalls a former technical AGT employee. "And that's the way it was done, there was never any checks carried out."

Another engineer not affiliated with AGT who worked in Syria recalls that routing controlled technologies through Dubai diverted attention from where, exactly, these technologies were ending up: "When I was in Syria, I saw a ton of different USA brands, Cisco, IBM and all of them arrived from Dubai".[50]

[50] Privacy International was unable to independently verify claims that Cisco and IBM equipment supplied in Syria.

The Hustle

During the late 2000s, governments across the Middle East and North Africa faced increasing domestic unrest. By mid-2011, Bahrain, Egypt, Libya, Syria, Tunisia, and Yemen were facing full blown uprisings. In the run-up to this unrest, their governments had been willing to buy whatever might help them regain control — including more surveillance technologies.

Fortunately for AGT, the region was its area of expertise. Its clients for both surveillance and other technology projects in 2010 included governments of Saudi Arabia, Kuwait, UAE, Jordan, Egypt, Bahrain and Qatar. AGT also attempted to cultivate business in Sudan, arranging to meet in Dubai with Presidential advisor and former head[51] of Sudan's National Security and Intelligence Service, Salah Abdallah Gosh in 2011. Gosh has been accused of having a significant role in organizing the Sudanese government's support to militias in the Darfur conflict.[52] AGT deny meeting Gosh, stating they have never done business with either Sudan or South Sudan.



Doing business at an international military and police technology trade show in 2015.
Obtained by Privacy International.

51 "Sudanese president names new intelligence chief," Al Arabiya, 14 August 2009, http://www.alarabiya.net/articles/2009/08/14/81753.html

52 "The Foreign Office, Sudan's secret police chief, and the war on terror", The Independent, 26 November 2006, http://www.independent.co.uk/news/world/politics/the-foreign-office-sudans-secret-police-chief-and-the-war-on-terror-6229800.html



DEFENCE DAYS INVITATION

amesys
a Bull group company

Bull

Bull & Amesys have the pleasure to invite you to Defence Days
at « Yachts de Paris » club – Port Henri IV – Paris IV

Tuesday, March 15th and Wednesday, March 16th 2011
From 9:30 am to 6:00 pm

Program

> Workshops, showroom and equipment demonstrations

Interception
- GSM
- Microwave
- Radar
- IP
- Open Source Intelligence

Road Runner
FRL
ELIT
EAGLE
OSINT

Jamming
- RCIED and communications

SHADOW

Data Processing
- Extreme computing
- Mobile Data Center
- Data storage and archiving

bullx
MOBULL
BULL Storeway

Security
- End to End Data Protection
- Data loss Prevention
- Infrastructures security

TRUSTWAY
DLP
VAUBAN

Aircraft equipments
- Portable equipments
- Embedded equipments

DACOTO
NEURON

> Conferences and meetings all day
- New interception solutions
- Jamming : a challenge for people protection
- How to protect a network against data loss
- Nomadic equipment protection
- Extreme computing for Defence
- Data centers evolution : challenge and opportunities
- Infrastructures security
- Portable and embedded aircraft equipments

Government officials from Tanzania to South Africa learned about interception products on offer at Defense Days, sponsored by Amesys and Bull with assistance from AGT.

Obtained by Privacy International

Libya: a cash cow

On 15 February 2011, up to 2,000 people took part in overnight protests against the arrest of a prominent government critic and lawyer. Dozens of protesters were killed in fighting between security forces and the protesters. Nine months later, in October, the National Transitional Council declared the country 'liberated', as Gaddafi's government had been earlier forced out of the capital Tripoli, and Gaddafi killed. The civilian death toll numbered in the thousands.

Documents seized in 2011 from Libya's security services offices confirmed that VASTech had provided communications surveillance capacities to the government.[53] Behind the scenes, in the two years leading to the revolution, AGT had facilitated a surveillance project[54] codenamed 'Mehari', according to documents obtained by Privacy International. But the project largely consisted of facilitating VASTech's interests in Libya.

Company accounts reveal that AGT received over 7.9 million UAE dirham (approximately 1.3 million UK Pounds) between late 2009 and late 2011 marked for a 'Mehari' project. Persons familiar with the payments stated that it was a "paper project" — that the majority of funds VASTech provided to AGT were paid out in consulting invoices to third parties for facilitating VASTech's business in Libya rather than a technical project AGT was responsible for implementing. AGT assisted when VASTech ran into difficulties importing equipment into Libya, according to company accounts and a person with knowledge of the project. Financial records show no indication that 'Mehari project' funds were used to procure any physical equipment or software.

AGT and VASTech did not respond to requests for clarification on the Mehari project. VASTech stated that the company withdrew from Libya in 2011.

The funds provided from this project did, however, allow AGT to finance other parts of the company and pay off urgent bills from increasingly angry creditors. The Libyan funds allowed AGT to continue paying various members of the Chbib family in Syria. A cousin of the family made 25,000 UAE per month (around 50,000 UK Pounds per year) for 'business development' work at AGT. This was still under half of the company director's own salary, excluding the ample housing, car, and holiday allowances the company already paid. Samer Chbib, the Chbib brothers' uncle, facilitated much of AGT's work in Syria and handled large transfers for an 'STE project' in January and February 2010 and throughout the year. At least two other Chbibs based in Syria were engaged profitably in translation and other consulting services.

[53] "Firms Aided Libyan Spies," The Wall Street Journal, 30 August 2011, http://www.wsj.com/articles/SB10001424053111904199404576538721260166388

[54] From December 2009 to January 2010, VASTech ME FZE paid over 5.8 million UAE dirhams (around 978,000 UK Pounds) to AGT. Together this comprised the 'commission' fee AGT received for facilitating the 'Mehari' project. Part of the total sum was paid onward in 'consulting fees' to individuals or companies whose identities Privacy International was unable to confirm. In July 2010, VASTech's Frans Dreyer travelled to Tripoli to 'have a meeting with Mahari [sic]' as part of a regional tour. Mehari – whether referring to a person, a team of people, or an institution – was also referred to as 'Mahri' and 'Mahari'. The code name may derive from the Tripoli hotel popular with foreigners, the 'Radisson Blu Mahari'. AGT received a further sum of approximately 360,000 UK Pounds for a 'Libya project' from VASTech mostly in October 2011. AGT paid out almost all of this in two separate cheques dated one month before earmarked for a "Mehari project".

Libyan business was good but risky money. "[P]lease do not give any Country Name… No country name or clients," Chbib advised one staff member in an email about Libya seen by Privacy International. Many employees were kept in the dark about the company's work outside of their own narrow area, recalled several former employees. "[Anas] Chbib told us not to talk about anything that was going on outside of what we were working on," recalled a former technical employee. "So when we knew he was going to Libya, this sort of thing, we weren't allowed to discuss that." Chbib continued to travel on the 'Mehari' project in late 2011, and into 2012. Libya's fledgling transitional government was struggling to control the country. Fighting erupted two years later, returning Libya to civil war.

