~~PRIVACY~~
~~INTERNATIONAL~~

For God and My President: **State Surveillance In Uganda**

Privacy International thanks the following individuals and organisations:

BBC Newsnight
Netzpolitik
The Citizen Lab (University of Toronto, Canada)
Claudio Guarnieri

We also acknowledge the dozens of individuals and organisations in Uganda, the United Kingdom and Germany who cannot be named. A handful of these took significant risk to share information with us, for which we are 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.

For God and My President:

State Surveillance In Uganda

October 2015

~~PRIVACY~~
~~INTERNATIONAL~~

www.privacyinternational.org

Chieftaincy of Military Intelligence building, Mbuya Hill, 2012.
Photo obtained by Privacy International.

List of Acronyms

A4C	Activists for Change
CCTV	Closed-Circuit Television
CDF	Chief of Defence Forces
CIID	Police Criminal Investigations and Intelligence Directorate
CMI	Chieftaincy of Military Intelligence
ESO	External Security Organisation
FDC	Forum for Democratic Change
ICT	Information and Communication Technology
IGP	Inspector General of Police
ISO	Internal Security Organisation
IT	Information Technology
JIC	Joint Intelligence Committee
LAN	Local Area Network
MP	Member of Parliament
NRA	National Resistance Army
NRM	National Resistance Movement
RICA	Regulation of Interception of Communications Act (2010)
UCC	Uganda Communications Commission
UPDF	Uganda People's Defence Force
UPF	Uganda Police Force

Executive Summary

Yoweri Museveni was re-elected to his fifth term as President of Uganda in February 2011. The electoral process was marred by widespread evidence of vote-buying and misuse of state funds. In April 2011, activists and opposition politicians organised loosely as Activists for Change (A4C) and launched a series of protests across the country to draw attention to police brutality and the rising cost of living. They encouraged Ugandans to peacefully walk to work in protest.

The Government reacted violently to the 'Walk to Work' protests and urban unrest. In the first month, Government forces killed at least nine unarmed people. Over 100 were injured. Kizza Besigye, the leading presidential challenger and the then-leader of the opposition Forum for Democratic Change (FDC) party was dragged from his vehicle and pepper sprayed in the face, sustaining serious injuries. Over 600 people were arrested and detained without charge. Some bore marks consistent with allegations of whipping and beatings. Members of Parliament were arrested, manhandled and placed under 24-hour surveillance and preventative detention. A4C launched a second round of protests in late 2011 which continued into 2012 before eventually subsiding in late 2012.

Behind the scene, officials of the Chieftaincy of Military Intelligence (CMI) and Uganda Police Force (UPF), acting on presidential orders, used an intrusion malware, short for malicious software, to infect the communications devices of key opposition leaders, media and establishment insiders. The secret operation was codenamed Fungua Macho ('open your eyes' in Swahili), according to documents acquired by Privacy International and published as part of this report.

The tool chosen as the 'backbone' of the operation, FinFisher, is intrusion malware at the time manufactured by the Gamma Group of companies, headquartered in the UK.[1] Once infected, a person's computer or phone can be remotely monitored in real time. Activities on the device become visible. Passwords, files, microphones and cameras can be viewed and manipulated without the target's knowledge.

The CMI and Police used state funds to purchase the full 'Fintrusion suite' in

[1] FinFisher operations and sales have since been spun off to "FinFisher GmbH", the new name (as of September 2013) for Gamma International GmbH, a German branch of Gamma Group.

late 2011. Over a period of 2011 to 2013, at least 73 people were involved in the operation targeting key opposition leaders, media and establishment insiders. Operatives bribed people close to their targets to get access to personal phones and computers on which they installed the malware, according to a confidential intelligence brief prepared for President Museveni. CMI officials also requested more funds to expand the operation and bribe further insiders. Obtaining personal information to use as blackmail was an explicit goal of the operation, according to secret Government documents.

Covert FinFisher 'access points' in the form of fake Local Area Networks (LANs) were installed within Parliament and key Government institutions. Actual and suspected Government opponents were targeted in their homes. Fake LANs and wireless hotspots were set up in apartment estates and neighbourhoods where many wealthy Ugandans and expatriates live.

Twenty-one hotels in Kampala, Entebbe and Masaka were also prepared to allow for infection of Operation Fungua Macho's targets. The management of some of the hotels collaborated with the operation to install fake Wi-Fi portals and install FinFisher on desktop computers in the hotels' business centres, according to the Ugandan military briefing document. All major conference hotels in Kampala, where high-level events such as heads of state meetings and political party conferences occur and business transactions are negotiated, were included in the target list contained in a Government document.

Gamma International GmbH, a German branch of Gamma Group, sold FinFisher to the Ugandan Government. By training Ugandan officials on the use of FinFisher, Gamma International GmbH provided indirect support to operation Fungua Macho. Gamma's response to this investigation is included as an annex.

Gamma trained four Ugandan officials to use FinFisher in Germany in December 2011. On the 19th and 20th January 2012, two Gamma officials met with senior intelligence officials in Kampala and briefed them on FinFisher's capabilities, according to a company document obtained by Privacy International from a separate source.

Ugandan police and military officials travelled to Germany and the Czech Republic as visitors of Gamma to attend ISS (Intelligence Support Systems) World, the key international surveillance trade show, in June 2012, according to company documents. The Ugandan officials attended demonstrations of surveillance products from Gamma partner companies from around the world. These companies sell technologies including centralised communications monitoring centres. Oelkers reportedly returned to Kampala at least three

times in 2013, according to the Wikileaks Counter Intelligence Unit.
Next year, Ugandans will vote in the fifth presidential election since President Museveni first came to power in 1986. As preparations for the election progress, complaints of bias against opposition candidates and restrictions on political organising are increasing. The Government is widely assumed to be increasing its surveillance efforts against persons opposed to President Museveni's candidacy, as journalists and activists prepare to weather the political storm.

The Ugandan Government is also currently in advanced stages of procuring a communications monitoring centre, five years after its Parliament passed the Regulation of Interception of Communications Act. In 2013, the inter-agency Joint Security/ICT technical committee invited bids for the project from seven technology companies based in China, Israel, Italy, Poland and the United Kingdom.

While it was expected that the monitoring centre would be operational by the 2016 elections, at the time of writing it is not. The Police also attempted to procure further technologies from intrusion malware supplier and rival to Gamma Group, Hacking Team, in mid-2015.

The Walk to Work movement subsided in 2012. Popular support for the movement dwindled. The A4C pressure group was declared illegal. Attempts to organise publicly were consistently intercepted and dispersed.

The targeting of political opponents and others for surveillance without a court warrant is illegal under the Regulation of Interception of Communications Act. However, the Anti-Terrorism Act (2002) gives almost unfettered discretion to intercept communications and carry out surveillance, without judicial authorisation and oversight. Ugandan laws and oversight mechanisms need to be significantly reformed and strengthened to ensure compliance with international human rights, including privacy, freedom of expression and peaceful assembly. This is particularly important in light of the use of surveillance technologies such as FinFisher malware as described in the evidence obtained by Privacy International.

Along with more heavy-handed tactics, the use of surveillance technology has chilled free speech and legitimate expressions of political dissent. Covert, extrajudicial surveillance projects like those documented in this report have contributed to making Uganda a less open and democratic country. This situation is likely to worsen with the eventual addition of the centralised communications monitoring centre under the intelligence services' control. Unless these issues are addressed, claims that Uganda is a burgeoning democracy ring hollow.

Recommendations

To the Parliament of Uganda

- Conduct an inquiry on Operation Fungua Macho ('the operation') to:
    - establish the timeline and individuals responsible for the operation
    - establish the extent of surveillance using FinFisher products and other surveillance technologies during the operation
    - identify the individuals and institutions targeted
    - identify the 70+ individuals claimed by the Chieftaincy of Military Intelligence to be involved in the operation
    - establish whether and the extent to which, properly approved warrants were sought to carry out surveillance under the operation
    - establish the amount of state funds used during the operation
    - investigate Chieftaincy of Military Intelligence claims that state funds were used to fund 'bribery' and 'blackmail' under the operation
    - investigate whether state agents' activities under the operation are in violation of the Computer Misuse Act (2011);
- Publish and make publicly accessible all results of the inquiry.
- Provide the legal basis under which this operation was authorised.

To the Ministry of Justice and Constitutional Affairs

- Review the Regulation of Interception of Communications Act (2010) – including with the view to:
    - ensuring that it applies to all interception of communications, including in the context of anti-terrorism investigation;
    - limiting the scope of interception of communications to the investigation of serious crimes or actual threats to national security; and
    - requiring court warrant for accessing of communication data as well as content of communications.
- Review the Anti-Terrorism Act (2002) to bring it into line with international

human rights law, including with the view to repealing Part VII on Interception of communications and surveillance.

