PRIVACY INTERNATIONAL

THE PRESIDENT'S MEN?

Inside the Technical Research Department, the secret player in Egypt's intelligence infrastructure



Privacy International wants to thank the individuals who have helped us with this investigation and who cannot be named. A handful of these individuals took significant risks to share information with us, for which we are very grateful.

This report is primarily based on original documentation provided in confidence to Privacy International.

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

We have contacted the following companies in the development of this report: Advanced German Technology (AGT), A6 Consultancy, GNSE Group, Hacking Team, Nokia Group, Siemens, Solve IT and Universal Advanced Systems. Additionally, we have contacted the Egyptian Government. Attempts to reach Egyptian German Telecommunications Industries (EGTI) were unsuccessful.

THE PRESIDENT'S MEN ?

Inside the Technical Research Department, the secret player in Egypt's intelligence infrastructure

February 2016

PRIVACY INTERNATIONAL

www.privacyinternational.org



Official emblem of the General Intelligence Directorate at the front of its headquarters in Cairo. This is the only image Privacy International could find of GIS headquarters.

Photo: Attractionist Arabic Wikipedia

Introduction

Intelligence agencies now play a central role in governments' security apparatus. When unchecked, their roles become more vague, their capabilities grow dramatically, and their purposes expand beyond the security of the people. In undemocratic countries, the security of the government quickly becomes the priority.

The story of Egypt's intelligence agencies is tied up with Egypt's history of autocratic rule. While more is becoming clear about Egypt's intelligence agencies we are finding that there are some elements of the intelligence community that have escaped scrutiny to date. This Privacy International report sheds light on the existence of the Technical Research Department (TRD), a secret unit that most likely sits within the Egyptian General Intelligence Service (GIS). The TRD has come to our attention because of their extensive ambitions to purchase surveillance technologies. We have uncovered evidence of a number of European surveillance companies that have been dealing with the TRD. Throughout the recent history of autocratic rule and revolution, the TRD's role has continued unabated in the shadows.

This Privacy International report exposes the TRD, a secret key player in the world of Egyptian intelligence, and documents the capabilities the TRD has obtained from Western companies – including Nokia Siemens Networks (NSN) and Hacking Team – who have sold them sophisticated surveillance technologies, even as Egypt was, and indeed still is, in the throes of violent conflict.

Egypt's intelligence apparatus

The national intelligence agencies comprise the GIS (Al-Mukhabarat Al-Amma), the Military Intelligence and Reconnaissance Administration (Al-Mukhabarat Al-Harbeya), the National Security Service (Mabaheth Alamn Alwatany), and the Administrative Control Authority (Ar-Raqabaal-Idareya).

Gamal Abdel Nasser, Egypt's second president greatly influenced Egypt's current intelligence infrastructure. With the coup in 1952, he planned to make Egypt a leading player in the emerging Non-Aligned Movement of African and Asian States. He decided he would need a service that would facilitate his agenda through covert action and act as the eyes and ears of Egypt. The Military Intelligence Department was at the time focused on Israel, the main military threat. It was roughly around that time that the GIS was created to fulfil this new mission of conducting non-military covert operations.[1]

1 O Sirrs. A History of the Egyptian Intelligence Service. Routledge Taylor & Francis Group, London and New York, 2010, p. 41

The most internationally recognised intelligence agency is Egypt's National Security Service, an intelligence unit inside the Ministry of Interior. In 2011, it was purportedly dismantled following the Arab Spring uprising that ended the Government of then-President Hosni Mubarak. It was deemed responsible for much of the oppression and many of the human rights violations under the Mubarak Government.[2] The dissolution of an intelligence agency is a rare act, and is often in recognition of a significant need for change. Nonetheless, the National Security Service was restored in 2013 by the interim Government of Adly Mansour following the overthrow of the Muslim Brotherhood, and in advance of the Sisi Government.[3]

The GIS, meanwhile, is the main intelligence agency in charge of providing both domestic and foreign intelligence. Located in the district of Kobry El Koba in Cairo, the GIS is not attached to a minister, it is accountable only to the president,[4] who appoints the head of the GIS.[5]

While most of the intelligence agencies described above have a clear mission and publicly known heads of staff, the TRD operates in total secrecy – so secretive indeed that its existence appears to never have been publicly avowed by the Egyptian Government.

2 Egypt dissolves notorious internal security agency", BBC, 15 March 2011, http://www.bbc.co.uk/news/world-middle-east-12751234

3 "Egypt restores feared secret police units", The Guardian, 29 July 2013, http://www.theguardian.com/world/2013/jul/29/egypt-restores-secret-police-units

4 "General Intelligence Service (GIS) Mukhabarat", GlobalSecurity.org, http://www.globalsecurity.org/intell/world/egypt/gis.htm

5 "El-Sisi visits General Intelligence Service headquarters", Ahram Online, 1 January 2015, http://english.ahram.org.eg/NewsContent/1/64/119293/Egypt/Politics-/ElSisi-visits-General-Intelligence-Service-headqua.aspx

Shedding light on the shadows: TRD in context

A history of political repression

Although its exact creation date is unclear, according to an intelligence expert who spoke with Privacy International, the TRD was created under President Hosni Mubarak, as a unit within the GIS that would be accountable directly to him only. Between 1981 and 2011 Mubarak headed a heavily corrupt political regime.

Mubarak reportedly created this unit to ensure that his administration could keep political opponents in check. It was apparently created as an autonomous unit within the GIS - a unit the President could go to, for instance, when the GIS refused to conduct certain activities.

It is, however, unclear when exactly the TRD was created. Dates listed in documentation we have seen in fact suggest that the TRD was already in place under Anwar Saddat, Hosni Mubarak's predecessor.

Regardless of when it was set up it is nonetheless clear that the TRD reflects a historical tendency in Egypt in which heads of state rule with an iron fist, even against highly ranked members of government. After taking office, Sadat imprisoned two of the most powerful figures of the former administration: the Minister of Interior, Sharawy Gomaa, in charge of the secret police; and the Vice President, Ali Sabri.

In February 2011, the government of President Hosni Mubarak fell under the pressure of the protests sweeping across the region. The TRD was unaffected. That year, the TRD purchased a monitoring centre and interception management system, important infrastructure for carrying out interception of telecommunications networks.

After the fall of Mubarak, the Supreme Council of the Armed Forces, the interim military government, ruled the country until June 2012. The Freedom and Justice Party, formed by the Muslim Brotherhood, took office after a democratic election that had taken place that month. In November 2012, President Mohammed Morsi suspended the constitution. Less than a year later, in July 2013, the military led by Colonel General Abdel Fattah el-Sisi overthrew the new government in a coup.[6]

The new government promptly outlawed the Muslim Brotherhood as "a

6 "Egypt: Abdul Fattah al-Sisi profile", BBC, 16 May 2014, http://www.bbc.co.uk/news/world-middle-east-19256730

7 "Egypt's Muslim Brotherhood faces election ban", Al Jazeera, 15 April 2014, http://www.aljazeera.com/news/middleeast/2014/04/egypt-muslim-brotherhood-faces-election-ban-201441515542699473O.html

terrorist organisation". Its members were banned from standing during future elections.[7] Sisi first appointed Adly Mansour, then the chief justice of the Supreme Constitutional Court, as an interim president. In June 2014, Sisi officially took the reins following a presidential election that he won with 96% of the vote.[8]

The Muslim Brotherhood and alleged associates of the organisation have been severely repressed since the Sisi government took power, according to human rights organisations. Human Rights Watch has called the Rab'a Killings –the killing of at least 1,150 protesters in August 2014 –"a crime against humanity".[9]

Repression continues unabated. Non-governmental organisations (NGOs) and activists in Egypt have faced further crackdowns. Law 107 of 2013, on the Right to Public Meetings, Processions and Peaceful Demonstrations bans protests in Egypt. This law was heavily criticised during the Universal Periodic Review at the UN in November 2014.[10] Law 107 has been used to justify the arrest of many government opponents and civil rights activists. In December 2014, the President decreed that people receiving foreign funding for activities "deemed harmful to national interests" could face life sentences.[11] The decree was a major blow against Egyptian civil society and media organisations, many of which rely on foreign funds.[12]