Aftermath

The conflict in Syria devastated much of its communications infrastructure. Among the massive population outflux were many of its skilled engineers. Security forces arrested activists and suspected government opponents en masse; hundreds would be arrested, tortured or disappeared. The Syrian Electronic Army, a pro-government hacker militia, engaged in widespread cyberattacks against activists and anti-government groups. Targeted malware, hacking[56] and 'man in the middle' attacks[57] have also been used to identify and spy on dissidents.

The surveillance infrastructure in Syria is still in place, but it is only partially effective and being managed albeit not very effectively by Syrian staff, according to two persons close to the project. The most difficult and complex part of the system to maintain — the probes — requires maintenance that is difficult to accomplish in a highly volatile region where sabotage and damage to the network is rife.[58]

AREA, the Italian company who won one of the major surveillance infrastructure contracts, claims it halted work on the Syrian system.[59] It was also forced to pay a fine to the US Department of Commerce for violating US export control regulations.[60] The company is still active in the Middle East. In June 2016, the Italian government granted AREA a license to export surveillance technology to Egypt,[61] despite an EU joint motion several months prior calling for a suspension in exports of surveillance equipment[62] to Egypt in light of the murder of an Italian doctoral student allegedly at the hands of Egyptian security forces. Italian police raided AREA's offices in December 2016, suspecting violations of European embargoes.[63] Meanwhile, AREA's partner in the Syria project, French company Qosmos, is being investigated by the French courts for possible complicity in torture. The results of that case are still pending.[64]

56 "Behind the Syrian Conflict's Digital Front Lines", FireEye Special Report, 2015, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf

57 "A Syrian Man-In-The-Middle Attack against Facebook", Electronic Frontier Foundation, 5 May 2011, https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook

58 People also managed to work around the government's network surveillance. One computer specialist recalls: "DPI, deep packet inspection, the government benefited from that. It was effective, but going around it took only 10 days after that, and it became known how to go around it…. People would also change, defect with the crisis, within the STE, they were pro-change, so a lot of these services were effected."

59 "Italian Firm Said to Exit Syrian Monitoring Project", Bloomberg, 9 November 2011, http://www.bloomberg.com/news/articles/2011-11-09/syrian-monitoring-project-may-end-as-italy-firm-weighs-options (accessed May 2016)

60 "Italian Company Agrees to $100,000 Penalty for Unlawful Technology Export to Syria", US Department of Commerce, 17 September 2014, https://www.bis.doc.gov/index.php/about-bis/newsroom/press-releases/107-about-bis/newsroom/press-releases/press-release-2014/643-italian-company-agrees-to-100-000-penalty-for-unlawful-technology-export-to-syria

61 "L'Italia esporterà software di sorveglianza in Egitto", La Stampa, 28 June 2016, http://www.lastampa.it/2016/06/28/italia/litalia-esporter-software-di-sorveglianza-in-egitto-11iR9uYFcPpkP9PebyHdwM/pagina.html

62 "Joint Motion for a Resolution", European Parliament, 9 March 2016, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+P8-RC-2016-0338+0+DOC+XML+V0//EN

63 Italian Cops Raid Surveillance Tech Company Accused of Selling Spy Gear to Syria", VICE Motherboar1 December 2016, http://motherboard.vice.com/read/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria

64 "Network surveillance: Qosmos, a tool provider for Syria's leader al-Assad", Reflets.info, 9 May 2014, https://reflets.info/network-surveillance-qosmos-a-tool-provider-for-syrias-leader-al-assad/

As for middleman company AGT, it continues to operate, in part due to investment by Switzerland-based financiers. In April 2015, AGT attempted to broker the sale of intrusion software from Hacking Team to Egypt's military intelligence,[65] despite its poor reputation among industry peers[66] and Egypt's increasingly draconian treatment of journalists, opposition members and activists.[67]

AGT has to date avoided scrutiny of its business dealings, which, as for many other surveillance middleman companies, have remained obscured even from the company's own staff. "I always had the feeling something is not right there," recalls one former employee. "I never really felt good about the business they did. But I never knew anything in detail. If you say [they were] selling surveillance, that would sound like them."

[65] "I: Military Intelligence Egypt", email from E Shehata to Aghiath Chbib, 9 April 2015, available at: https://wikileaks.org/hackingteam/emails/emailid/554337. Accessed September 2015.

[66] "Re: Anas and Ayat from AGT [was: Fwd: MILIPOL Doha 2012]", email from Mostapha Maana to Hacking Team officials, 15 October 2012, available at: https://wikileaks.org/hackingteam/emails/emailid/608555 . Accessed September 2016.

[67] "State repression in Egypt worst in decades, says activist", The Guardian, 24 January 2016, http://www.theguardian.com/world/2016/jan/24/state-repression-egypt-worst-weve-ever-seen-activist-hossam-bahgat

Conclusion

The Syrian government built a surveillance state using Western technology provided by companies and their middlemen at a time when the abuses of the government would have been well known to even the most casual observer. Certain of the surveillance technology suppliers seem happy to have turned a blind eye, or at least not to have sought to know, the conduct of their intermediaries and of the end-users of their products. AGT, as an intermediary, managed to profit from questionable sales to governments, such as to the Syrian government and Libyan government under Colonel Gaddafi, that were publicly engaged in repression.

Privacy International recommends that governments and their relevant authorities:

- Ensure that all relevant surveillance technologies are subject to a licencing regime, which is reviewed on a regular basis. Develop a policy mechanism to efficiently identify products that can be subjected to export licensing with sufficient input from a range of stakeholders, including independent technical experts, academics, and civil society. Particular attention should be paid to ensuring that the inclusion of any technology does not harm security research or otherwise negatively impact the development of the information and communications technology sector.
- Work within existing export control regimes and with multilateral institutions and other states to identify and mitigate challenges to applying and enforcing export control regulations on surveillance technologies, particularly regarding brokering, re-export, incorporation, and diversion issues.
- Ensure human rights criteria are included in export control assessment procedures that are specific to surveillance technologies. Export licences should be denied where there is a risk the surveillance technologies will be used to facilitate internal repression or to otherwise undermine human rights, or if there is no clear legal framework governing their use. Human rights criteria should take into account the human rights record of the end user of the technology, the potential for the technology to be used in a manner not compliant with international human rights standards, the legal framework to regulate the use of the technology by the end user and oversight mechanisms.
- Require companies exporting surveillance technologies to provide clear end-use assurances from their customers in contractual agreements. Those assurances must encompass human rights safeguards and protect against the arbitrary and unlawful use of surveillance technologies.
- Ensure that data about licensing decisions is available to legislative bodies and the public to allow scrutiny and accountability for decisions and to provide information about the surveillance trade. This data should contain the category of license applied for, the category of equipment applied for, details concerning the exporter, details concerning the end-user, the total cost of license applied for, the destination of the export for which the license has been applied for, and the decision by the licensing authority concerning the application.