- Establish an independent and effective oversight mechanism (such as a Surveillance Commissioner) with a mandate to monitor the all stages of interceptions of communications under the revised Regulation of Interception of Communications Act to ensure they are compliant with Uganda's domestic and international commitment to the right to privacy and other human rights.
- Assess and determine whether the use of FinFisher and other intrusion malware is compliant with Uganda's domestic and international human rights obligations and make publicly available any findings related to the above inquiry;
- Ensure that its communication surveillance laws, policies and practices adhere to international human rights law and standards including the principles of legality, proportionality and necessity; and take the necessary measure to ensure that all interception activities – including access to stored communications – are subject to prior judicial authorisation.

To the Auditor General, and Public Accounts Committee, Uganda Parliament

- Review all classified expenditures by the Office of the President, the Uganda Police Force and the Uganda People's Defence Force for the past five years and identify any purchases of equipment that can be used to intercept or monitor communications, including communications content and metadata;
- Make publicly available the results of the review.

To the Office of the President, the Uganda Police Force and the Uganda People's Defence Force

- Cease all use of intrusion malware such as FinFisher and other products;
- Halt all procurement of intrusion malware and other hacking tools pending the results of the Parliamentary inquiry;
- Halt the procurement of the monitoring centre required by the Regulation of Interception of Communications Act (2010) pending the results of the Parliamentary inquiry
- Abide by any reformed legislation governing communications surveillance.

To the named hotels and housing estates

- Investigate the extent to which FinFisher was deployed within their establishments;
- Cease cooperation with surveillance operations, pending the results of a Parliamentary inquiry.

To the Export Control Organisation within the Department of Business Innovation and Skills of the Government of the United Kingdom, and the Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) of the German Government

- Investigate the lawfulness of any transfers of products or training from the Gamma Group, FinFisher and/or affiliated companies and Ugandan end-users from 2011 to the present;
- Make publicly available the results of the investigation
- Ensure national and EU regulations require that human rights criteria are assessed by licensing authorities for any applications for the export of FinFisher, other spyware, and other surveillance technologies;
- Ensure that all future exports of surveillance technologies, including the export of monitoring centres, are assessed in accordance with human rights criteria and an assessment of the legal framework in the country of destination governing the use of the technology.

The Plan

Uganda's Government has been led by the National Resistance Movement (NRM) under the direction of President Yoweri Museveni since 1986. In his almost thirty years of rule, the Ugandan Government has built up an intelligence apparatus that concentrates power around the President in a number of overlapping and competitive intelligence and police agencies.

Intelligence structures

The power to gather intelligence and conduct surveillance are concentrated around three institutions: the Uganda People's Defence Force (UPDF), the Uganda Police Force (UPF), and the Office of the President (State House). The President exercises control over sensitive intelligence operations while day-to-day spying for intelligence gathering appears less centralised. Senior leaders and technical experts within intelligence circles are often reshuffled and reassigned among these agencies on Presidential direction.[2]

The 1987 Security Organisations Act established the Internal Security Organisation (ISO) and External Security Organisation (ESO). These two agencies are directed by Director Generals appointed by, and accountable to, the President, and exist to collect intelligence and provide advice on Uganda's security directly to the President.[3]

The 2003 Police Act gives the President the power to appoint the Police Inspector General and his deputy, as well as the majority of the members of the Police authority which oversees police functions, and veto power over any potential dismissals of senior-ranking officials.[4] As Commander-in-Chief of the defence forces, the President may appoint the Chief of Defence Forces and virtually all high-ranking officials[5] and enjoys discretionary powers over the activities of the High Command.[6]

[2] See for example 'Museveni reshuffles army generals', New Vision, 29 December 2011, http://www.newvision.co.ug/news/315138-museveni-reshuffles-army-generals.html and 'Don't underestimate Muhoozi, Museveni tells top commanders', The Independent, 21 June 2013, http://www.independent.co.ug/cover-story/7929-dont-underestimate-muhoozi-museveni-tells-top-commanders

[3] Art 3, Security Organisations Act (1987)

[4] Art 5, 8, Police Act (1994)

[5] Art 8, UPDF Act (2005)

[6] Each UPDF officer is required to declare allegiance first to the President and then the Republic of Uganda: "I... Swear by the almighty God/do solemnly and sincerely declare and affirm that [he/she] will be faithful to and bear true allegiance to the President and the Republic of Uganda." Fifth Schedule, UPDF Act (2005)

The National Security Council, established in 2000, responds directly to the President[7] and comprises cabinet ministers, ISO, ESO, army and police officials, most of which are appointed by the President and up to five additional members, also appointed by the President and approved by Parliament.[8] The Joint Intelligence Committee, composed of security experts appointed by the President and chaired by the Minister of Internal Affairs, reportedly meets once a week to share intelligence on national security threats.[9] An Information and Communication Technologies (ICT) Technical Committee within the Joint Intelligence Committee advises on technology purchases and is responsible for many decisions related to defence and intelligence procurement, as this report shows.

Confidential coffers

Much of the equipment used in military and intelligence operations is procured using classified expenditure budgets. These budgets are audited by the Auditor General and reviewed by the Parliamentary Defence and Internal Affairs Committee, though members told Privacy International that they have never seen a detailed report on how the classified expenditures are spent.

The Government's use of confidential 'classified expenditures' budgets has increased significantly. The classified expenditure allocation under the Ministry of Defence budget doubled from UGX 122 billion (US$ 48.9 million) in the 2012-2013 fiscal year to UGX 300 billion (US$ 115.38 million) in 2013-2014,[10] despite protests from Members of Parliament who alleged that the use of classified budgets risked breeding corruption and diverting resources[11] from priorities like soldier salaries and military hospitals.

The 2015-2016 defence budget is at its highest ever – UGX 1.4 trillion (US$ 442 million). UGX 607 billion[12] (US$ 190.8 million) was designated as classified, prompting concerns[13] funds were being diverted to the President's election campaign.[14]

[7] Art 219, Constitution of Uganda (1995)

[8] National Security Council Act (2000)

[9] "Terror in Kampala", The Independent, 18 July 2010, http://www.independent.co.ug/index.php/cover-story/cover-story/82-cover-story/3198-terror-in-kampala-

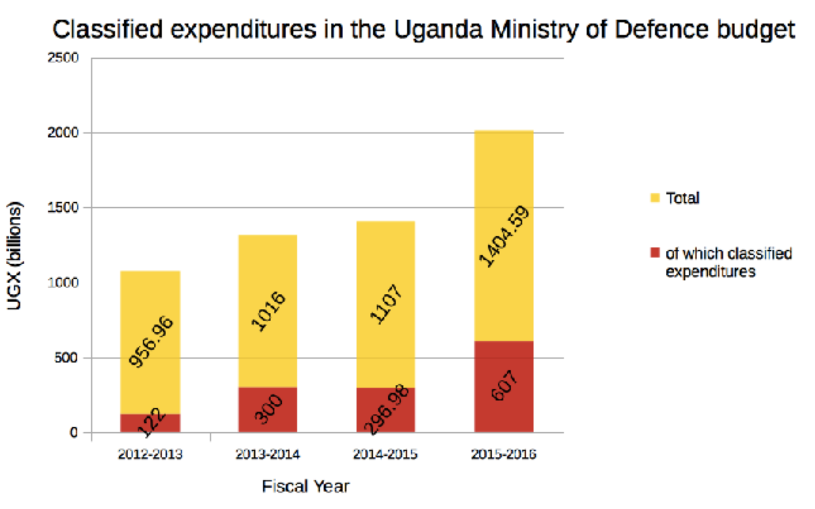
[10] "Report of the Committee on Defence and Internal Affairs on the Ministerial Policy Statements and Budget Estimates for the Fiscal Year 2013-2014-3, August 2013. Figures account for currency exchange rates. Classified expenditures represented 12.7% the 2012-2013 fiscal year Ministry of Defence budget (UGX 956.96 billion) and 29% of the 2013-2014 budget (UGX 1.016 trillion)

[11] "MP Wants Classified Expenditure Off Budgeting System", Red Pepper, 5 September 2013, http://www.redpepper.co.ug/mp-wants-classified-expenditure-off-budgeting-system/

[12] Represents 43% of total budget. Ministry of Defence Vote 004 Policy Statement, FY 2015/2016, April 2015

[13] Hansard, Uganda Parliament, 26 May 2015. http://www.parliament.go.ug/cmis/browser?id=workspace%3A//SpacesStore/b487b970-607a-493b-8ac0-4512a1033903

[14] Ugandan Defence Minister Crispus Kiyonga stated that "[t]he budget for Defence cannot be used for elections. It's just a coincidence that our expenditures under classified have increased because we have critical needs." "Tempers flare in House over Shs1.4 trillion Defence budget", Daily Monitor, 27 April 2015, http://mobile.monitor.co.ug/News/Tempers-flare-in-House-over-Shs1-4-trillion-Defence-budget/-/2466686/2698122/-/format/xhtml/-/137mfl8/-/index.html



The military's "classified expenditures" budget has increased significantly since 2012. Source: Ministry of Defence budget documents.