Attacks on journalists

In 2013, three Al Jazeera journalists – Peter Greste, an Australian citizen, Mohamed Fadel Fahmy, a dual citizen of Egypt and Canada, and Baher Mohamed, an Egyptian citizen –were arrested and condemned to seven years in jail (ten years for Mohamed) on charges of conspiring with the Muslim Brotherhood to spread false news.[13]

8 "Abdel Fatah al-Sisi won 96.1% of vote in Egypt presidential election, say officials", The Guardian, 3 June 2014, http://www.theguardian.com/world/2014/jun/03/abdel-fatah-al-sisi-presidential-election-vote-egypt

9 "Egypt: Rab'a Killings Likely Crimes Against Humanity", Human Rights Watch, 12 August 2014, https://www.hrw.org/news/2014/08/12/egypt-raba-killings-likely-crimes-against-humanity

10 "Egypt - 20th Session of Universal Periodic Review", UN Web TV, 5 November 2014, http://webtv.un.org/meetings-events/human-rights-council/universal-periodic-review/20th-upr/watch/egypt-20th-session-of-universal-periodic-review/3876287212001

11 "Egypt's human rights group 'targeted' by crackdown on foreign funding", The Guardian, 24 September 2014, http://www.theguardian.com/world/2014/sep/24/egypt-human-rights-crackdown-foreign-funding

12 Ibid

13 "Egypt Deports Peter Greste, Journalist Jailed with 2 Al Jazeera Colleagues", The New York Times, 1 February 2015, http://www.nytimes.com/2015/02/02/world/africa/egypt-releases-and-deportsal-jazeera-journalist-from-australia.html

14 "2015 World Press Freedom Index – Egypt", Reporters Without Borders, 2015, https://index.rsf.org/#!/index-details/EGY

Thirty journalists were arrested in 2014.[14] That year, a journalist – Mayada Ashraf – was shot and killed during a protest. Ashraf's colleague who witnessed the attack stated that she was shot while running from gunfire that came from the direction of the police. The Police denied the accusation.[15]

In November 2015, the military detained Hossam Bahgat, the founder of the Egyptian Initiative for Personal Rights, an Egyptian human rights organisation, and a journalist from Mada Masr, in relation to articles he had written about the military. He was held for three days.[16]

The establishment and continued existence of a secretive intelligence unit such as the TRD is consistent with a wider pattern of political repression by unaccountable security services. It is not compatible, however, with a country that has supposedly undergone a democratic renewal.

REPORTERS WITHOUT BORDERS 2015 PRESS FREEDOM INDEX



15 "Mayada Ashraf", Committee to Protect Journalists, 2014, https://cpj.org/killed/2014/mayada-ashraf.php

16 "A statement by Hossam Bahgat on his military detention, interrogation.", Mada Masr, 10 November 2015, http://www.madamasr.com/sections/politics/statement-hossam-bahgat-his-military-detention-interrogation

An office within the General Intelligence Service

The TRD's headquarters are in the Kobry El Kobba district of Cairo, according to contract documents from surveillance technology companies Advanced German Technology and Hacking Team (see annex). Kobry El Kobba is also the district where the GIS have their headquarters. In a leaked email from surveillance company Hacking Team, an employee of Hacking Team states that the TRD's headquarters are located in the same building as the "secret services," without specifying which secret service.[17] This is consistent with information provided by an intelligence expert we have spoken to, that the TRD is a unit within the GIS. It is also worth noting that in the various documents that have been leaked over the past five years from surveillance companies, the GIS' name never appears. This could indicate that the TRD has been purchasing surveillance technologies on behalf of the GIS.

Hungry for more technologies

The TRD possesses wide-ranging surveillance capabilities, as indicated by the range of surveillance technologies the unit has purchased. This includes a communications monitoring centre, interception management system, and highly intrusive spyware.

It remains unclear if the TRD's budget is independent from the GIS and whether technologies purchased by the TRD are also used by the GIS. The TRD appears to benefit from a sizeable budget. Hacking Team expected to earn € 1 million from the sale of intrusive surveillance technologies to the unit, according to Hacking Team's leaked client overview, an administrative document listing how much each of their customers would pay every year.

> "The purpose of our visit was to meet the Technical Research Department (TRD) of the intelligence for a POC [proof of concept]. We met them for a day and a half, everything went smoothly […]. On the second day, the head of the department showed up for a couple of hours. They all were very happy and decided to purchase RCS (we are talking about more than 1M Euro)."[18]
>
> Email from m******a@hackingteam.it to rs****s@hackingteam.it, on June, 21st 2013

17 Hacking Team employees do not appear to have actually visited the TRD offices, as they were meeting in their intermediary's offices, and had limited contact with TRD officials. Wikileaks Hacking Team emails ID 14661 https://wikileaks.org/hackingteam/emails/emailid/14661

18 Wikileaks Hacking Team emails ID 602607 https://wikileaks.org/hackingteam/emails/emailid/602607

The TRD is always on the lookout for new capabilities, according to an industry source familiar with the unit, who stated "if you start a business selling the sort of technologies they are interested in, you don't need to approach them. They will investigate you and eventually approach you."

Presidential budget

Like the GIS, the budget of the TRD is independent from the Ministry of Defence and the Ministry of Interior, which have their own intelligence units. In emails discussing potential business with the TRD, Hacking Team employees made it clear that the TRD is accountable only to the President, who directly allocates its budget.[19] Though the unit's budget is not publicly known, according to one source it has the largest budget of the intelligence agencies in terms of "security solutions. "

A very secret secret service

While the GIS and the Egyptian Military Intelligence and Reconnaissance Administration are both well known to the public and their respective directors are public figures, the TRD is only hinted at in public documentation. This may be due to its obscure mission, which seems to be to serve as the president's personal intelligence agency, according to an intelligence source familiar with the TRD. Its purpose is reported to be in part to spy on other government officials and potential opponents. The TRD does not appear to have been established by decree or other legal measure.