Privacy International recommends that companies selling surveillance technologies:

- Ensure they have a functioning compliance regime to mitigate against sanctions and export control violations.
- Carry out due diligence research on any potential beneficial end-users prior to agreeing to a transaction.
- Not sell or provide a surveillance product if the potential beneficial end-users of the product cannot be clearly identified or has a documented record of human rights abuse that is likely to be enabled by the product.
- Not sell or provide a surveillance product to a customer if there is no clear legal framework or oversight mechanism governing use of the product within the destination country.
- Stipulate clear end-use assurances in contractual agreements with customers encompassing human rights safeguards and protecting against the arbitrary and unlawful use of the surveillance product.
- Carry out a periodic review of the sale or provision of surveillance products and refuse to carry out maintenance, training, or updates if the end-user does not conform to contractual obligations, including end-use assurances.
- Develop internal policies relating to re-sellers and distributors, and include provisions in contractual agreements with these entities ensuring their adherence to sanctions and export control regulations and to the developer's own human rights provisions.
- Original Equipment Manufacturers (OEMs) should ensure that the company incorporating their equipment adheres to export control regulations and to the OEM's own human rights provisions.
- Commit to and publish strong Corporate Social Responsibility (CSR) commitments conforming to the United Nations' Guiding Principles on Business and Human Rights' in relation to 'human rights'.
- Initiate an annual review of adherence to CSR commitments and international human rights standards and publish its outcomes. Included within this should be strong transparency measures containing, to the greatest extent possible, a list of end-users.

Annex 1

Excerpt from STE call for tenders for a Central Monitoring System, October 2007

FAX

Our Ref : 768 /20/1/1
Date : 2/10/2007

To : AGT
Fax no : 0097143904757
Sub : Technical Tender Book to Central monitoring system for public data network (PDN) and the Internet in the Syrian Arab Republic.

Dear Sirs,

You are kindly requested to submit a trial project of the above mentioned tender according to the technical requirements specified in the enclosed book of conditions.

Please be noted that STE will send the legal and financial book of conditions and the final technical vision of the future network. And later you can submit a financial and technical bid with the legal proving documents per the provision **of law no. 51 of 2004** under condition that the complete bid is to be submitted two weeks after putting the trial project under testing.

Please be noted that all costs resulted from submitting and testing of the trail project will be at your expense.

Waiting for your trial project within /3/ weeks from the date of this correspondence.

Best regards

STE Director General

Annex 1 continued

Excerpt from STE call for tenders for a Central Monitoring System, October 2007

Technical Tender Book to central monitoring system
For public data Network services (PDN) and the Internet
In Syrian Arab Republic

1- introduction:

Syria is considered one of the most growing countries in the Middle East Region concerning the use of Internet. The Public Data Network (PDN) constitutes a complete and integrated infrastructure which was built for this purpose. This network is built over the port wholesale concept.

This increasing growth has imposed many challenges in the face of achieving monitoring requirements which are needed by LEA: Law Enforcement Agencies. It has clearly become necessary to move towards a monitoring system that has the ability to cope with the fast increase in the number of Internet users, in addition to the great diversity of applications.

The aim of this tender is to build a centralized monitoring system which should be independent of the Network, high-performance, highly scalable, and has the ability to meet the monitoring requirements mentioned here in this tender.

The current network contains about 18600 dialup ports, and 3500 broadband ports (DSL) in service. In addition to this, 12500 broadband ports are being installed and should enter service before the end of 2007. The network is expected to scale up to 300 thousand broadband ports and 30 thousand dialup ports by the end of 2008.

Concerning internet services providers, there are seven providers currently connected with the PDN. There are also two providers that own their own independent access networks and international links (which will be later

1

Annex 1 continued

Excerpt from STE call for tenders for a Central Monitoring System, October 2007

of the PDN.

2- **General requirements:**

Bidders are requested to provide a complete offer include the following tasks:

1- Supply of hardware and software needed to meet the requirements mentioned in this tender.

2- Supply, install, and put into operation a complete live testing system over the current network. The testing system will be put under continuous evaluation for a period of 2 months at least, in order to verify its performance and reliability. It should be capable of monitoring a network with about 15.000 broadband ports, and meet all qualitative requirements of the monitoring system. The result of technical evaluation will rely heavily on the output of this live testing.

3- The testing system should be equipped will a requirements for connection with the PDN, and with the ISPs (if it is needed). Two monitoring terminals should be supplied (item 3-7).

4- Provide two levels of training:

   i- Training the users to use and operating the system (30 users).

   ii- Training a number of technicians and engineers on the operation and management of the system which includes complete and partial installation (20 technicians).

5- Provide the necessary upgrades to meet expansion requirements as they are explained in the annex. These upgrades should be provided within a period of 4 months after the notification to the bidder.

6- Repair or replace failed equipment within a period of 48 hours maximum.

2

Annex 1 continued

Excerpt from STE call for tenders for a Central Monitoring System, October 2007

asked to provide a clear and detailed description of testing steps and procedures, along with a sample of the resulting report.

8- The bidder must commit to provide spare parts for the system equipment for a period of 10 years at least. In case the provider cannot commit to this, the system should be able to work over alternative standard equipment (e.g. Inter-based servers) and without a performance drop exceeding 10%. The bidder should prove this through direct testing.

9- The bidder should provide as a mandatory part of his answer, a list of compliance statements including detailed response to each of the technical points in this tender book. The bidder may use only one of two possible answers : compliant, or Not compliant (partial compliance is considered as not compliant). All the conditions are considered mandatory (except conditions where it is stated clearly that "it is preferable"), and non-compliance of one of them may lead to disqualification of the offer.

10- The bidder has to offer a detailed technical design explaining the different stages of capturing, collecting, analyzing and storing the data. He has also to mention clearly the eventual bottlenecks and the means of expansion, along with a detailed description of the protocols used in the system and their compliance with international standards. Priority is given to the standards of ITU, the standards of IETF and then the standards of ETSI.

11- The system will be put into service in two phases: the first phases covers the current network and it should be done as soon as possible. The second phase aims at covering the system that will have been installed bye the end of 2008.

3

Annex 1 continued

Excerpt from STE call for tenders for a Central Monitoring System, October 2007

should start immediately after obtaining commencement order.

i- Supplying of the equipment.

ii- Training of users (technical).

iii- Installation of monitoring system to the current network and put it into operation.

iv- Installation all centralized parts of the system needed for monitoring upon achieving the expected capacities at the end of 2008.

- The second phase: monitoring of the future network which will be executed after the kickoff of the expansion project. The final design for the network will be provided to the bidder in order to proceed with the implementation.

The bidder is asked to provided the detailed set of hardware, software, and various tasks which need to be carried on during each of these phases.