Spy plots and intelligence rivalries

Uganda's intelligence agencies, and the military in particular, have been accused of illegally surveilling and wiretapping phone since the mid-2000s. The CMI was wiretapping phones from its headquarters in 2006, according to Radio Katwe,[15] and monitoring politically important individuals and foreign phone numbers calling certain regions of Uganda.[16] Most politicians with whom Privacy International spoke assume that their phones have been or are currently monitored.

The close control that Ugandan law accords the President over the country's intelligence agencies has not prevented intelligence failures and rivalries within and among agencies. In 2013, the President reportedly demanded the reorganisation of the ISO and ESO following the publication by the Daily Monitor of information implicating the President in an assassination plot against a top security official opposed to an alleged plan to install Museveni's son as the country's next President.[17] In 2015, the Special Branch unit of the UPF was disbanded for allegedly passing on intelligence reports to foreign governments.[18] That year, the Police Criminal Investigations and Intelligence Department (CIID) was split into two units and a new one was inaugurated under direct control of the Inspector General of Police.

[15] Radio Katwe stands by story on CMI phone-tapping in Uganda", Radio Katwe, 15 March 2006, http://katwe.blogspot.co.uk/2006/03/radio-katwe-stands-by-story-on-cmi.html

[16] Radio Katwe's website was blocked during the 2006 elections and shut down shortly following the CMI report

[17] "Museveni wants spy agencies overhauled", Daily Monitor, 15 July 2013, http://www.monitor.co.ug/News/National/Museveni-wants-spy-agencies-overhauled/-/688334/1914988/-/14idpyv/-/index.html

[18] "Police spy unit disbanded due to indiscipline – Kayihura", Daily Monitor, 26 January 2015, http://www.monitor.co.ug/News/National/Police-spy-unit-disbanded-due-to-indiscipline---Kayihura/-/688334/2602054/-/xuejmtz/-/index.html

The new Special Operations Unit was quickly accused of duplicating the work of the CIID, the Flying Squad and other units.[19]

Insulated from the reshuffling of intelligence responsibilities, the President's son, Brigadier Muhoozi Kainerugaba,[20] directs an autonomous and well-resourced unit, the Special Forces Command.[21] The unit is responsible for the President's security and reportedly conducts the most sensitive spying operations at his request.[22]

Regulating surveillance

The Regulation of Interception of Communications Bill, first proposed in 2007, attempted to regulate communications surveillance. The Bill would allow for lawful interception and monitoring of communications across Uganda's telecoms networks.[23] It was read for the first time in Parliament in April 2008, but had stalled for two years. Parliamentarians questioned the lack of detail in the ICT Committee's report on consultations around the Bill and various other provisions.

But the Bill became law following twin bomb attacks in Kampala in July 2010. As Ugandans gathered in bars and restaurants to watch the FIFA World Cup final on 11th July, militants[24] linked to the Islamist group Al Shabaab detonated bombs at Lugogo Rugby Club and the Ethiopian Village restaurant, killing over 70 people and shocking the nation.[25] Three days later, the Ugandan Parliament passed the Regulation of Interception of Communications Act 2010 (RICA).

RICA requires intelligence officials, including the Police,[26] to seek judicial authorisation for interception of communications.[27] The law authorises

[19] "New anti- crime unit, CIID clash" , Daily Monitor, 20 April 2015, http://www.monitor.co.ug/News/National/New-anti-crime-unit--CIID-clash/-/688334/2690952/-/mf7pmpz/-/index.html

[20] Kainerugaba cut his teeth as commanding officer for the Motorized Infantry Unit of his father's Presidential Guard Brigade, soon after graduating from the UK's Royal Military Academy Sandhurst in 2000.

[21] "Brig. Muhoozi Kainerugaba, the Commander Special Forces Command", UPDF, 21 June 2014, http://specialforcescommand.go.ug/brig-muhoozi-kainerugaba-the-commander-special-forces-command/

[22] The group is the most recent manifestation of the President's personal protection unit, the High Command Unit founded within the National Resistance Army (NRA) during the 'Bush War' struggle that brought President Museveni to power. Headquartered in Entebbe, the unit is a specialised component of the UPDF tasked with carrying out special missions. It is accountable directly to its commander, currently the President's son, Muehoozi Kainerugaba, who in turn reports directly to both the Chief of Defense Forces (currently Katumba Wamala) and the President. It does not appear to have been established by any law. See "Mission", UPDF, 2015, http://portal.defence.go.ug:10039/wps/portal/mod-home/armed-forces/special-forces-command/!ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOIt_Q0sDL0NjLz8Lf3NDRwtDEwDA41dDQxczPULsh0VAUeQFfY!/ and "History of the UPDF-SFC", UPDF, 18 June 2014, http://specialforcescommand.go.ug/history-of-the-updf-sfc/

[23] Hansard, Uganda Parliament, 22 June 2010. http://www.parliament.go.ug/cmis/browser?id=workspace%3A//SpacesStore/a7bf58da-b555-4647-a806-ae5605f5c352

[24] "Somali militants 'behind' Kampala World Cup blasts", BBC News, 12 July 2010, http://www.bbc.co.uk/news/10602791

[25] "Militants Find Symbolic Targets in Uganda", Wall Street Journal, 13 July 2010, http://www.wsj.com/articles/SB10001424052748704288204575362400675683926

[26] The CDF, and Directors General of ESO and ISO, and the Inspector General of Police or any of their nominees (Art 4).

[27] Hansard, Uganda Parliament, 24 June 2010. http://www.parliament.go.ug/cmis/browser?id=workspace%3A//SpacesStore/6e119547-471b-4a7b-b4d3-0191f89c0627

intelligence officials[28] to apply to intercept communications subject to a warrant issued by a designated judge and not, as an earlier version of the Bill stated, the Minister of Security.

Telecommunications and internet service providers are required to ensure their services are technologically capable of allowing lawful interception, and in such a way so that the target of the interception remains unaware of it.[29] Furthermore, the Act requires service providers to retain metadata, although the terms and conditions of the retention are not specified in the Act.[30]

The Act also provided for the establishment of a Monitoring Centre under the control of the Minister[31] – the "sole facility through which authorised interceptions shall be effected."[32]

But this law does not clarify the practice of surveillance in Uganda.

Firstly, the law does not replace the provisions for interception contained in the Anti-Terrorism Act 2002 – it appears to contradict them. This law gives almost unfettered discretion for state officials to conduct surveillance, without the need to obtain judicial authorisation. The powers of surveillance are broad, including interception of phone calls, emails or other communications, 'electronic surveillance', as well as monitoring of meetings, or doing "any other thing reasonably necessary" for the purpose of surveillance.[33] And the justifications of such surveillance are very broad, including safeguarding public interest, and protecting the national economy from terrorism.[34]

Secondly, the opacity of the surveillance practices in Uganda is compounded by Government unwillingness to disclose information and the lack of effective independent oversight of intelligence agencies. When an MP asked about the status of the monitoring centre project, then Minister of Security Amama Mbabazi refused.[35] The monitoring centre project – and state of communications surveillance in Uganda in general – would remain in the shadows.

[28] The CDF, DG of ESO, DG of ISO and IGP or any of their nominees (art 4)

[29] Art 8, Regulation of Interception of Communications Act (2010)

[30] Art 11, Regulation of Interception of Communications Act (2010)

[31] Art 1, Regulation of Interception of Communications Act (2010)

[32] Art 3, Regulation of Interception of Communications Act (2010)

[33] Art 19(5), Regulation of Interception of Communications Act (2010)

[34] Art 19(4), Regulation of Interception of Communications Act (2010)

[35] Hansard, Uganda Parliament, 23 July 2014, http://www.parliament.go.ug/cmis/browser?id=workspace%3A//SpacesStore/1e87bcc0-e5f6-4a97-8849-07e2135227a0

The 2011 Elections and Walk to Work

On 18th February 2011, Ugandans went to the polls to choose their leader and national representatives. President Museveni won with over two-thirds of the popular vote. Museveni had triumphed over the opposition in 2001 and 2006 through fraud,[36] intimidation and violence leading up to polling day.[37] The opposition, rallied by the leading contender and Museveni's former ally Kizza Besigye, rejected the results on both occasions and unsuccessfully contested the results in court.