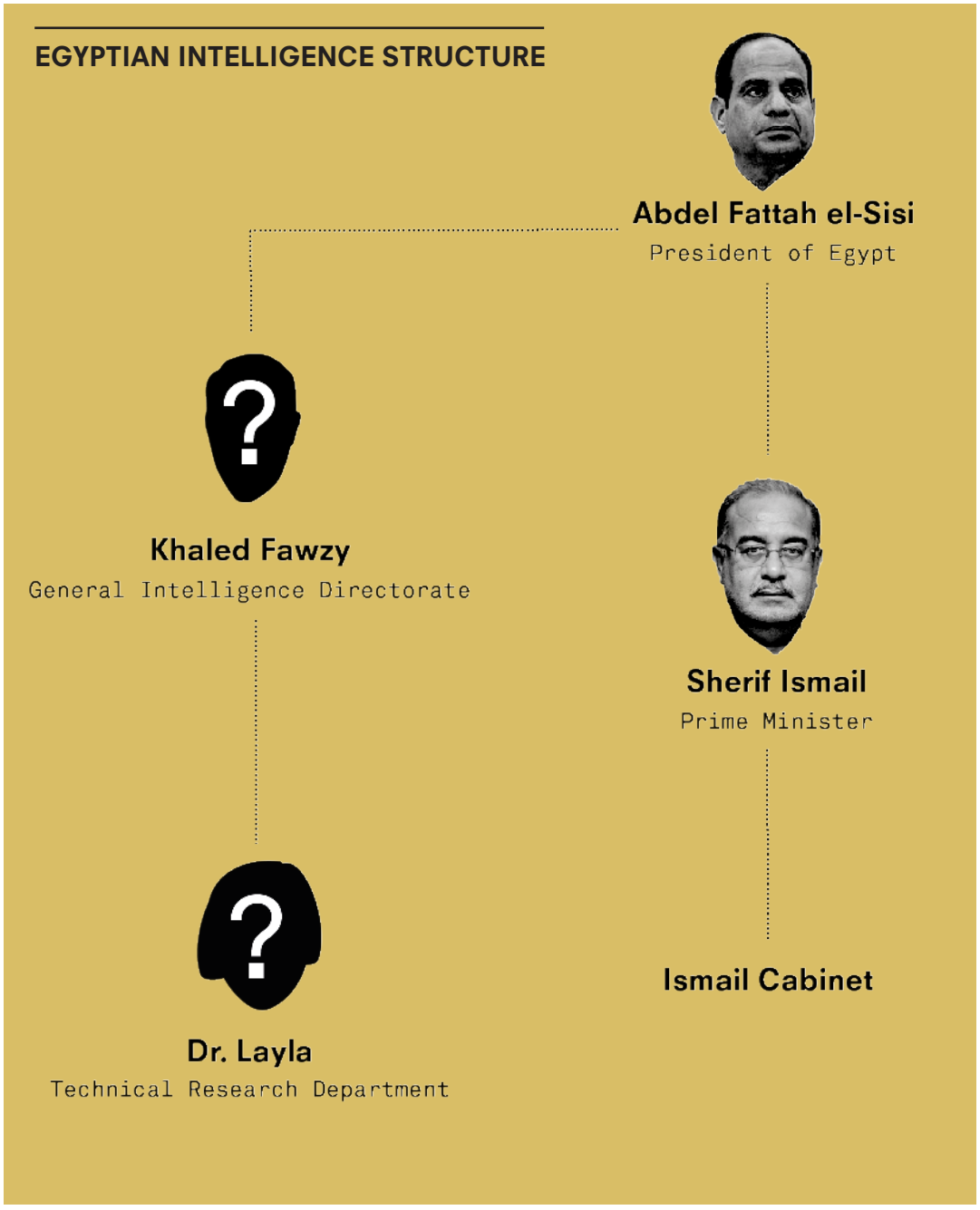
However, the TRD is real. The TRD is a customer of Systems Engineering of Egypt (SEE Egypt), a company that sells products on behalf of surveillance technology manufacturers such as Blue Coat (which develops Deep Packet Inspection technology) and Axis (which makes CCTV equipment and software).[20]

Who runs the TRD?

The TRD appears to recruit individuals with doctorates in Electronics and Engineering or Computer Science, according to former employees' profiles. One Hacking Team employee who claims to have met the head of the TRD refers to her as General Layla.[21] This is striking as Egypt has a largely male-dominated army. In other documents she is addressed as Dr. Layla, which implies she holds a doctorate. Yet in one of the bills sent to the TRD, the TRD director is addressed as "Dear Sir" (see annex). Individuals familiar with Egypt's intelligence infrastructure suggest it is not entirely surprising that a woman would be the head of the TRD. The TRD appears to largely recruit academics; a woman with expertise in engineering, for instance, would not be out of place there. If part of the TRD Director's job involves managing

19 Wikileaks Hacking Team emails ID 14661 https://wikileaks.org/hackingteam/emails/emailid/14661
20 SEE customers http://www.seegypt.com/selected%20customers.asp
21 Wikileaks Hacking Team emails ID 14661 https://wikileaks.org/hackingteam/emails/emailid/14661

military officers, she may have been granted a honorary title as "General," a common process for civilians who find themselves leading members of the military, according to a source familiar with Egyptian institutions.



The TRD's mass surveillance capabilities

Nokia Siemens Networks: providing the TRD with ears and eyes

Nokia Siemens Networks (NSN) was a Helsinki-based joint venture of German conglomerate Siemens AG and Finnish telecommunications company Nokia. Following controversy in 2009, when it was revealed that NSN had sold monitoring centre equipment in Iran,[22] NSN sold its subsection, 'Siemens Intelligence Solutions' to Perusa Partners Fund 1 LP, a private investment firm based in Munich. The new company was named Trovicor.[23]

However, NSN and Trovicor then worked together anyway. Documents obtained by Privacy International revealed that NSN was still selling monitoring centres to Pakistan after 2009, and referred to Trovicor as an "NSN vendor" and a "3rd party who will be delivering the onshore services on behalf of NSN".[24]

Previously undisclosed documents about NSN's business in Egypt, obtained by Privacy International, reveal that by 2011 NSN had sold an x25 network to the TRD - a legacy technology allowing dial-up internet access. It would enable access to the internet even if the main internet infrastructure is shut down in the country, as happened in Egypt during the revolution.

NSN also sold to the TRD – in 2011 or before – an interception management system and a monitoring centre for fixed and mobile networks. These two technologies offer mass surveillance capabilities, enabling the Egyptian government to intercept phone communications of any line routed through the interception management system.

The documents further reveal that Universal Advanced Systems (UAS), a company that presents itself as "a leading Egyptian solution provider for […] lawful interception systems"[25] mediated the sale of these products. UAS claims to be an "exclusive agent of more than 10 international companies (European and American)." Neither NSN nor Trovicor are officially listed as

22 "Iran's Web Spying Aided By Western Technology", The Wall Street Journal, 22 June 2009, http://online.wsj.com/ news/articles/SB124562668777335653?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB124562668777335653.html

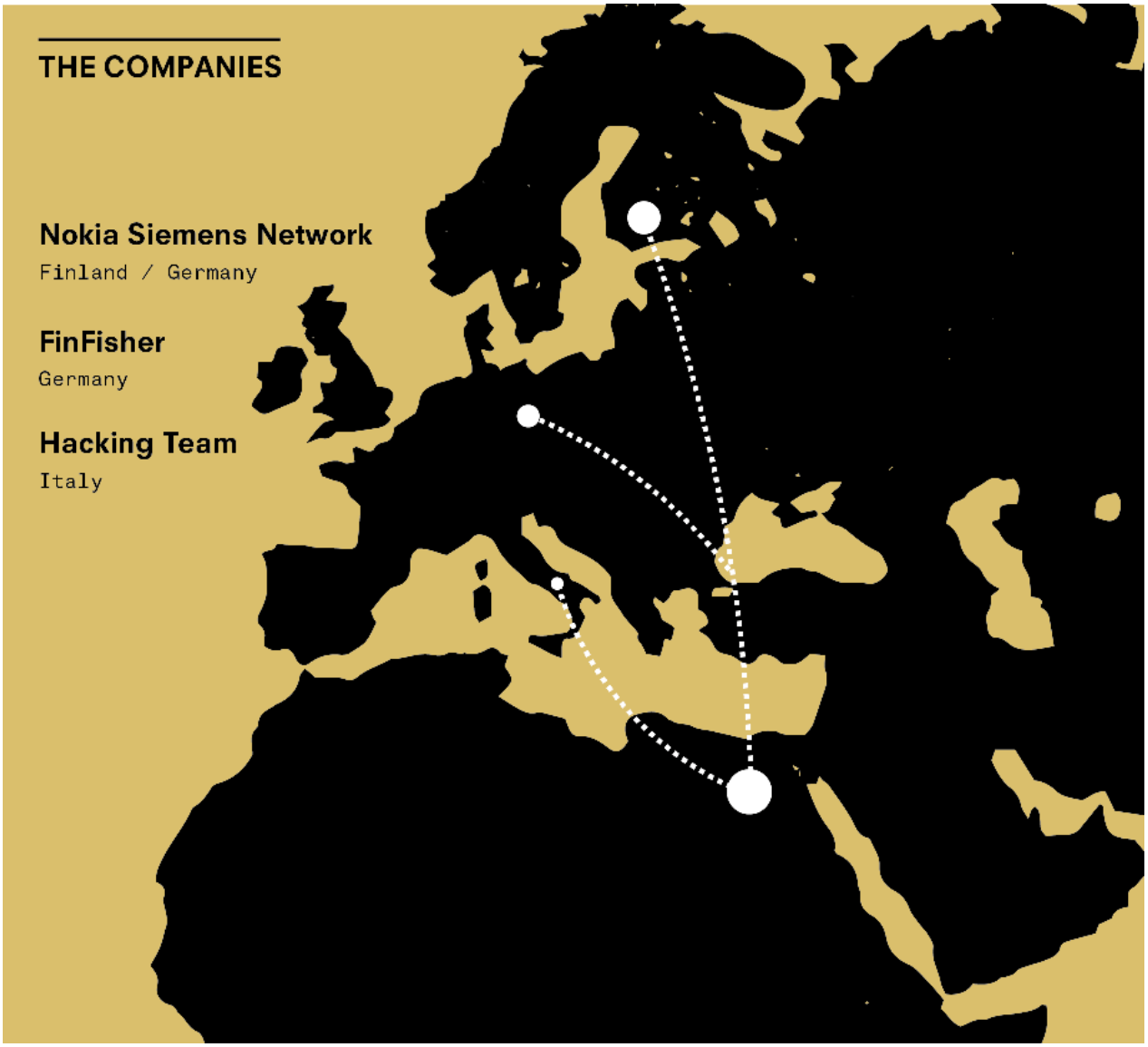
23 "Trovicor", Perusa, 24 April 2009, http://www.perusa-partners.de/deutsch/beteiligungen/liste/trovicor.php and