3- The technical requirements:

3-1- general requirements

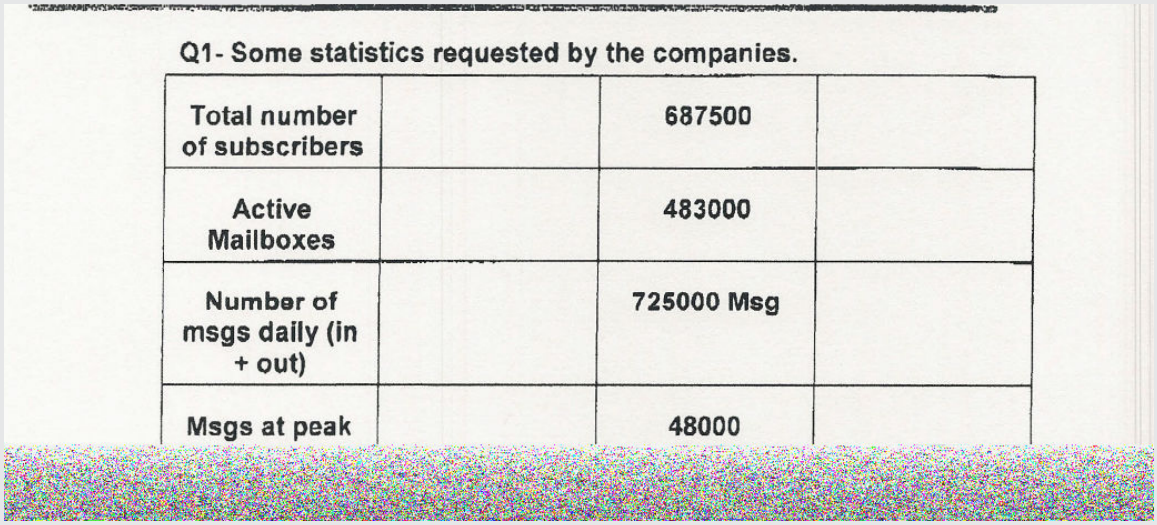
1- The system must be centralized and has the ability to monitor all the networks which use data communication services inside the Syrian territories and with all its different forms as follows:

- Different entities linked to the PDN including service providers and other corporate networks.
- ISPs which are not connected to the PDN.
- The entities which have data networks not connected through the PDN (e.g. using leased lines to connect between branches)

4

Annex 2

Excerpt from STE requirements for Content Filtering project, April 2009



Q1- Some statistics requested by the companies.

Total number of subscribers		687500	
Active Mailboxes		483000	
Number of msgs daily (in + out)		725000 Msg	
Msgs at peak		48000	

Annex 2 continued

Excerpt from STE requirements for Content Filtering project, April 2009

shall not be blocked at the IGW level, it is up to the bidder to find the right solution to block the propaganda email as specified in the RFP.

Q3
Do you know the splitting of messages per language?
Response: Unfortunately, this information is not available.

Q4
Can you provide us the maximum number of keywords that would be configured as blocking criteria and the number of messages.
Response: Our experience varies greatly, at one moment, the total accumulated size of mail messages over 3 days reached 70GBs. Given that we are not the authors of these messages, we cannot give a firm figure for the blocking criteria. Please specify the number that your proposed solution could handle currently along with the potential for expansion.

Q5
Referring to ANNEX1 IGW network diagram, please indicate the following information
-exact physical positioning of monitoring points, specifying if they are located in different sites of the same city or they are in distinct cities. For instance could be acceptable to monitor 10GE interfaces of IGW distribution routers toward the core network.
Response: We leave this choice totally to the bidder, although we don't really see any need to have monitoring points located in different cities. The bidder should do his best to come with a solution which is mostly (if not fully) deployed at the IGW. We don't mind that the 10GE interfaces of IGW distribution routers toward the core network be monitored provided that all the RFP requirements are implemented and met.

Q6
-Number, type and characteristics of links to be monitored.
Response:
The links are explained in the diagram, we attach an updated one which contains the final diagram.

Annex 2 continued

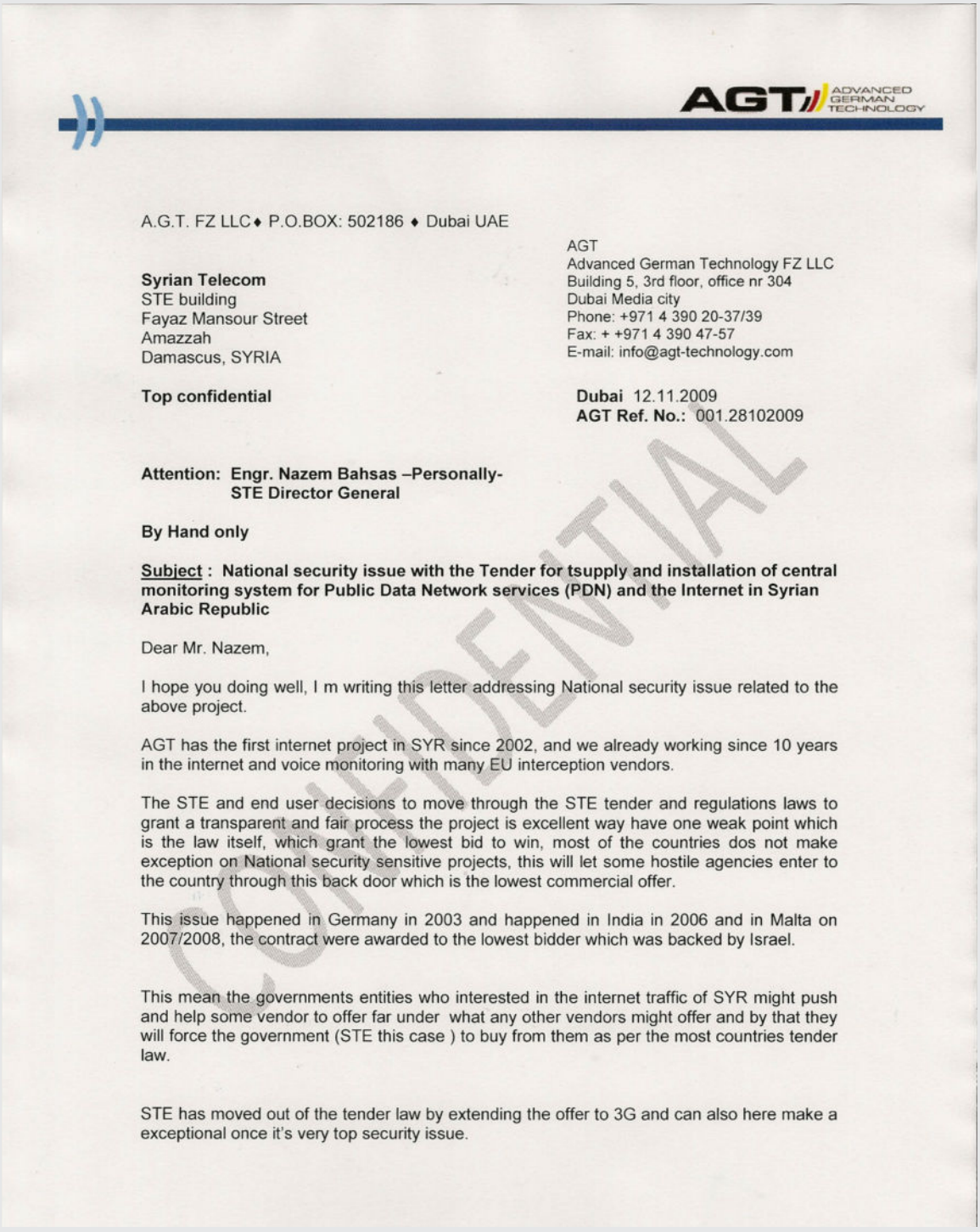
Excerpt from STE requirements for Content Filtering project, April 2009

Q7
Does STE plan to have well defined links when the project will start or will links gradually change (e.g. initially 8 STM-1, then 4 STM-4, finally four STM-16).
Response:
We don't have any specific plans, but given that bandwidth is increasing, it is logical that STE will move to higher density links on the mid and long term.