The 2011 election was noticeably less turbulent than the previous two cycles.[38] The NRM party largely succeeded in buying off voters and disproportionately directing state resources towards the President's campaign. Yet the new administration was caught off guard a few months later when activists and opposition politicians organised protests across the country to draw attention to police brutality and the rising cost of living. They encouraged Ugandans to peacefully 'walk to work.'

In the first month of the protests at least 600 people were arrested and detained without charge; some bore marks consistent with allegations of whipping and beatings. Nine unarmed persons were killed.[39] Members of Parliament were arrested, manhandled and placed under 24-hour surveillance.[40] Citing the Criminal Procedure Code, the Police preventatively arrested protest leaders[41] and disrupted gatherings. Plainclothes and uniformed officers beat protesters. Besigye was pepper sprayed in the face, dragged from his car and arrested, sustaining serious injuries. On the day Museveni was inaugurated into his third elected term, the Police used teargas to disperse crowds who had gathered along the road to the airport to welcome Besigye, who was returning from medical treatment in Nairobi.

Protests continued throughout 2011. The Government, in turn, was engaged in a fierce war of words against the movement. The Police publicly accused Activists for Change (A4C) of attempting to illegal import arms and of

[36] "Uganda hit by violence as opposition claims election fraud", The Guardian, 26 February 2006, http://www.theguardian.com/world/2006/feb/26/uganda.deniscampbell

[37] "Uganda: Election Irregularities Require Judicial Probe", Human Rights Watch, 2 March 2006, https://www.hrw.org/news/2006/03/02/uganda-election-irregularities-require-judicial-probe

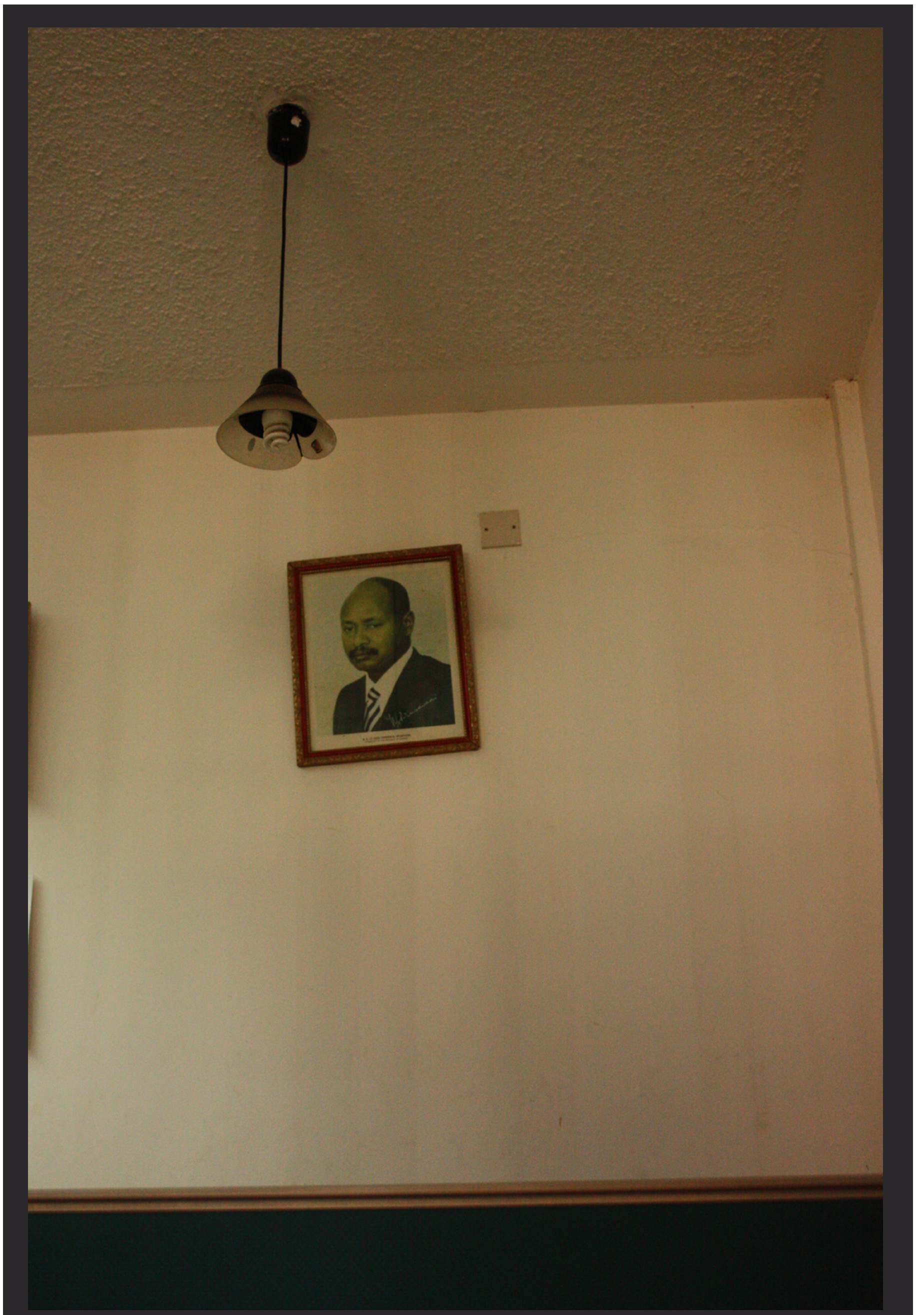
[38] The European Union observation mission called the 2011 election process "fairly open and free". By contrast, during the 2006 elections, the government launched legal cases against Besigye on charges of treason and terrorism, among others and violence was reported leading up to polling day. See "EU election observation mission to Uganda in 2011", EU, 2011, http://eeas.europa.eu/eueom/missions/2011/uganda/index_en.htm and "Uganda Presidential and Parliamentary Elections", EU, 23 February 2006, http://www.geneseo.edu/~iompress/Archive/final.pdf

[39] Uganda: Launch Independent Inquiry Into Killings", Human Rights Watch, 8 May 2011, http://www.hrw.org/news/2011/05/08/uganda-launch-independent-inquiry-killings

[40] "Besigye's home under surveillance", Daily Monitor, 16 August 2011, http://www.monitor.co.ug/News/National/-/688334/1219632/-/bkej2az/-/index.html

[41] "Besigye detained under colonial law", Daily Monitor, 20 May 2011, http://www.monitor.co.ug/News/National/-/688334/1166110/-/c1gr93z/-/index.html and "Police Arrest Mpuuga for late Night Interrogation", Uganda Radio Network, 25 April 2011, http://ugandaradionetwork.com/story/police-arrest-mpuuga-for-late-night-interrogation

sending young people to train as terrorists in Afghanistan.[42] The movement's leadership, meanwhile, was preparing to relaunch a second round of protests in January 2012.



A greying photo of President Museveni watches over a hotel business centre in Entebbe. Photo: Privacy International, 2015.

[42] "Opposition planning to import guns, says IGP", Daily Monitor, 25 December 2011, http://www.monitor.co.ug/News/National/-/688334/1295050/-/bfk4thz/-/index.html

The Spyware

By December 2011, the Government knew it was facing a political crisis. On 5th December, the Directorate of Technical Intelligence of the UPDF purchased[43] a powerful surveillance tool that they would use to illegally spy on protest organisers, Government officials, media houses, intelligence insiders, and private citizens in an operation called ‘Fungua Macho’(which translates as ‘open your eyes’), according to a secret presidential briefing document on the operation, which is included as an annex.

Gamma and company

The tool in question was the ‘Complete IT Intrusion Portfolio’ of ‘FinFisher’, a surveillance malware supplied by Gamma International GmbH. The Gamma group of companies is widely known for producing FinFisher. Gamma Group is headquartered in the UK where it has at least three companies listed at its Hampshire address.[44] In 2013, production of FinFisher was spun off into a Germany-based company, FinFisher GmbH, the new trading name for Gamma International GmbH. Gamma has a network of companies including holding and shell companies abroad. There are at least four Gamma-linked companies in Lebanon,[45] including one linked to Elaman, a partner company to Gamma and also reportedly its international sales agent. Gamma has a regional office in Malaysia and a company registered in the British Virgin Islands.