24 "Provision of Lawful Intercept capability in Iran", Nokia, 22 June 2009, http://networks.nokia.com/news-events/press-room/press-releases/provision-of-lawful-intercept-capability-in-iran
"Tipping the scales: Security and surveillance in Pakistan", Privacy International 21 July 2015, https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf

25 About UAS http://www.uas-eg.com/about.html

their partners.

Another company involved in the transaction of the x25 network was Egyptian German Telecommunications Industries (EGTI). The company is partly owned by Siemens and is described as "a joint venture between the Egyptian government and Siemens AG Germany."[26] On a national scale, EGTI was also in charge of installing an EWSD exchange, a telephone exchange system for landlines and mobile phones in Egypt.[27]



26 EGTI The High Technology Company, Internet Archive, 4 December 2000, https://web.archive.org/web/20001204204500 http://egti.com/profile.htm

27 Ibid

Lawful Interception

Network interception technologies are tools that require physical installation onto a network to perform communications surveillance. Network interception technologies contrast with tactical technologies, which are mobile surveillance tools that do not require physical installation onto a network, but rather receive data wirelessly or from devices directly. The deployment of a network interception platform typically involves three types of commercial actors that provide different types of products and services:

- The first type of commercial actor is the **manufacturer** of the equipment that forms the basis of a network; in this case, NSN. The equipment such companies supply includes switches and exchanges used to connect traffic between lines, as well as other hardware and services which ensure telecommunications infrastructure, as a whole, is able to support different networks and services.

- The second type of commercial actor is the **telecommunications service provider (TSP)** which manages a network and charges subscribers for services. TSPs are responsible for ensuring that their activities comply with the national legislation of the country where they operate. This usually includes statutory requirements that the TSP facilitate access by law enforcement and security agencies to their networks and to their subscribers' data.

- The third type of commercial actor is the **surveillance technology company** – such as UAS – that directly markets and sells products and services for intelligence and law enforcement purposes. These companies provide 'solutions' designed to enable state agencies to intercept, analyse or disseminate data from networks. Surveillance companies sell these solutions either directly to governments or to TSPs.

There are legal obligations in many countries that TSPs make their networks interception compliant. Some TSPs therefore contract surveillance companies at their own expense, and incorporate electronic surveillance solutions within their networks. Governments across the world require that telecommunications providers make their networks compatible by applying and enforcing "Lawful Interception" standards. The standards of the Communications Assistance for Law Enforcement Act (CALEA) in the US and the European Telecommunications Standards Institute (ETSI) in Europe are two examples of frameworks designed to ensure that all telecommunications network equipment manufacturers and TSPs design telecommunication infrastructure to be accessible by states.

In Egypt, article 64 of the 2003 Telecommunication Regulation Law states that:

"With due consideration to inviolability of citizens private life as protected by law, each Operator and Provider shall, at his own expense, provide within the telecommunication networks licensed to him all technical potentials

including equipment, systems, software and communication which enable the Armed Forces, and National Security Entities to exercise their powers within the law."

The law does not define which "National Security Entities" are entitled to conduct the interceptions, so interception from the TRD is actually likely to be lawful within such a vague legal definition.[28]

The TRD's purchase of mass surveillance technologies such as a monitoring centre and an interception management system is greatly concerning. The sale of these technologies by Trovicor to Bahrain and Iran triggered international outrage. Bahraini government authorities used such technologies to arrest opponents who were then tortured, while being read transcripts of their text messages and phone conversations.[29] In Iran, monitoring centres from NSN were allegedly used during the 2009 protests unrest to crack down on activists.[30]

Considering Egypt's human rights record, it is very concerning that a secret unit such as the TRD, which appears to have no form of oversight or clear legal mandate, has surveillance capabilities that enable it to monitor the phone and internet communications of anyone in Egypt. Egypt already has a tradition of using surveillance as a means of intimidation. After the 2011 protests, a TV programme broadcast phone conversations of well-known activists to shame them in the eyes of the general public.[31] An Egyptian activist said transcripts of her emails and online chats with her partner were slipped under her door. The National Security Service summoned her for questioning shortly thereafter.[32]

AGT: another German contract for the TRD

The TRD also purchased technology from the German company Advanced German Technology (AGT) in 2006, according to another document obtained by Privacy International, contained as an annex. The reseller for AGT in Egypt at the time was SEE Egypt.[33] AGT specialises in lawful interception and prides itself in selling technologies to various public sector bodies, including intelligence agencies. It is unclear what technologies were purchased and whether or not they were surveillance technologies. The technologies are referred to as SGS-1100 and SG-1100 and cost US$21,188 and US$18,688, respectively. In total the TRD spent over US$50,000 including the "Basic Support" it purchased from AGT.

28 Article 64, Telecommunication Regulation Law – Law No 10 of 2003 http://www.tra.gov.eg/uploads/law/law_en.pdf

29 "Torture in Bahrain Becomes Routine With Help From Nokia Siemens", Bloomberg, 22 August 2011, http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking

30 "Iran's Web Spying Aided By Western Technologies", Wall Street Journal, 22 June 2009, http://www.wsj.com/articles/SB124562668777335653#mod=rss_whats_news_us

31 "Egyptians fear return of surveillance state", Al Monitor, 15 January 2014, http://www.al-monitor.com/pulse/originals/2014/01/egypt-eavesdropping-scandal-fear-return-police-state.html#

32 "Sexual assault and the state: A history of violence", Mada Masr, 7 July 2014, http://www.madamasr.com/sections/politics/sexual-assault-and-state-history-violence

33 http://www.seegypt.com/

Hacking Team and FinFisher: the TRD's targeted tools

Hacking Team's obscure client

In July 2015, the Italian company Hacking Team was itself hacked: more than one million emails and many administrative documents stored on its servers were leaked to the public. The company had been repeatedly exposed for selling its highly intrusive spyware to oppressive regimes. Its Remote Control System (RCS) malware grants the attacker complete control of the computer of their target. The attacker can then, for example, access any content stored on the computer, monitor its use in real time, log keystrokes and passwords, capture screenshots and activate the computer's webcam.

RCS has been deployed to spy on journalists and activists. In 2014, researchers at Citizen Lab, part of the University of Toronto, exposed the use of RCS against a group of Ethiopian journalists.[34] Journalists and activists in Morocco and the UAE had previously been targeted with serious impacts on their work and mental well-being.[35]

The TRD was one of Hacking Team's major customers, willing to pay €1 million for the license and customer service.[36]

The TRD have two contracts: the first was initially with an intermediary known as A6 Consultancy[37] and then with Solve IT.[38][39] The second contract was with the GNSE Group, a company of the conglomerate Mansour Group, which belongs to the second richest family in Egypt. GNSE presents itself as a company offering service to "secure information, applications and networks."[40]

The contract with A6 had apparently still not been formally concluded as of June 2015. In the 2015 client overview, A6 is still listed under prospective customers and expected to pay €750,000 for the year.