Q8
In the links to monitored, what're the traffic volumes estimations based on application type (e.g. how much is the SMTP traffic in the 1 GB trunk ? How much the Webmail one, And so on).
Response
Unfortunately this information cannot be provided.

Annex 3

Letter from AGT to STE asking to be reconsidered for Central Monitoring System project, November 2009



AGT ADVANCED GERMAN TECHNOLOGY

A.G.T. FZ LLC♦ P.O.BOX: 502186 ♦ Dubai UAE

Syrian Telecom
STE building
Fayaz Mansour Street
Amazzah
Damascus, SYRIA

AGT
Advanced German Technology FZ LLC
Building 5, 3rd floor, office nr 304
Dubai Media city
Phone: +971 4 390 20-37/39
Fax: + +971 4 390 47-57
E-mail: info@agt-technology.com

Top confidential

Dubai 12.11.2009
AGT Ref. No.: 001.28102009

Attention: Engr. Nazem Bahsas –Personally-
STE Director General

By Hand only

Subject : National security issue with the Tender for tsupply and installation of central monitoring system for Public Data Network services (PDN) and the Internet in Syrian Arabic Republic

Dear Mr. Nazem,

I hope you doing well, I m writing this letter addressing National security issue related to the above project.

AGT has the first internet project in SYR since 2002, and we already working since 10 years in the internet and voice monitoring with many EU interception vendors.

The STE and end user decisions to move through the STE tender and regulations laws to grant a transparent and fair process the project is excellent way have one weak point which is the law itself, which grant the lowest bid to win, most of the countries dos not make exception on National security sensitive projects, this will let some hostile agencies enter to the country through this back door which is the lowest commercial offer.

This issue happened in Germany in 2003 and happened in India in 2006 and in Malta on 2007/2008, the contract were awarded to the lowest bidder which was backed by Israel.

This mean the governments entities who interested in the internet traffic of SYR might push and help some vendor to offer far under what any other vendors might offer and by that they will force the government (STE this case) to buy from them as per the most countries tender law.

STE has moved out of the tender law by extending the offer to 3G and can also here make a exceptional once it's very top security issue.

CONFIDENTIAL

Annex 3 continued

Letter from AGT to STE asking to be reconsidered for Central Monitoring System project, November 2009

Annex 4

Excerpt of AGT-VASTech proposal for brute force voice identification of phone users in Syria, July 2009

AGT ADVANCED GERMAN TECHNOLOGY

VASTech

Evaluation of the practicality of brute force Speaker Identification in massive sets of calls

Proposal of an alternative approach that is more practical and provides an improved benefit:cost ratio

Annex 5

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

Index

1 RCS/AGT Proposal to SCT 4
1.1 Overview 4
1.2 RCS Capability 6
1.3 Solution Deployment 6
1.4 Network Scenario 6
1.5 Logical Architecture 7
2 Probing Subsystem 7
2.1 AM Element Manager 8
2.2 Provisioning 9
2.2.1 Static-IP 9
2.2.2 Keyword 9
2.2.3 VoIP 9
2.2.4 User: 9
2.2.5 DHCP 10
2.2.6 DNS 10
2.3 Diagnostic and alarms 10
2.4 Management and maintenance 10
3 Monitoring Subsystem 10
3.1 Architecture 11
3.2 IP Traffic reception 11
3.3 IP Traffic decoding 11
3.3.1 Web 12
3.3.2 Email 12
3.3.3 Chat 12
3.3.4 File transfer 12
3.3.5 Audiovideo 13
3.4 IP Traffic presentation 13
3.5 Production of forensic archival copies of the traffic 14
3.6 Authentication 14
3.7 IP traffic storage 14

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

4 Physical Arrangement 15
4.1 Target number 15
4.2 TIP 16
4.3 IVS distributed system 16
4.3.1 Backend IVS 17
4.3.2 Frontend IVS 17
4.4 Clients 18
4.5 Physical arrangement 18

Figures

Figure 1 "RCS Layered solution" 5
Figure 2 "Network Scenario" 7

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

1 RCS/ AGT Proposal to SCT

This document has been prepared to be a proposal according to SCT requirements. RCS /AGT reserves the right to review this proposal should this assumption be incorrect. The system proposed in this document is a comprehensive telecom monitoring solution to be implemented in order to provide a monitoring coverage of SCT Internet Service Provider, with particular regards to the Satellite one way connectivity.
The proposed system is ready for future expansion, upgrade and adding of optional capabilities and functions.

The proposed system is based on the state of the art solution

- AM (Administration Module - Element Manager)
- IVS (Internet Visualization System)
- TIP (Tactical IP Probe).

Key points of these products are:

- Flexibility
  - They can be used over any kind of IP networks -including tunnelized networks- conveyed by several different media (including Satellite)
- Scalability
  - The solution (HW and/or SW) can easily be upgraded to manage an increasing requirements in terms of number of Interceptions, bandwidth, depth of analysis.
- Ease of use
  - The solution has been designed with an advanced GUI in order to be extremely user-friendly.

1.1 Overview

The following Figure 1 "RCS Layered solution" shows how RCS covers layered structure (as per RCS Model of Unified LI System) to provide solution to SCT.

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

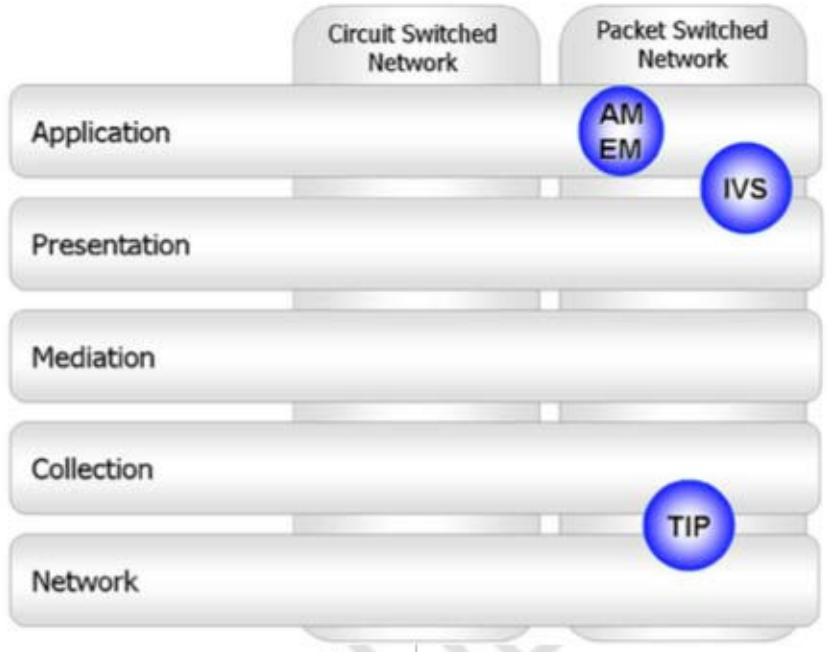


Figure 1 "RCS Layered solution"

Application - Warrant processing, target setup, network management., information collection & analysis.