Stephan Oelkers is at the centre of Gamma/FinFisher’s international network. He is Managing Director of FinFisher GmbH, CEO of FinFisher Labs GmbH, Managing Director of FinFisher Holding GmbH, and was CEO of Gamma International Holding GmbH in mid-2013 – all based in Munich, Germany.

Oelkers personally travelled to Uganda as part of Gamma International GmbH’s business with the Ugandan government. On 19th and 20th January 2012, he and a colleague, Alexander Hagenah, presented a FinFisher IT

[43] The purchase was made by CMI, within the UPDF’s budget, which falls under the Ministry of Defence budget. See for example Section 3 Security Sector, National Budget Framework Paper, 2012-2013, Government of Uganda.

[44] Gamma International (UK) Ltd (Company No. 06343869), Gamma TSE Ltd (Company No. 03821494 – to which the Gamma Group website specifically refers), G2 Systems Ltd (Company No. 04027614) are all incorporated within the UK and registered with Companies House in London. They share the registered address of 25 St Thomas St, Winchester, Hampshire SO23 (which is the location of professional companies secretaries’ corporation) and share some company directors.

[45] “Ethiopia expands surveillance capacity with German tech via Lebanon”, Privacy International, 23 March 2015, https://www.privacyinternational.org/?q=node/546

Intrusion Seminar to Ugandan government officials. Business cards shared at the meeting and an excerpt of the seminar Powerpoint slides are included as annexes.[46]

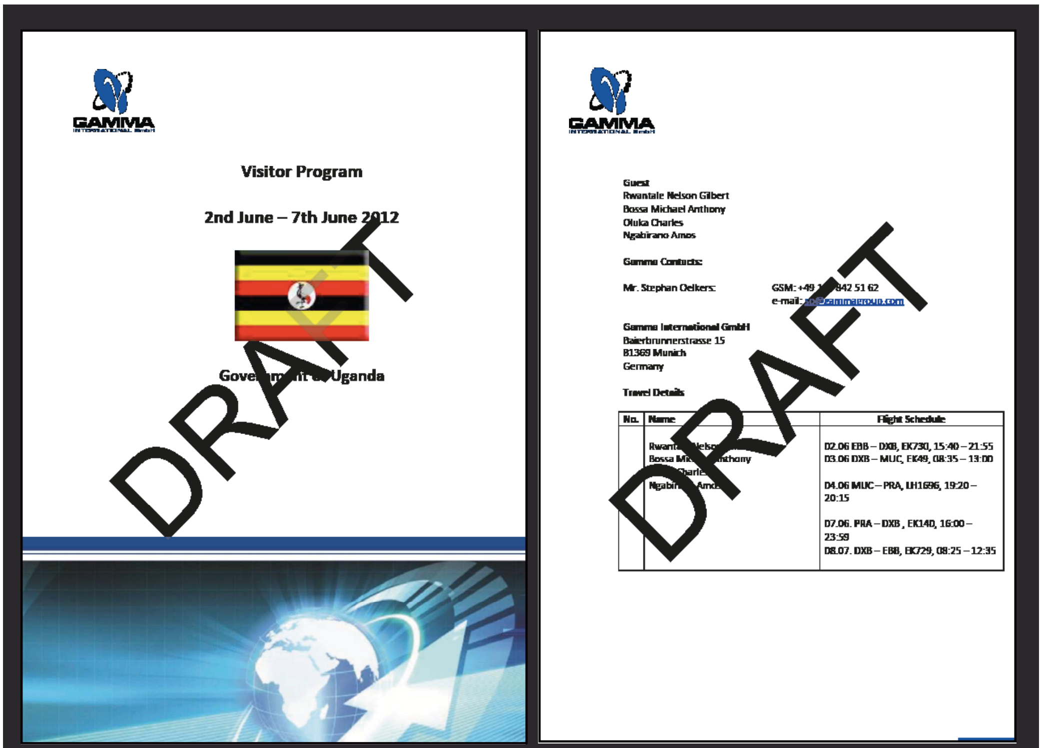
Showcasing spyware

Gamma and FinFisher representatives pitch their products directly to governments in private meetings and at specialised security and defence trade shows. In June 2012, four Ugandan officials travelled as guests to Gamma's Munich offices, where they were invited to witness demonstrations of products from Gamma partner companies Trovicor (Germany), Utimaco (Germany), Polaris (US), Cobham (UK) and 1rstWAP (Indonesia). A few days later, they travelled to ISS (Intelligence Support Systems) World (popularly known as the 'Wiretapper's Ball') in Prague and stayed in the Clarion Congress Hotel, according to confidential company documentation obtained by Privacy International, included as an annex.

Intrusion technologies are capable of collecting, modifying and extracting data communicated and stored on a device. To do this, malware must be installed on the device. Once installed, it embeds itself in all system functions, collecting and transmitting data to the operator as the infected device operates normally from the user's perspective. This data can include a real-time recording of the user's screen; live audio and video feeds from the device's camera or microphone; and communications sent from the device. Even passwords for services can be collected. Encryption provides no protection against FinFisher – data that is encrypted or password-protected could still be available to the malware operator.

Intrusion technologies can monitor Voice over IP communications (e.g. Skype), telephone calls, email, messenger chats, the exact device location, webcams and microphones, and every password entered in the device. Collected information is then inconspicuously transferred through international networks of servers to the operator of the intrusion technology. Intrusion systems, like Gamma's, are designed and regularly tested to avoid detection by antivirus programmes. This makes such intrusive software incredibly difficult to detect on a machine using the conventional antivirus software that many users assume will protect them.

[46] This is not the first time Gamma-linked interests have been present in Uganda.The largest shareholder in Gamma International GmbH is Louthean John Alexander Nelson. In 2008, CBRN Team Limited, a security company Nelson directed from 2006 until its dissolution in 2011, won a contract to provide training and equipment in advance of the Commonwealth Heads of Government Meeting (CHOGM) in 2007. CBRN Team Limited's financial director pleaded guilty in a UK court to making corrupt payments to a Ugandan government adviser on technology. There is no evidence Nelson or the Gamma companies were involved in the case.



GAMMA INTERNATIONAL GmbH

Visitor Program

2nd June – 7th June 2012

Government of Uganda

DRAFT

GAMMA INTERNATIONAL GmbH

Guest
Rwantale Nelson Gilbert
Bossa Michael Anthony
Oluka Charles
Ngabirano Amos

Gamma Contacts:

Mr. Stephan Oelkers: GSM: +49 1 842 51 62
e-mail: so@gammagroup.com

Gamma International GmbH
Baierbrunnerstrasse 15
81369 Munich
Germany

Travel Details

No.	Name	Flight Schedule
	Rwanta Nelso Bossa Mi nthony Charle Ngabir Amo	02.06 EBB – DXB, EK730, 15:40 – 21:55 03.06 DXB – MUC, EK49, 08:35 – 13:00 04.06 MUC – PRA, LH1696, 19:20 – 20:15 07.06. PRA – DXB , EK140, 16:00 – 23:59 08.07. DXB – EBB, EK729, 08:25 – 12:35

DRAFT

Four Ugandan government officials visited Gamma's Munich headquarters and surveillance trade show ISS World in Czech Republic in June 2012. Source: Excerpted document obtained by Privacy International.

Facilitating repression

Using FinFisher, the Ugandan Government intended to gather "hordes of data" on "negative minded politicians" with the aim of "easily crushing them by being a step ahead", as the Presidential briefing document describes. FinFisher would have been an ideal tool for this goal. FinFisher has been used by some of the most repressive states globally to intimidate, harass and blackmail.