34 "Hacking Team and the Targeting of Ethiopian Journalists", Citizen Lab, 12 February 2014, https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/

35 Privacy International's report Their Eyes on Me, highlights the experiences of individuals targeted using RCS in Morocco https://privacyinternational.org/?q=node/554

36 Wikileaks Hacking Team emails ID 602607 https://wikileaks.org/hackingteam/emails/emailid/602607

37 http://a6-consultancy.com/

38 http://solve-it-solutions.com/. Wikileaks Hacking Team emails ID 14890 https://wikileaks.org/hackingteam/emails/emailid/14890

39 It appears very likely that A6 and Solve IT are actually the same company whose name was changed. Both companies have now taken down their websites. About GNSE

40 http://www.gnsegroup.com/Profile/aboutGNS.aspx

An email from March 2015[41] reveals the kind of capacities the TRD was trying to obtain:

"The TRD will lead the negotiations with HT, TRD is requesting an offer for 3 THREE different systems, each equipped with 200 Licenses (and same actual configuration). TRD would like to have a bulk discount for purchasing 3 systems at once, to have per system: same configuration as discussed recently (including software with 200 licenses + Hardware + Services + Training on site and in HT premises). 2 years warranty including SW updates for a final price of 800K Euro per system (3 x 800,000 = 2,400,000 Euro). The deal can be closed either in one contract or in three different contracts simultaneously. If the above conditions are accepted by HT, the deal can be closed within one month time."

The contract with GNSE had already concluded by the time the emails were leaked. The client overview showed that Hacking Team was owed € 412,000 in 2015 and that €15,000 had already been paid.

For that sum, as the leaked client list shows, the TRD could target 25 individual devices, an average amount when compared to other countries such as Thailand, Mexico and Uzbekistan.

The TRD had specific requests for Hacking Team. The TRD wanted to target Apple 's iPhones and Mac computers, according to emails exchanged with GNSE. But the TRD was also planning to target Windows users — they explained to Hacking Team that of the Windows users they would be targeting, 90% would be using illegal copies of the operating system.[42] They therefore wanted Hacking Team to design malware not only capable of targeting Apple products but also illegally-obtained versions of Microsoft Windows.

FinFisher: teasing targets with "confidential" bait

The TRD also used FinFisher, another intrusion malware suite similar to Hacking Team's product, according to research published by Citizen Lab in October 2015.[43]

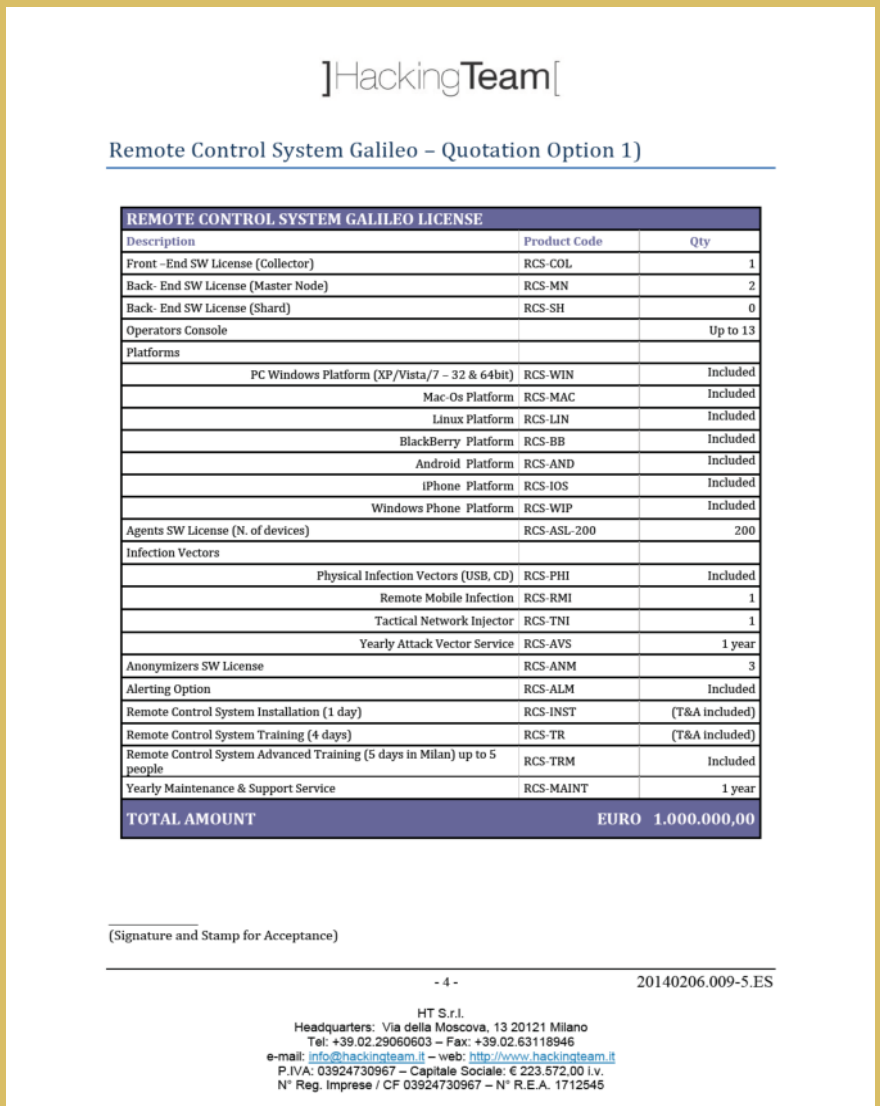
Citizen Lab was able to identify about twenty domain names affiliated to the TRD. The IP addresses used for a FinFisher server were also used by a Hacking Team employee the day he was scheduled to deliver the installation to the TRD. On one of the web pages, the researchers found a FinFly Web sample - the web page was created to infect targets with the FinFisher malware.[44] The researchers had also identified an IP address behind a FinFisher server and were able to link that IP address to the TRD.[45]

41 Wikileaks Hacking Team emails ID 554233 accessed on 03/08/2015
42 Wikileaks Hacking Team emails ID 602607 https://wikileaks.org/hackingteam/emails/emailid/602607 accessed on 03/08/2015
43 "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation", Citizen Lab, 15 October 2015, https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/
44 Ibid
45 Ibid

According to Citizen Lab, MOLERATS, a cyber criminal group that have targeted "political Islam" groups and Israel, was using spyware that appeared to be linked to the TRD. This suggests a connection between the intelligence service and the group. The malware file MOLERATS used as a bait to attract its targets promised pictures of a Jordanian air force pilot who had been burned alive.[46]

In yet another case observed by Citizen Lab, FinFisher was hidden behind a document entitled "A Highly Classified Report." Again, the malware was communicating with the IP address identified as being the TRD's.[47]

HACKING TEAM QUOTATION 1



]HackingTeam[

Remote Control System Galileo – Quotation Option 1)

REMOTE CONTROL SYSTEM GALILEO LICENSE		
Description	Product Code	Qty
Front –End SW License (Collector)	RCS-COL	1
Back- End SW License (Master Node)	RCS-MN	2
Back- End SW License (Shard)	RCS-SH	0
Operators Console		Up to 13
Platforms		
PC Windows Platform (XP/Vista/7 – 32 & 64bit)	RCS-WIN	Included
Mac-Os Platform	RCS-MAC	Included
Linux Platform	RCS-LIN	Included
BlackBerry Platform	RCS-BB	Included
Android Platform	RCS-AND	Included
iPhone Platform	RCS-IOS	Included
Windows Phone Platform	RCS-WIP	Included
Agents SW License (N. of devices)	RCS-ASL-200	200
Infection Vectors		
Physical Infection Vectors (USB, CD)	RCS-PHI	Included
Remote Mobile Infection	RCS-RMI	1
Tactical Network Injector	RCS-TNI	1
Yearly Attack Vector Service	RCS-AVS	1 year
Anonymizers SW License	RCS-ANM	3
Alerting Option	RCS-ALM	Included
Remote Control System Installation (1 day)	RCS-INST	(T&A included)
Remote Control System Training (4 days)	RCS-TR	(T&A included)
Remote Control System Advanced Training (5 days in Milan) up to 5 people	RCS-TRM	Included
Yearly Maintenance & Support Service	RCS-MAINT	1 year
TOTAL AMOUNT		EURO 1.000.000,00

(Signature and Stamp for Acceptance)

- 4 - 20140206.009-5.ES

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Quotation for Remote Control System (RCS). RCS is malware that would allow the Technical Research Department to obtain full access to their targets' computers and smartphones.