Presentation - Modifying all data and communications protocols and formats into a form understood by the application layer and vice-versa

Mediation - Communication and interfacing with the collection and presentation layers to control and manage the diverse network elements that would form the core of the unified solution

Collection - Collecting the required data and information from the targets identified within the diverse operator and service provider networks

Network - Equipment that interfaces and connects into the service provider or operator network.

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

1.2 RCS Capability

RCS products, described below, are deployed in many countries. RCS has many years of experience in not only supplying equipment, but also wide range of services:

Consultancy on LI solutions
Site survey & site preparation (provided by RCS engineers or certified local companies)
Installation, configuration test and commissioning (provided by RCS engineers or certified local companies)
Training on customer site (provided by RCS trainers)
Support
Maintenance
Security audit
Project management

1.3 Solution Deployment

RCS designed the solution here detailed granting the best trade-off in terms of

Security
Scalability
Cost effectiveness

1.4 Network Scenario

The project has been designed taking into account information provided by SCT reported in the Figure 2 "Network Scenario".
RCS reserves the right to review the proposal should this assumption be incorrect.

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

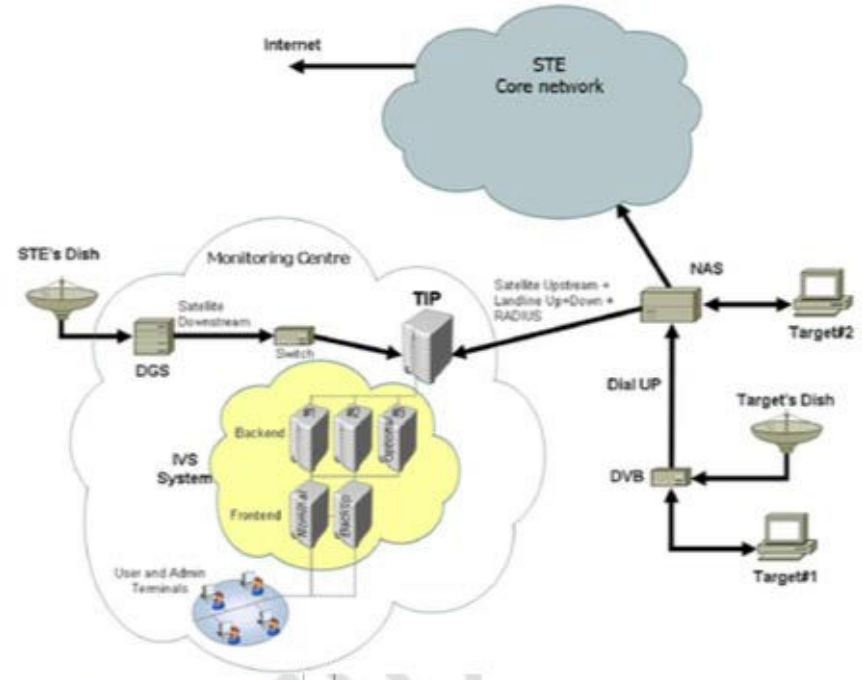


Figure 2 "Network Scenario"

1.5 Logical Architecture

The proposed solution is designed to analyze and eventually intercept the traffic exchanged by SCT's subscribers: all the traffic is analyzed at wire-speed by the ***Probing Subsystem*** and the relevant one is saved in standard PCAP files when the content match with one or more configured interception rules.

Seized traffic is delivered in realtime to the ***Monitoring Subsystem***, where PCAP files are recorded, stored and decoded.

2 Probing Subsystem

The proposed probing subsystem lean on the well established RCS's Tactical IP Probe (TIP), a 1+1Gbps single server software based interception Probe already used in many contests. RCS's TIP runs over COTS [Commercial-Off-The-Shelf] hardware (see the following paragraph §4.2 for

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

details) with Linux operative system, allowing an easy system management with scripts or standard software.

RCS's TIP includes the following capabilities:

Network sniffing

Wire-speed packet filtering and collection

Mediation to the Monitoring Subsystem

The probe is connected in a passive way, receiving a copy of the "to be monitored" packet streams. The traffic replication can be done by mean of a mirror (span) port or through physical "tapping" (optical or electrical) of the identified connection.

The proposed TIP probe are ready to receive Ethernet packets, meaning that wiretapping over different transport network -such as ATM or SONET- require a review of the current offer. Moreover, they are able to handle both L2TP-tunnelized and not-tunnelized (plain) IP packets, allowing to intercept targets belonging to "hosted ISPs".

Packets are saved in PCAP standard format with precise timestamp: for this reason, TIP servers periodically synchronize the internal clock to a master NTP server.

2.1 AM Element Manager

The proposed administration solution, is based on RCS's AM Element Manager modules.

This software module is hosted by the TIP server, and is accessed as a secured website through a normal web browser.

Included functionalities are:

- Provisioning of the interception targets
- Diagnostic and alarms
- Management and maintenance

An authentication system guarantee both the security and the desired visibility of data: different users can be configured to have access only to the desired function (provisioning, monitoring, administration...), maybe from different clients located in different premises: for example an investigator can access the system from the LEA client for provisioning purposes -without having access to the network configuration page-, while a technician is accessing the system from a local client for monitoring the CPU usage -without seeing any target-related data-.

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

2.2 Provisioning

The administration system includes the capability to configure the interception elements (Probes and IVS) in order to provide the interception of targets.

The system has two classes of interception targets: **user** and **content**

The following paragraph describes the Target allocation for all the target types supported by the system.

2.2.1 Static-IP

Triggers interception upon any IP-level parameter match. Typical applications :

- Interception of static IP-address users, a range of IP-addresses, some specific IP-ports over a certain IP-address range.

AND+OR chains of rules can be easily implemented.

2.2.2 Keyword

Triggers interception upon keyword match on reconstructed IP flows Typical applications:

- interception of keyword spotted emails, web pages, webmails, chats.

Keywords can be strings or regular expressions ("bomb", info@easygain.com, [Ff]errari, any word...) Flow reconstruction and keyword search are done upon a pre-filtered subset of the whole traffic: pre-filtering rules are specified using "Static-IP" parameters. unmatching flows are discarded after they reach a settable threshold (typical: 512KByte)

2.2.3 VoIP

Triggers IP/RTP interception upon SIP/H.323 user match: URI, alias. Typical applications:

- interception of the VoIP calls from/to a VoIP number, a country/area...