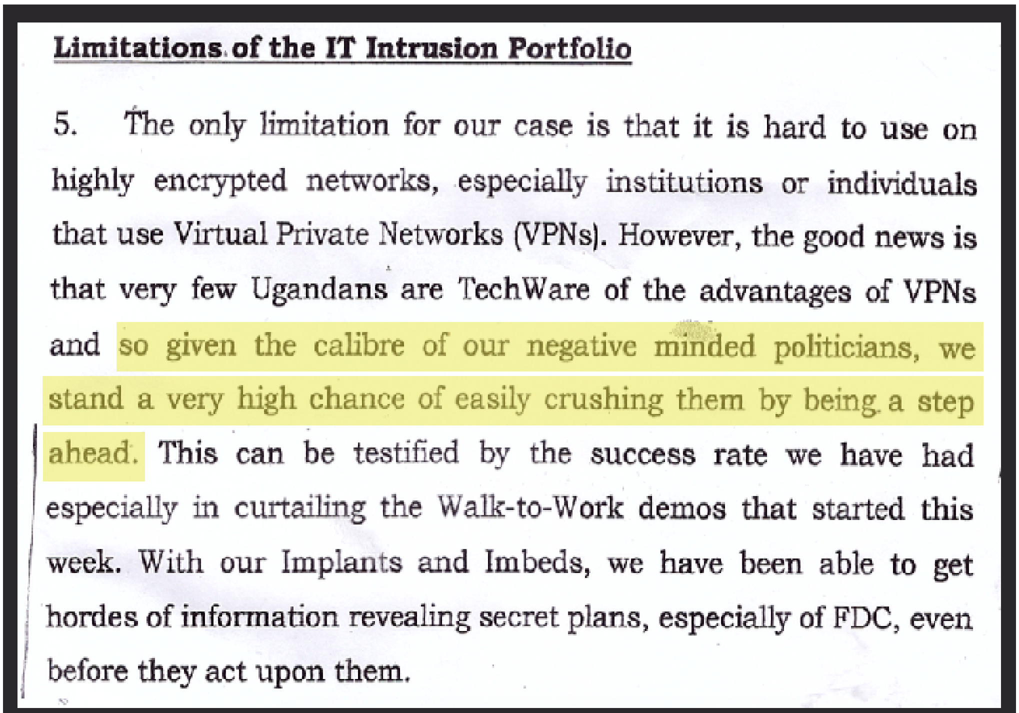
Case Study: FinFisher Cases

Moosa Abd-Ali Ali, Jaafar Al Hasabi and Saeed Al-Shehabi are three pro-democracy activists from Bahrain who suffered variously from years of harassment, imprisonment and torture at the hands of the Bahraini Government. They have been granted asylum in the UK. In 2014, leaked Gamma documents revealed that the three were among a group[47] of prominent Bahraini lawyers, politicians and activists targeted by the Bahraini Government using FinFisher.[48]

[47] Bahrain Watch identified a list of 77 computers infected by Bahraini authorities as part of the leaked documents. "Bahrain Government Hacked Lawyers and Activists with UK Spyware", Bahrain Watch,7 August 2014, https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/

[48] Gamma International GmbH had previously denied that it had ever sold the Bahrain government the spyware following a forensic investigation by The Citizen Lab. Martin Muench, speaking for Gamma, suggested that they may have acquired a demonstration copy of the product. "Gamma Says No Spyware Sold to Bahrain; May Be Stolen Copy", Bloomberg Business, 27 July 2012, http://www.bloomberg.com/news/articles/2012-07-27/gamma-says-no-spyware-sold-to-bahrain-may-be-stolen-copy

The Ethiopian Government is also a FinFisher client.[49] Tired of living under constant surveillance and harassment, Ethiopian dissident Tadesse Kersmo and his wife left for the United Kingdom in 2009 where they were subsequently granted asylum. In April 2013, Mr Kersmo became aware of a report published by the Citizen Lab, an interdisciplinary research lab at the Munk School of Global Affairs of the University of Toronto, that mentioned a spyware campaign targeting members of Ginbot 7, an Ethiopian opposition group. A subsequent analysis by Privacy International and Bill Marczak, a research fellow at the Citizen Lab, of Mr Kersmo's computer suggests that in June 2012, three years after escaping persecution, his computer appears to have been infected with one of the FinFisher products, FinSpy.



Limitations of the IT Intrusion Portfolio

5. The only limitation for our case is that it is hard to use on highly encrypted networks, especially institutions or individuals that use Virtual Private Networks (VPNs). However, the good news is that very few Ugandans are TechWare of the advantages of VPNs and so given the calibre of our negative minded politicians, we stand a very high chance of easily crushing them by being a step ahead. This can be testified by the success rate we have had especially in curtailing the Walk-to-Work demos that started this week. With our Implants and Imbeds, we have been able to get hordes of information revealing secret plans, especially of FDC, even before they act upon them.

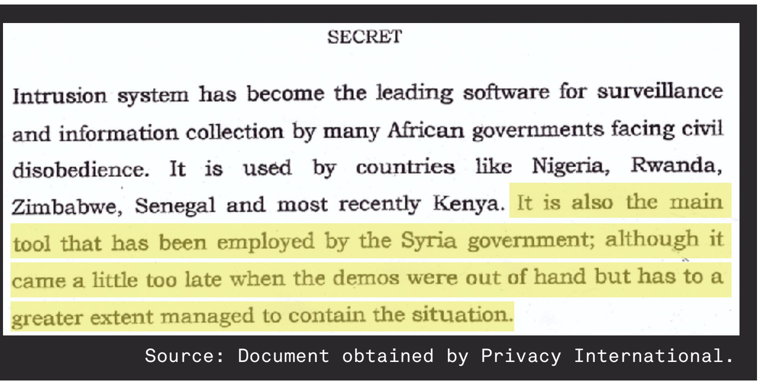
Operation Fungua Macho, launched after President Museveni was reelected in 2011, targeted organisers of the Walk to Work demonstrations and Forum for Democratic Change (FDC) opposition party, among others. Source: Document obtained by Privacy International.

[49] "You Only Click Twice: FinFisher's Global Proliferation", The Citizen Lab, 13 March 2013, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

Michael Bbosa, then Director of Technical Intelligence, assured President Museveni in his ‘Progress Report on Operation Fungua Macho’ that Kenya, Nigeria, Rwanda, Senegal and Zimbabwe – governments “facing civil disobedience” – were users of FinFisher. Governments in all these countries have been accused of massive human rights violations. If governments of these countries are indeed using FinFisher, then those countries would join a list of 25 other countries that are reportedly FinFisher clients, according to research by The Citizen Lab.[50]

In a bid to impress the President, Bbosa made a further boastful claim that Syria is a FinFisher user. Syria has been wracked by civil war since protests against the Government erupted early 2011. The conflict gradually morphed from prominent protests to an armed rebellion after months of military sieges. “It [the intrusion system] is also the main tool that has been employed by the Syria government,” stated Michael Bbosa, “although it came a little too late when the demos were out of hand, but has to a greater extent managed to contain the situation.” Gamma’s response is included as an annex.

The Director of Technical Intelligence of the UPDF claimed in the Presidential briefing document that FinFisher was used in a number of countries, including Syria. Privacy International was not able to verify this claim.



SECRET

Intrusion system has become the leading software for surveillance and information collection by many African governments facing civil disobedience. It is used by countries like Nigeria, Rwanda, Zimbabwe, Senegal and most recently Kenya. It is also the main tool that has been employed by the Syria government; although it came a little too late when the demos were out of hand but has to a greater extent managed to contain the situation.

Source: Document obtained by Privacy International.

Infections

FinFisher can be installed on a device in a number of different ways. In less than five minutes, the FinFisher malware can be inserted directly onto a phone or computer. For particularly security-savvy targets, FinFisher can be disguised as a PDF, word processing document or other file that the target will inadvertently download and execute; or as a fake website which, when visited by the target, will download FinFisher onto the target’s device. A device can also be infected by connecting to a fake network access point. This can be a Wi-Fi log-in screen disguised as an ordinary hotspot portal. FinFisher is designed to activate with a simple inadvertent click by the user. It is designed to bypass most antivirus programs.

[50] These include Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, United Kingdom, United States, and Vietnam.

Compromising public institutions

The CMI and UPF put much effort into their infection plans, as detailed in a presidential briefing document. The CMI complained about the "meagre funds" available to "bribe more collaborators especially from the inside circles of opposition members" who would make their targets' devices accessible for direct infection. Seventy-three 'operatives' were involved. Ideally, Fungua Macho required 150 operatives – and much more money.

FinFisher was installed in the buildings of the ISO, ESO, Parliament[51] and also the two main agencies responsible for the operation – the UPF and CMI. Fungua Macho operatives targeted specific people. "People deemed dangerous to state security like government officials and opposition politicians are being surveilled", wrote Michael Bbosa, Director of Technical Intelligence in his 19th January 2012 operational update to the President. The update specifically named "all MPs and influential people involved in the Walk-to-Work Demos".