46 Ibid
47 Ibid

Writing the next chapter

This report has sought to expose the existence of the TRD, a highly secretive unit likely situated within the GIS. The TRD is accountable only to the President and its likely function includes gathering intelligence on individuals in other government branches. We have exposed some of the surveillance technologies the unit has purchased: on the one hand, equipment for mass interception of communications; and on the other, malware for targeted spying. While we do not claim that the TRD itself is conducting mass surveillance, it currently has at least part of the necessary equipment to do so without any oversight mechanism in place or prior parliamentary debate.

Many questions about the TRD remain unanswered. When exactly was it created? Why was it created? What is its mandate? To what extent does it collaborate with the country's main intelligence agencies? Were the technologies purchased by the TRD used by the GIS? What is its architecture? Who really heads the TRD? Who regulates it?

Transparency in intelligence is necessary for a democratic society. The fact that a secret unit – unknown to the general public and apparently without any democratic oversight – can afford to spend millions of euros surveilling potentially every Egyptian citizen's communications is a grave human rights issue that the Egyptian government must address. We hope that this report will serve as a catalyst for further research and investigation.

In July 2014, the European Parliament had called for a ban on exporting monitoring technology to Egypt. This represents a first step in the right direction.

Privacy International asks that the Egyptian government explicitly avow the existence and the role of the TRD. Its operations must be explained to the public and subject to oversight. A process of judicial authorisation of surveillance requests must be put in place for surveillance conducted by the TRD and the unit must comply with international law. Egypt is a signatory of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which both explicitly protect the right to privacy.

Privacy International urges Egypt to be far more transparent about its surveillance infrastructure and ensure it fully complies with international law.

ANNEX 1: AGT Purchase Order

Systems Engineering of Egypt
ش.م.م

45, Hassan Afatoun St., Golf Ground
Cairo, Egypt
Tel +20 2 2921100/2689455(56/57/58)
Fax +20 2 2901673/2689459)

Purchase Order

To	: Advanced German Technology	From	: Mohamed Farag
Attn	: Mr. Aghiath	e-mail	: mfarag@seegypt.com
Fax	: +971 4 390 47 57	P.O#	: AGT/131/2006
Tel.	: +971 4 390 20 39	Pages	: 1
		Date	: 27/11/2006

We would like to place an order with the following items:
Your Prompt Response Is Highly Appreciated.

Item	P/N	Description	Qty	Unit Price	Discount	Ex. Price
1	APP-SGS-1100	SGS-1100 - 8 x 10/100/1000 FE This with Management license for one cluster.	1	$ 21,188.00	12%	$ 18,645.44
2	APP-SG-1100	SG-1100 - 8 x 10/100/1000 FE- Max.	1	$ 18,688.00	12%	$ 16,445.44
3	(R)M3-APP-SGS-1100	Basic Support 8/5- 3-year- 8/5Renewal - add R	1	$ 9,534.00	12%	$ 8,389.92
4	(R)M3-APP-SG-1100	Basic Support 8/5- 3-year- 8/5Renewal - add R	1	$ 8,408.00	12%	$ 7,399.04
		Basic Support: 8/5-call logging via Web and phone, next business day response time, software updates, hardware replacement service.				
		Total Price in US Dollar				$ 50,879.84

Payment Conditions : Technical Research Department.
Kobri El Koba, Cairo,
Egypt.
Consignee Name Mr. Sherif Fayez.
Contract No. (MX/22/2006-2007).
Prices : In US Dollar
Requested Ship Date : 4 to 6 weeks.
Payment : wire transfer (Advanced Payment).
Shipping Information : The shipping Doc's should be handed by the shipper agent , do not attached with the shipment or inside the Box's
Certificate of origin :Certificate of origin is required and must be stamped from the Egyptian Embassy
Invoice : The total amount invoice is required and must be stamped from the Chamber Of Commerce and Industry & from the Egyptian Embassy

Logistic Manager [redacted]

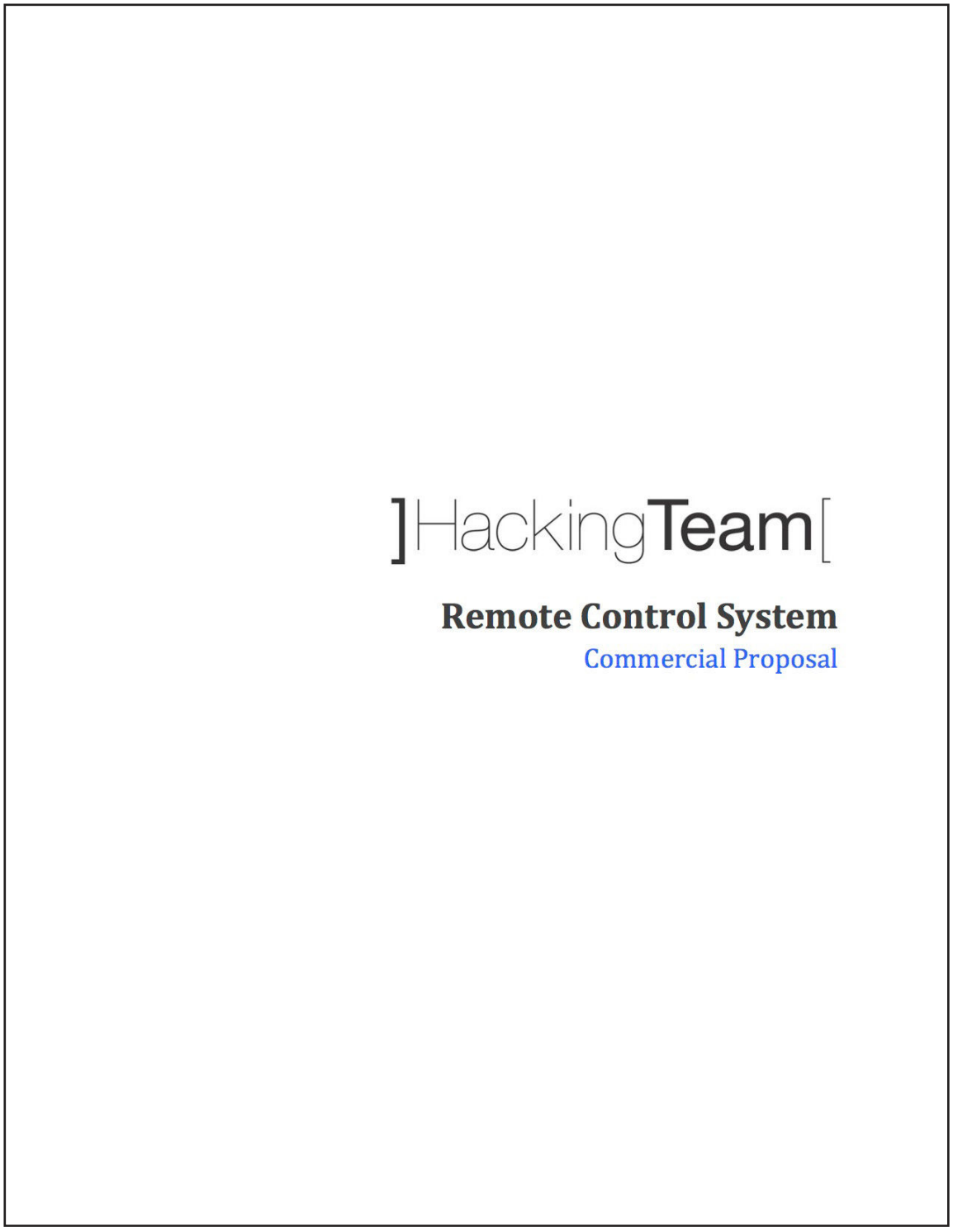
Logistic Ass. Manager [redacted]

Thank you & Best Regards

Logistic Coordinator [redacted]

Page 1 of 1

ANNEX 2: Hacking Team's commercial proposal to the TRD



ANNEX 2: Hacking Team's commercial proposal to the TRD

]HackingTeam[

January 05, 2015

Technical Research Department - TRD
Kobry El Kobba
Cairo - Egypt

Att. Dr. Layla

Offer N. 20140206.009-5.ES

Subject: Proposal for Remote Control System

Dear Sir,

As for your kind request, please find the proposal regarding the Remote Control System – Galileo.