2.2.4 User:

Triggers IP interception upon Radius authentication parameter match: username, NAS-port-ID (line identifier). Typical applications:

- interception of an ADSL user, a Dialup user

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

2.2 Provisioning

The administration system includes the capability to configure the interception elements (Probes and IVS) in order to provide the interception of targets.

The system has two classes of interception targets: **user** and **content**

The following paragraph describes the Target allocation for all the target types supported by the system.

2.2.1 Static-IP

Triggers interception upon any IP-level parameter match. Typical applications :

- Interception of static IP-address users, a range of IP-addresses, some specific IP-ports over a certain IP-address range.

AND+OR chains of rules can be easily implemented.

2.2.2 Keyword

Triggers interception upon keyword match on reconstructed IP flows Typical applications:

- interception of keyword spotted emails, web pages, webmails, chats.

Keywords can be strings or regular expressions ("bomb", info@easygain.com, [Ff]errari, any word...) Flow reconstruction and keyword search are done upon a pre-filtered subset of the whole traffic: pre-filtering rules are specified using "Static-IP" parameters. unmatching flows are discarded after they reach a settable threshold (typical: 512KByte)

2.2.3 VoIP

Triggers IP/RTP interception upon SIP/H.323 user match: URI, alias. Typical applications:

- interception of the VoIP calls from/to a VoIP number, a country/area...

2.2.4 User:

Triggers IP interception upon Radius authentication parameter match: username, NAS-port-ID (line identifier). Typical applications:

- interception of an ADSL user, a Dialup user

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

2.2.5 DHCP

Triggers IP interception upon MAC-address or Modem-ID match. Typical applications:

- Interception of a cable-modem user

2.2.6 DNS

Triggers IP interception upon Server-Name match. Typical applications:

- interception of an Internet Server regardless if its address is static or not

RCS is available to provide separate quotation for any further requirements issued by SCT.

2.3 Diagnostic and alarms

The administration solution includes a diagnostic system that collect all the alarms gathered from the TIP. The alarms can be:

- System alarms (i.e. HW failure)
- Performance alarms (i.e. input bandwidth exceed the nominal one)
- Activity alarms (i.e. one specific interception target log in)

The notification can be by SMS, email or the AM alarm console.

2.4 Management and maintenance

The administration solution includes a management system that enables to check the performance of the interception system and allows maintenance activity.

3 Monitoring Subsystem

The Monitoring Subsystem is the central Law Enforcement Monitoring Facilities from which the LEA intends to decode and inspect the intercepted data. The proposed solution is based on IVS (Internet Visualization System) that is a client server architecture, and both clients and servers have conveniently been located into the Monitoring Center, but other combination are suitable, provided that the necessary network connectivity (may be a VPN) between sites is guaranteed.

The main functionalities implemented in the Monitoring Subsystem are:

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

- IP traffic reception;
- IP traffic decoding;
- IP traffic presentation;
- Production of forensic archival copies of the traffic;
- IP traffic storage;

3.1 Architecture

The proposed Monitoring Subsystem is a Client-Server system that stores all the target-based intercepted data on the server storage for security and privacy reasons.

The clients are MS-Windows based Personal Computer and they retain only the web-based application needed to browse decoded contents. Data are dynamically downloaded from the IVS and they remain present in the client workstation only for the time needed to view it.

Firmly based upon RCS experience in investigative activity, IVS is a scalable modular platform which follows the development of Internet applications.

The current proposal include five IVS server, the characteristics of which are described in the following paragraph §4.3.

3.2 IP Traffic reception

Data sent by TIP probe, is received by IVS in standard PCAP format. The transfer can be in realtime (streaming ETSI) or as batch file transfer.

The recording speed is the one allowed by the network connection.

3.3 IP Traffic decoding

The system is able to identify thousands of different IP protocols and decode the most popular and relevant of them.

More than 4000 internet protocols are recognized and classified (tagged), while the following are decoded:

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

3.3.1 Web

- HTTP
- MMS (.mms file + multimedia contents)

3.3.2 Email

- SMTP
- POP3
- IMAP4
- NNTP
- EML (.EML files - RFC_822)
- WEBMAIL:
  - Hotmail
  - Yahoo!
  - Gmail
  - All standard webmail are presented as Web pages

3.3.3 Chat

- MSN
- IRC
- YAHOO
- ICQ
- C6
- Paltalk
- Volano (web chat)
- Terra (web chat)
- Lycos (web chat)
- Gtalk (web chat)

3.3.4 File transfer

- FTP
- EMULE
- MSN
- IRC
- YAHOO
- ICQ

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

- C6
- Paltalk

3.3.5 Audiovideo

- H323
- SIP
- MSN Video Call
- YAHOO Video Call
- Paltalk Audio
- Paltalk Video
- Icq Audio

3.4 IP Traffic presentation

Designed to fit the requirements of users with different technological skills, IVS is a flexible tool whose employment is within occasional users reach but, at the same time, ensures full support to skilled users.

After decoding, the operator's access to the intercepted communications may be carried out in any of two supported methods:

- Offline Browsing, that allows to review all the data accumulated for a given target (or set of targets);
- Online browsing, that allows to observe the activities of a single target in real-time (the display window follows the actual activities of the target whenever he is connected to the Internet)

The decoded data are immediately graphically displayed as though the operator was in front of the target's monitor.

When the investigation is run by qualified personnel, this effortless usability accelerates the analysis, enabling the operator to find quickly on screen the most important pieces of the IP communication.

At the same time IVS can also present detailed views of the same traffic enabling the analysts to examine the deep structure of gathered information.

IVS client application allow the user to manage Investigation activity providing a suite of useful tools like as:

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

Search function

Possibility to set a relevance for any Item and Session

Possibility to edit a Digest for any Item

Fast filtering and sorting on different Item Types

Report generation for export or printout

Beside IVS's client application functionalities, Windows's standard tools are available for saving, printing, playing any kind of resources.

3.5 Production of forensic archival copies of the traffic

The system provides the functionality of archiving the traffic data from any IVS workstation by every user that has the needed right (interception administrator), based on authentication.

The archiving is made by optical disks that contain the raw and decoded data, in a format that can be easily browsed by any browser (i.e. without the need of a any special application, and over any platform like MS-Windows, Linux, MAC-OS...), providing a kind of GUI similar to the online IVS.

3.6 Authentication

The access authentication for the workstations, both users and administrative, is by username/password, or optionally by smartcard.

3.7 IP traffic storage

All the received data are stored as raw PCAP files in the server storage, as well as the decoded resources (web pages, audio files, images...). IVS keeps both the raw and decoded data for matching two binding requirements:

- realtime responses to user queries on decoded data
- possibility to reprocess (re-decode) raw traffic after a decoder update.

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

4 Physical Arrangement

4.1 Target number

Based on RCS' 20 years of experiences in the LI solutions provider, and having many of the top worldwide countries as clients, we can confirm that the size of a monitoring system has to be calculated following two main concepts:

Target/Subscriber ratio (also known as "interception rate")

Target/Operators ratio

For the interception rate, the maximum value ever seen in all European and Extra-European countries is 1:2000 (i.e.: 1 target each 2000 subscribers). Considering the special context of this project, with the need of content-oriented monitoring, we considered for this project a ve



Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

Anyway is also important to understand that the mentioned values are not rigid limitations on the system: due to the modular architecture, RCS' system can be easily scaled up whenever there is the need.