> **"Due to leakages from within the state apparatus, activity-spyware and gadgets targeting specific people have been deployed in the following institutions: CMI, ISO, ESO, Uganda Police and Parliament.**
>
> **We are also looking for people to use from within their own circles so as to access their gadgets."**
>
> 29 January 2012 Progress Report, Operation Fungua Macho

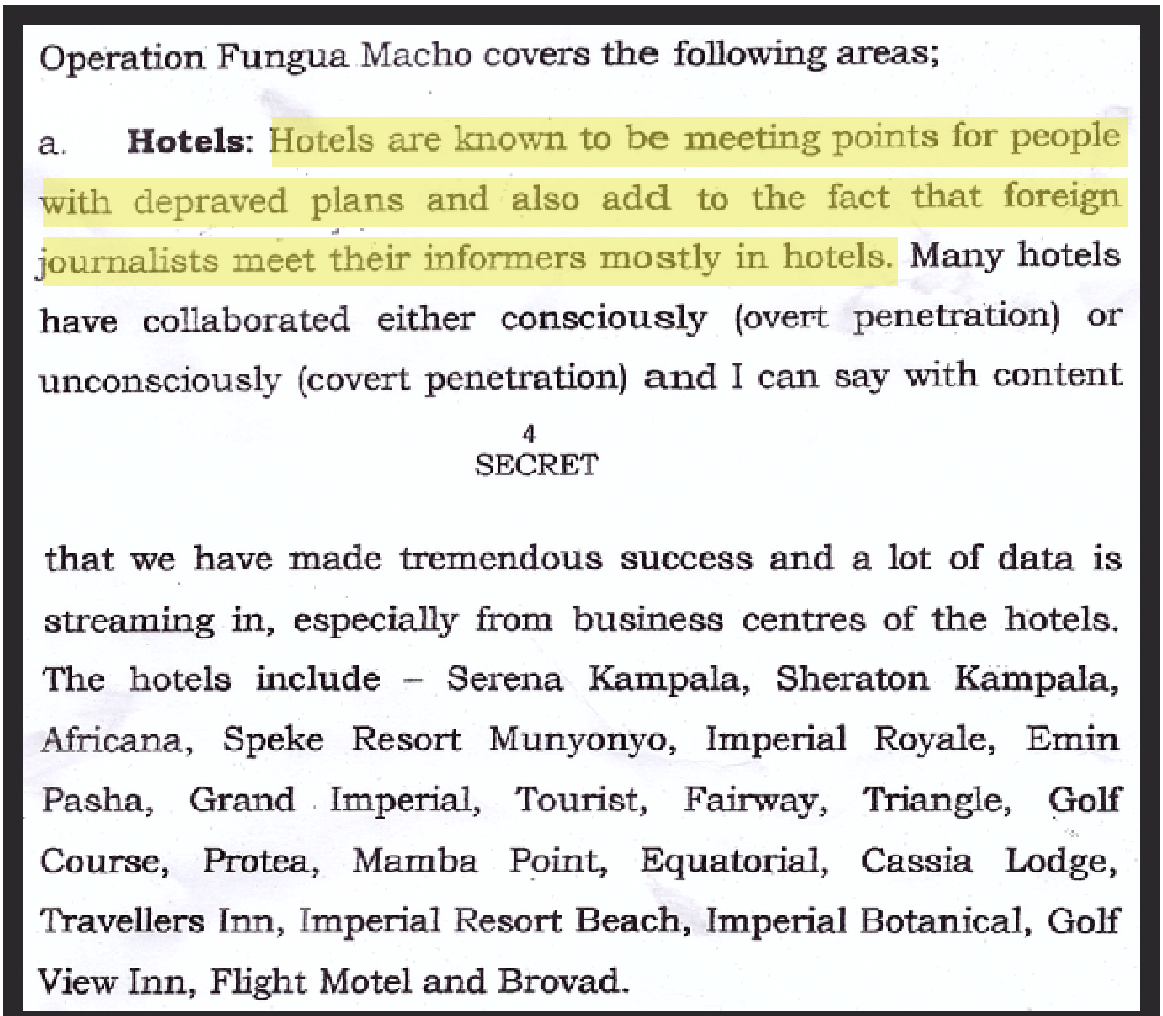
Hitting home – and hotels

Targets were not safe in their own homes. FinFisher fake access points were created in the Munyonyo neighbourhood and the leafy Kololo neighbourhood in central Kampala, as well as upmarket Lubowa and Kensington housing estates, according to the briefing document.

Furthermore, 21 mostly high-end hotels in Kampala, Entebbe and Masaka were compromised as part of the spying operation. These hotels were specifically selected because they were known to be meeting points for politicians and journalists as well as hosting political events.

Major political events in Kampala often occur at high end hotels. These include party conferences, heads of states meetings and industry meetings. FinFisher access points were installed on the Wi-Fi networks and/or business centres of these hotels. Security around the business centres is lax. Privacy International visited all 21 hotels in 2015 and found that computers in two-thirds did not protect administrator privileges, meaning that covert installation of a program onto the desktop computers would have been a simple task.

[51] At least one of the Parliamentary office buildings currently appears to have a system that monitors telecommunications signals inside the building and is capable of capturing phone identifying information.



Operation Fungua Macho covers the following areas;

a. **Hotels**: Hotels are known to be meeting points for people with depraved plans and also add to the fact that foreign journalists meet their informers mostly in hotels. Many hotels have collaborated either consciously (overt penetration) or unconsciously (covert penetration) and I can say with content

4

SECRET

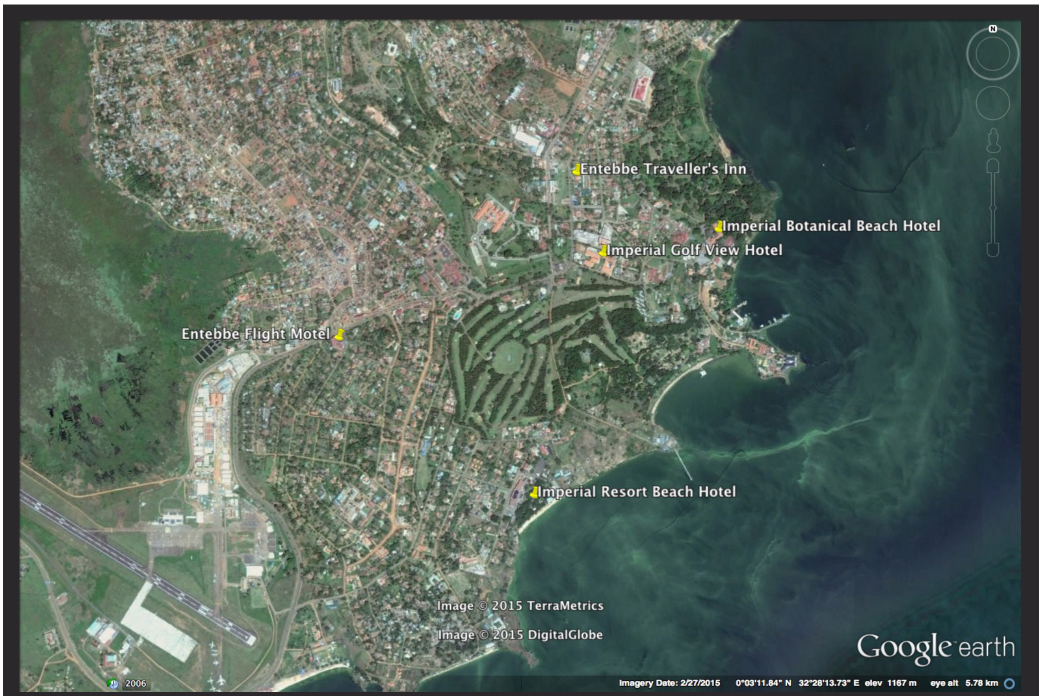
that we have made tremendous success and a lot of data is streaming in, especially from business centres of the hotels. The hotels include – Serena Kampala, Sheraton Kampala, Africana, Speke Resort Munyonyo, Imperial Royale, Emin Pasha, Grand Imperial, Tourist, Fairway, Triangle, Golf Course, Protea, Mamba Point, Equatorial, Cassia Lodge, Travellers Inn, Imperial Resort Beach, Imperial Botanical, Golf View Inn, Flight Motel and Brovad.

Operation Fungua Macho reveals government sensitivities over information leakage to foreign journalists. The CMI claims to have compromised 21 hotels through ‘overt’ and ‘covert’ means to address this threat. Responses from the hotels and estates mentioned are included as annexes. Source: Document obtained by Privacy International.

The management of a number of these hotels were aware of the installation, according to the Presidential briefing document. The potential collaboration of hotels with security services has serious implications. Guests and visitors pay expensive rates for physical security, comfort and privacy that these largely high-end establishments claim to offer. Responses from the establishments that chose to respond to Privacy International’s inquiries are included as an annex.

“Many hotels have collaborated either consciously (overt penetration) or unconsciously (covert penetration) … we have made tremendous success and a lot of data is streaming in.”

29 January 2012 Progress Report on Operation Fungua Macho


Entebbe Traveller's Inn
Imperial Botanical Beach Hotel
Imperial Golf View Hotel
Entebbe Flight Motel
Imperial Resort Beach Hotel
Image © 2015 TerraMetrics
Image © 2015 DigitalGlobe
Google earth
2006
Imagery Date: 2/27/2015 0°03'11.84" N 32°28'13.73" E elev 1167 m eye alt 5.78 km

Five hotels in Entebbe were equipped with FinFisher, according to the Presidential briefing document.