It is however understood that this proposal and the agreement subsequent to your acceptance shall be automatically terminated pursuant to Sections 1353 and ff. of Italian Civil Code should any necessary license or authorization required for the export of the product - under Italian laws, the EU legislation and/or any other applicable laws - be not granted to HT within a period of 120 days from the date of your acceptance. It is also understood that HT shall give notice of the occurrence or the non-occurrence of the Condition in a timely manner, being further agreed that the above condition subsequent can be waived by HT also after its occurrence.

Don't hesitate to contact me for any further information.

Best Regards

[redacted]
Key Account Manager
HT S.r.l.

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ANNEX 2: Hacking Team's commercial proposal to the TRD

]HackingTeam[

Remote Control System Description

Please refer to the following document for technical description:

- HT_Galileo_SolutionDescription_2.3

Remote Control System Technical Requirements

Please refer to the following document for technical requirements:

- HT_Galileo_TechnicalRequirements_v2.3.pdf

Professional Services: Installation and Training

1. Installation

The solution will be installed at Customer Site by HT field application engineers.
Duration of the activities is actually planned for one (1) working day and it will be under Customer responsibility to prepare the Operation Environment as indicated in the Technical Requirements document.

2. Training

Following the installation, we will provide four (4) days of training focused on the usage of Remote Control System Galileo.
This training will be performed at Client Site.
Please refer to the following document for product training:

- HT_Galileo_Product Training_v1.2

3. Maintenance & Support

Maintenance for one (1) year is included.
Please refer to the following document for Maintenance and Support:

- HT_Galileo_SolutionDescription_2.3

4. On Site Support

On-site support will be delivered, if requested, by senior Hacking Team Field Application Engineer and will include assistance to the end user in the daily activity.

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ANNEX 2: Hacking Team's commercial proposal to the TRD

]HackingTeam[

Remote Control System Galileo – Quotation Option 1)

REMOTE CONTROL SYSTEM GALILEO LICENSE		
Description	Product Code	Qty
Front –End SW License (Collector)	RCS-COL	1
Back- End SW License (Master Node)	RCS-MN	2
Back- End SW License (Shard)	RCS-SH	0
Operators Console		Up to 13
Platforms		
PC Windows Platform (XP/Vista/7 – 32 & 64bit)	RCS-WIN	Included
Mac-Os Platform	RCS-MAC	Included
Linux Platform	RCS-LIN	Included
BlackBerry Platform	RCS-BB	Included
Android Platform	RCS-AND	Included
iPhone Platform	RCS-IOS	Included
Windows Phone Platform	RCS-WIP	Included
Agents SW License (N. of devices)	RCS-ASL-200	200
Infection Vectors		
Physical Infection Vectors (USB, CD)	RCS-PHI	Included
Remote Mobile Infection	RCS-RMI	1
Tactical Network Injector	RCS-TNI	1
Yearly Attack Vector Service	RCS-AVS	1 year
Anonymizers SW License	RCS-ANM	3
Alerting Option	RCS-ALM	Included
Remote Control System Installation (1 day)	RCS-INST	(T&A included)
Remote Control System Training (4 days)	RCS-TR	(T&A included)
Remote Control System Advanced Training (5 days in Milan) up to 5 people	RCS-TRM	Included
Yearly Maintenance & Support Service	RCS-MAINT	1 year
TOTAL AMOUNT		**EURO 1.000.000,00**

(Signature and Stamp for Acceptance)

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ANNEX 2: Hacking Team's commercial proposal to the TRD

]HackingTeam[

REMOTE CONTROL SYSTEM YEARLY SERVICES		
Description	Product Code	Price
Yearly Attack Vector Service Fee	RCS-EXP	Euro 70.000,00
Yearly Maintenance & Support Service Fee	RCS-MAINT	Euro 132.500,00

REMOTE CONTROL SYSTEM OPTIONAL FEATURES		
Description	Product Code	Price
Intelligence Module	RCS-INT	Euro 175.000,00

REMOTE CONTROL SYSTEM OPTIONAL SERVICES		
Description	Product Code	Price
IT- Training (ITTraining_0.4) price per each course up to 5 people	RCS-TRA	Euro 30.000,00
ON-SITE Support Service (8 weeks)	RCS-ONS	Euro 150.000,00

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ANNEX 2: Hacking Team's commercial proposal to the TRD

]HackingTeam[

Remote Control System Galileo – Quotation Option 2)

REMOTE CONTROL SYSTEM GALILEO LICENSE		
Description	Product Code	Qty
Front –End SW License (Collector)	RCS-COL	1
Back- End SW License (Master Node)	RCS-MN	2
Back- End SW License (Shard)	RCS-SH	0
Operators Console		Up to 5
Platforms		
PC Windows Platform (XP/Vista/7 – 32 & 64bit)	RCS-WIN	Included
BlackBerry Platform	RCS-BB	Included
Android Platform	RCS-AND	Included
Agents SW License (N. of devices)	RCS-ASL-50	50
Infection Vectors		
Physical Infection Vectors (USB, CD)	RCS-PHI	Included
Remote Mobile Infection	RCS-RMI	1
Tactical Network Injector	RCS-TNI	1
Yearly Attack Vector Service	RCS-AVS	1 year
Anonymizers SW License	RCS-ANM	3
Alerting Option	RCS-ALM	Included
Remote Control System Installation (1 day)	RCS-INST	(T&A included)
Remote Control System Training (4 days)	RCS-TR	(T&A included)
Remote Control System Advanced Training (5 days in Milan) up to 5 people	RCS-TRM	Included
Yearly Maintenance & Support Service	RCS-MAINT	1 year
TOTAL AMOUNT		**EURO 645.000,00**

_____
(Signature and Stamp for Acceptance)

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ANNEX 2: Hacking Team's commercial proposal to the TRD

]HackingTeam[

REMOTE CONTROL SYSTEM YEARLY SERVICES		
Description	**Product Code**	**Price**
Yearly Attack Vector Service Fee	RCS-EXP	Euro 70.000,00
Yearly Maintenance & Support Service Fee	RCS-MAINT	Euro 105.000,00

REMOTE CONTROL SYSTEM OPTIONAL FEATURES		
Description	**Product Code**	**Price**
Intelligence Module	RCS-INT	Euro 60.000,00

REMOTE CONTROL SYSTEM OPTIONAL SERVICES		
Description	**Product Code**	**Price**
IT- Training (ITTraining_0.4) price per each course up to 5 people	RCS-TRA	Euro 30.000,00
ON-SITE Support Service (8 weeks)	RCS-ONS	Euro 150.000,00

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ANNEX 2: Hacking Team's commercial proposal to the TRD

]HackingTeam[

Remote Control System Galileo – Quotation Option 3)

REMOTE CONTROL SYSTEM GALILEO LICENSE		
Description	Product Code	Qty
Front –End SW License (Collector)	RCS-COL	1
Back- End SW License (Master Node)	RCS-MN	2
Back- End SW License (Shard)	RCS-SH	0
Operators Console		Up to 13
Platforms		
Android Platform	RCS-AND	Included
Agents SW License (N. of devices)	RCS-ASL-50	50
Infection Vectors		
Physical Infection Vectors (USB, CD)	RCS-PHI	Included
Remote Mobile Infection	RCS-RMI	1
Tactical Network Injector	RCS-TNI	1
Yearly Attack Vector Service	RCS-AVS	1 year
Anonymizers SW License	RCS-ANM	3
Alerting Option	RCS-ALM	Included
Remote Control System Installation (1 day)	RCS-INST	(T&A included)
Remote Control System Training (4 days)	RCS-TR	(T&A included)
Remote Control System Advanced Training (5 days in Milan) up to 5 people	RCS-TRM	Included
Yearly Maintenance & Support Service	RCS-MAINT	1 year
TOTAL AMOUNT		**EURO 595.000,00**