4.2 TIP

The proposed TIP probe have the following features:

TIP Features

- ***Probe Platform:*** *one Dual Xeon Intel server (DELL PE2950)*
- ***Input Interfaces:*** 2*1GbE (electrical)
- ***Filtering Throughput:*** wire-speed
- ***Pre-processor Forwarding:*** 50Mbps max.
- ***Keyword/email/chat search capability:*** 20Mbps max.
- ***Targets:*** 75 max.
- ***Keyword search Targets:*** 20 max.
- ***Rules:*** 100 max
- ***Alerting:*** email and SMS support for both alarms and interception events

CONFIDENTIAL

4.3 IVS distributed system

As depicted in Figure 2 "Network Scenario", the IVS architecture is split in two layers:

Backend IVS:

Frontend IVS

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

Let's go through the distinction between the two layers.

4.3.1 Backend IVS

It's a processing server hosting the recording and decoding functionalities. Each server can handle up to 25 targets. The recorded file and the decoded resources are stored in the Frontend IVS storage, like so the database information that are remotely stored inside the Frontend IVS database.

The Backend IVS does not keep any stored information, so it doesn't need to be backupped.

Backend IVS Features:

- ***Platform:*** Dual Xeon Intel server (DELL PE2950)
- ***Number of Targets:*** 25 max

4.3.2 Frontend IVS

It's the server hosting the database and the presentation functionalities (WAS). A single server can handle up to 75 targets and 15 operator clients.

The Frontend IVS do store sensitive data, so in order to increase the availability of the service, it should be backupped by an hot-standby IVS Frontend Backup server.

The Backup server is autonomously responsible to keep its storage aligned to the Master server's one.

Frontend IVS Features

- ***Platform:*** Dual Xeon Intel server (DELL PE2950)
- ***Number of Targets:*** 75 max

CONFIDENTIAL

Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009

- ***Number of Clients:*** 15 max
- ***Direct attached storage:*** 3TByte

4.4 Clients

- ***IVS client:*** "state of the art" PC with DVD reader/writer

4.5 Physical arrangement

The proposed system consists in:

- 1 (one) TIP probe with AM - Element Manager
- 1 IVS System composed by
  - 2 (two) IVS Backend servers: working in load sharing on up to 50 targets (expandable to three servers, for managing up to 75 targets)
  - 2 (two) IVS Frontend servers: one as Master, one as hot-standby with storage backup
- 10 IVS Clients access capability

CONFIDENTIAL

Annex 6

Response from AGT, December 2016.

From: **Anas Chbib [AGT]** achbib@agt-technology.com
Subject: Re: Your messages from this morning
Date: 7 December 2016 at 07:15
To: Claire Lauterbach claire@privacyinternational.org
Cc: Aghiath Chbib [AGT] agchbib@agt-technology.com

AC

Dear Mr. Lauterbach,

thanks for your mail, I would to help you as much as I can to provide accurate statements.

I would like to assure you that AGT dos not own any surveillance technology, and we have been exiting the business of Lawful interception services, few years back, however we have been following all the export regulations related UN, and EU, having said that the technology suppliers are resonsible for the export license approval if its needed, and so far we have been never entered to any selling of technologies, where the export licenses has been not approved, if one were needed, please note till few years back majority of surveillance technologies solutions, a export licenses were not required, I m sure u are aware about it.

please find my comments to the inquiries you send:

1- we have been requested to offer, but we did not sell the RCS surveillance technology for that project.

2-this not accurate as we did not have such technology that time

3-yes we had offered but we did not sell at the end to them

4-internal issue of AGT (private) : Mr. Frans has pass away few years back, its accurate and has nothing to do with any project or export of any technologies.

5-its internal network forensic tool: has with public surveillance tool nothing to do, this for sure

it might happens, but there will be no sells to any account without getting the export license approval, and its mandatory in all our final quote, or sales process, adding to that, if we would do it, its the vendor responsibility to obtain the export license, and not the seller, and at the end its south African compnay, MTN is telecom operator with many location and licenses, if they wanted to use network forensic tool to identify any malware in the network, than its internal issue, this tool is not been made be installed on public networks.

6-this not accurate, it might be RFI or RFQ but never sold.

7-never sold, and if its offered the HW, it is local supply issue, and we can not, will not involve in any importing of HW like dell or others, to any country, not only Syria, beside it was available in SYRIA without any involvement of AGT, as we are not hardware vendor nor distributor.

8- AGT has large portfolio of services and offering around IT, for that : yes we are involved in more than 34 countries, from Data center, Digital forensic to Cyber security defenses tools and related IT services, we have been out of the Lawful interception business for few years back, and focusing on cyber crime investigation, and fighting crimes such drugs, anti terror, human trafficking, human part trafficking cartels etc..

9. AGT has never met the gentleman, and there is no business what so ever with Sudan(north of south) since the compnay was established till this moment.

10- we worked with Vastech, and again there was no breach of any international law on that.

11- this is privat issue related to some investment in the UAE in a very far sector from technology.

14- this bite private issue, and could harm the persons related -only by name - to our family, by providing such statements, they could be put in very unpleasant and dangerous positions, just because of your reports, please send me the names u have to comments on them one by one, as is very general statement, and there is few Chbib working in AGT since 2002, as e.g. in EGP, and in Dubai.

please let me know if you need any clarification, or help

looking forward to hear from you, by the way some journalist from USA has wrote to us about your report ? it public already ?
rgds
Anas

> On Dec 5, 2016, at 15:16, Claire Lauterbach <claire@privacyinternational.org> wrote:
>
> Dear Mr. Chbib,

Annex 6 continued

Response from AGT, December 2016.

> On Dec 5, 2016, at 15:16, Claire Lauterbach <claire@privacyinternational.org> wrote:
>
> Dear Mr. Chbib,
>
> Thank you for your messages of this morning.
>
> As explained in our letter, we are eager to have AGT's views on the issues we raise so as to accurately reflect your position. We request that you raise these issues in writing (by email) so as to maintain an accurate record of your company's views. I regret that we will be unable to discuss these matters orally.
>
> Privacy International is a UK-registered charity. We engage in research, advocacy and litigation on issues in the public interest. The provision of surveillance technologies to governments publicly engaged in repression is one such public interest issue on which we are active.
>
> Our research methods conform to accepted journalistic and public interest research standards. As such we invite you to correct, clarify, or otherwise respond to the key statements we will make.
>
> We would be grateful for your written response to the issues raised in our December 1 letter by the deadline indicated in the letter.
>
> Yours sincerely,
>
> Claire Lauterbach
> Researcher
> Privacy International
> +44(0)2034224321

Mit freundlichen Grüßen / With best regards
Anas Chbib
CEO and Group founder

Advanced German Technology GmbH /