_____
(Signature and Stamp for Acceptance)

REMOTE CONTROL SYSTEM YEARLY SERVICES

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ANNEX 2: Hacking Team's commercial proposal to the TRD

]HackingTeam[

Description	Product Code	Price
Yearly Attack Vector Service Fee	RCS-EXP	Euro 70.000,00
Yearly Maintenance & Support Service Fee	RCS-MAINT	Euro 95.000,00

REMOTE CONTROL SYSTEM OPTIONAL FEATURES		
Description	**Product Code**	**Price**
Intelligence Module	RCS-INT	Euro 60.000,00

REMOTE CONTROL SYSTEM OPTIONAL SERVICES		
Description	**Product Code**	**Price**
IT- Training (ITTraining_0.4) price per each course up to 5 people	RCS-TRA	Euro 30.000,00
ON-SITE Support Service (8 weeks)	RCS-ONS	Euro 150.000,00

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ANNEX 2: Hacking Team's commercial proposal to the TRD

]HackingTeam[

Note:

- Every Concurrent Agent license can be used for an unlimited amount of times. Once the investigation is over and the backdoor is uninstalled, it can be used to infect another target.
- The total number of device and platforms can be used in any combination.
- Each agent license will work on any type of operating system that has been bought.
- Hardware Equipment is not included.
- The yearly maintenance fee price is calculated on the purchased configuration, if the configuration changes the maintenance price will be recalculated.
- Remote Attack Vectors Service is a yearly subscription to be purchased every year.
- In refer to the Advanced Training: all travel and accommodations cost are not included
- Prices for additional year of subscription for Maintenance & Support Service and Remote Attack Vectors Service additional are valid for purchase orders received within 2015.

_____
(Signature and Stamp for Acceptance)

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ANNEX 2: Hacking Team's commercial proposal to the TRD

]HackingTeam[

Terms& Conditions

a. Warranty

The warranty period for HT software products is one year starting from date of delivery.

b. Financials

1. Pricing doesn't include VAT and local taxes.
2. Prices are reserved to Technical Research Department - TRD
3. Technical Research Department – TRD accepts to purchase the solution as above reported for a price of Euro
4. The End User Technical Research Department – TRD as to sign the attached "HT_EULAD" and the End User Statement.
5. Software Delivery and Product Training within 45 days upon the Purchase Order is received (to be agreed).
6. Terms of Payment
   - 50% Down Payment at PO date
   - 50% at Delivery Certificate signature date (please refer to the attached document)
7. Validity: The quotation is valid until 30 March 2015

c. List of Attachments:

- HT_Galileo_SolutionDescription_2.3.pdf
- HT_Galileo_Technical Requirements_v2.3.pdf
- HT_Galileo_Product Training_v1.2.pdf
- HT_Galileo_Delivery Certificate_v1.2.pdf
- EULAD
- E.U. Statement_1.0

_____
(Signature and stamp for Acceptance)

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ANNEX 3: Response from Nokia

NOKIA

February 22, 2016

Privacy International Report

Nokia is committed to the Universal Declaration of Human Rights and the human rights principles of the United Nations' Global Compact and has embedded them in our Code of Conduct and in our Human Rights Policy. We take steps to ensure that the technology we provide – legally and in good faith – will be used properly and lawfully.

Regarding the case of Egyptian German Telecommunications Industries (EGTI), it was a joint venture of the former Siemens Networks and the Egyptian government, and it transferred to Nokia Siemens Networks with the formation of the joint venture in 2007. Today, Nokia operates in Egypt under Nokia Solutions and Networks S.A.E., a joint venture serving Egyptian telecommunications operators.

As for Universal Advanced Systems, our investigations revealed a commercial arrangement we inherited from Siemens in 2007. We have not pursued new business with Universal Advanced Systems since then.

Regarding Lawful Interception (LI) technology, as a telecommunications equipment vendor we provide LI technology to our operator customers. This capability is a prerequisite for telecommunications operators to obtain a license, and is required by law in virtually all countries globally.

As for monitoring centers, Nokia divested this business in 2009, and we not do we believe that we had any such sales since then. When we sold the business, most customer records were transferred to the new owner and we do not have extensive visibility to possible pre-2009 sales.

Nokia has worked to implement the UN Guiding Principles for Business and Human Rights since they were first launched in 2011. In connection with this work, we were the first telecommunications vendor to define and to implement a human rights due diligence process to minimize and to mitigate the possible risk of misuse of Nokia technology in human rights violations.

As one of the founding members of the Telecommunications Industry Group, we remain committed to constructive dialogue with governments and NGOs around the complex and challenging issues of Internet censorship, privacy and surveillance.

Should you have any further questions, please do not hesitate to contact us at any time.

Sincerely yours,

Sandra Cornet-Vernet Lehongre
Director, Corporate Responsibility

© Nokia 2016

1 / 1

ANNEX 4: Response from Hacking Team

Dear Ms. Blum-Dumontet:

As you know, Hacking Team software is sold exclusively to governments and government agencies. Sales are regulated by Italian authorities. In cases in which a separate company is involved, Hacking Team still requires end users to certify in their contracts that the software will be used for lawful purposes and not used for any military activity. However, as you also know, the company does not identify individual clients or confirm information gleaned from stolen documents.

Privacy International has been a relentless critic of Hacking Team, and has enjoyed a good deal of publicity from this criticism. Nonetheless, I hope you will permit me to make a couple of obvious but generally ignored points about the product this company has developed and sells.

Of course, safeguards are important. That is why Hacking Team complies voluntarily and fully with the Wassenaar protocols implemented in Italy more than a year ago. For a Hacking Team sale to take place - to Egypt or elsewhere - it must be approved by the Italian authorities. We believe we are the only supplier of legal surveillance software to be subject to such regulation. Beyond complying with regulation, Hacking Team has always required customers to certify that they will use Hacking Team technology legally and not for military purposes. In fact, despite all the evidence published after the illegal attack on the company last July, there is nothing to show the company acted in any way illegally or in violation of any ban or regulation. Furthermore, the evidence clearly snows this technology is used as intended for law enforcement investigation and that the use of the technology is limited.

It is also worth noting that the sale of legal surveillance technology to Egypt is entirely legal. Egypt is an ally of the West including the U.S, most European countries and even of Israel. Not only is the sale of software to Egypt permitted, but also Western governments permit the sale of heavy weapons including F-16 fighter planes and Harpoon missiles to Egypt.

Finally, the sale of software for lawful surveillance is important for the protection of all of us. That is not only true of sales of such software to Western countries. Indeed, it may be even more important to provide tools for investigations in countries where there is wide-spread crime or terrorism or both. It should be obvious that investigating terrorists and their organizations in such a country could lead to the prevention of an attack in Paris, London or Berlin by those trained, financed and supported by elements that are active in the Middle East and elsewhere.

I hope you will include a full perspective of the situation in your forthcoming report.

Eric

ANNEX 5: Response from Siemens

Dear Mrs. Blum-Dumontet,

Thank you for your inquiry. First, I would like to make you aware that Siemens has transferred its network business to Nokia Siemens Networks, in April 2007. All relevant documents have been transferred to Nokia Siemens Networks as well, so we are not able to comment on the business that is related to Nokia Siemens Networks. Nokia Siemens Networks had been consolidated by Nokia.

In August 2013, Nokia Siemens Networks became Nokia Solutions and Networks. It is since then wholly owned by Nokia and will continue to be consolidated by Nokia.

I would like to ask you to address your questions to Nokia as we are unable to verify and to comment on your research.

Best regards,
Wolfram Trost