Men at (Cyber) Arms

The key players responsible for the execution of the Fungua Macho surveillance operation were security officials, several of whom answer directly to the President.

Yoweri Museveni: President of the Republic of Uganda

Yoweri Museveni is the current president of Uganda and will run for re-election in 2016. He enjoys a high degree of official and unofficial control of the intelligence services.[52] He personally launched the Fungua Macho surveillance operation by radio message from the State House in January 2012.

Museveni came to power in 1986 when the rebel National Resistance Army (NRA) he led ousted then-President Milton Obote and assumed control of the capital, Kampala. Museveni was elected in 1996, 2001, 2006 and again in 2011 after the NRM-dominated Parliament voted to remove term limits from the constitution.

Aronda Nyakairima: Former Chief of Defence Forces (UPDF), Minister of Internal Affairs (2013-2015)

A veteran of the 'Bush War' that brought the National Resistance Army and then-guerilla leader Yoweri Museveni to power, Aronda Nyakairima was appointed the Chief of Defence Forces (CDF) of the Ugandan military in 2005. As CDF, Nyakairima was responsible for sharing the data gathered using FinFisher under operation Fungua Macho with the Inspector General of the Police, Kale Kayihura, who jointly forwarded the information to the President.

Nyakairima was appointed Minister of Internal Affairs in 2013 and chaired the National Security Council.[53] He had spearheaded the National Security Information System[54] identity (ID) card project and the Registration of Persons Bill.[55] The bill requires Ugandans to present a national ID to any institution providing employment and financial services, among other

[52] For example, the 1987 Security Organisations Act states that actions taken on intelligence gathered must be sanctioned by the President or another authority directed by the President (Art 4), and the Office of the President officially.

[53] "Police can do better to protect Ugandans from killers – Aronda", Daily Monitor, 5 April 2015, http://www.monitor.co.ug/News/National/Police-can-do-better-to-protect-Ugandans-from-killers---Aronda/-/688334/2676308/-/2ylrirz/-/index.html

[54] "NSIS Mass Enrollment Strategy Launched," Ministry of Internal Affairs, November 2013, http://immigration.go.ug/media/nsis-mass-enrollment-strategy-launched

[55] Parliament passed the bill in February 2015.

Charles Bakahumura: Director of the Chieftaincy of Military Intelligence (CMI), UPDF

Charles Bakahumura has directed the Chieftaincy of Military Intelligence (CMI) of the UPDF since December 2011. Bakahumura regularly briefed President Museveni about the Fungua Macho operation.

Bakahumura is one of several Ugandan military officers, including the President's son, to have received military training in the UK. Bakahumura attended the Royal College of Defence Studies in the UK with a fellowship in 2010. He is reportedly involved in negotiations to facilitate the return of key political exiles in advance of the 2016 elections.[56]

Kale Kayihura: Inspector General of the Police (IGP), Uganda Police Force

Kale Kayihura was responsible for jointly forwarding the information gathered using FinFisher under the Fungua Macho operation to President Museveni.

A former military assistant of Museveni during the 'Bush War', Kayihura is widely seen as unfailingly loyal to his boss. Kayihura gained notoriety during the 2011 presidential election and the Walk to Work protests because of his brutality in crushing the protest movement.

Kayihura presides over the Joint Intelligence Committee. The JIC assembles the ISO, ESO, CMI and Police. Kayihura is heavily involved in defence procurement, and has been implicated in corruption scandals. He reportedly failed to account for UGX 15 billion (US$ 4 million) while commander of the Special Revenue Protection Services between 2001 and 2006.[57]

Amos Ngabirano: Head of the Police Directorate of Information and Communication Technology

Amos Ngabirano has headed the Police Directorate of Information and Communication Technology (ICT) since 2010. Its role is to plan, develop and advise the UPF on the implementation of ICT policies.

Ngabirano provided technical guidance on the procurement of FinFisher. He travelled to Germany and the Czech Republic in 2012 with Oluka, Bbosa and Rwantale. As a guest of Gamma International GmbH in Munich, the officials attended demonstrations of surveillance products from Gamma

[56] "CMI chief convinced me to return – Kyakabale", Daily Monitor, 23 March 2015, http://www.monitor.co.ug/News/National/CMI-chief-convinced-me-to-return---Kyakabale/-/688334/2662390/-/by788az/-/index.html

[57] "IGP Kayihura faces probe over SRPS' Shs 15bn", The Independent, 22 April 2009, http://www.independent.co.ug/column/insight/832-igp-kayihura-faces-probe-over-srps-shs-15bn

partner companies Trovicor (Germany), Utimaco (Germany), Polaris (US), Cobham (UK) and 1rstWAP (Indonesia). The four later attended the ISS World surveillance technology trade show in Prague with travel arrangements and hotels arranged by Gamma International GmbH.

Ngabirano travels internationally with IGP Kale Kayihura to procure policing and surveillance technology and receive training. He travelled to Colombia in 2013 to attend an Interpol training course with Kayihura and another colleague[58] and also travelled with IGP Kayihura to Italy in 2011 to visit a defence technology firm.[59]

Michael Bbosa: Director of Military Intelligence (2012), UPDF

Bbosa was Director of Technical Intelligence at the Chieftaincy of Military Intelligence (CMI) of the UPDF in 2012. He was responsible for preparing briefings regarding the Fungua Macho surveillance operation for his boss, Charles Bakahumura, to deliver to the President. He is currently Director of IT in the UPDF.

Bbosa travelled to Germany and the Czech Republic in 2012 with Oluka, Ngabirano and Rwantale. As guests of Gamma International GmbH in Munich, the officials attended demonstrations of surveillance products from Gamma partner companies Trovicor (Germany), Utimaco (Germany), Polaris (US), Cobham (UK) and 1rstWAP (Indonesia). The four later attended the ISS World surveillance technology trade show in Prague with travel arrangements and hotels arranged by Gamma International GmbH.

Bbosa has been central to security equipment procurement. In 2007 he was a member of the Security Technical Team responsible for procuring communications equipment for the Commonwealth Heads of Government Meeting (CHOGM). He reportedly commands a significant budget for surveillance.[60]

Charles Oluka: UPDF Captain

Oluka is a captain of the Ugandan army who is involved in defence technology procurement. Oluka chaired the contracts committee of the Internal Security Organisation (ISO) in 2008 and was attached to the Office of the President in 2011.

[58] “Bettering the Force”, The Investigator, 22 October 2013, http://investigator.co.ug/local/item/12282-bettering-the-force.html

[59] “The Uganda Police Force at the Rome Headquarters of Vitrociset”, Vitrociset, 11 July 2011, http://www.vitrociset.it/dett_editoriale.php?id_editoriale=182&lang=en

[60] The Red Pepper, 6 April 2015, held by Privacy International.

Oluka travelled to Germany and the Czech Republic in 2012 with Bbosa, Ngabirano and Rwantale. As guests of Gamma International GmbH in Munich, the officials attended demonstrations of surveillance products from Gamma partner companies. The four later attended the ISS World surveillance technology trade show in Prague with travel arrangements and hotels arranged by Gamma International GmbH. Oluka made arrangements to travel to 'Defense Days', a military technology event in Paris in February 2011 and a technology 'bootcamp' in Berlin in October 2011 as a guest of surveillance company Advanced German Technology (AGT).[61]

Nelson Rwantale: Engineer

Rwantale is an engineer for the Government of Uganda. Rwantale accompanied his colleagues Ngabirano, Bbosa and Oluka to Europe in 2012. In Munich, the officials attended demonstrations of surveillance products from Gamma's partner companies. The four later attended the ISS World surveillance technology trade show in Prague.

Stephan Oelkers: General Manager at Gamma International GmbH

Stephan Oelkers was the General Manager of Gamma International GmbH, based in Germany, when he visited Uganda in early 2012.

On 19th and 20th January 2012, Oelkers and his colleague Alexander Hagenah met Government officials in Uganda where they presented a FinFisher IT Intrusion Seminar. Oelkers was also the contact for the four Ugandan officials during their 2012 visit to Germany and the Czech Republic. Oelkers returned to Uganda throughout 2013.[62]

Stephan Oelkers is at the centre of Gamma/FinFisher's international network. He is Managing Director of FinFisher GmbH, CEO of FinFisher Labs GmbH, Managing Director of FinFisher Holding GmbH and was CEO of Gamma International Holding GmbH in mid-2013 – all based in Munich, Germany.

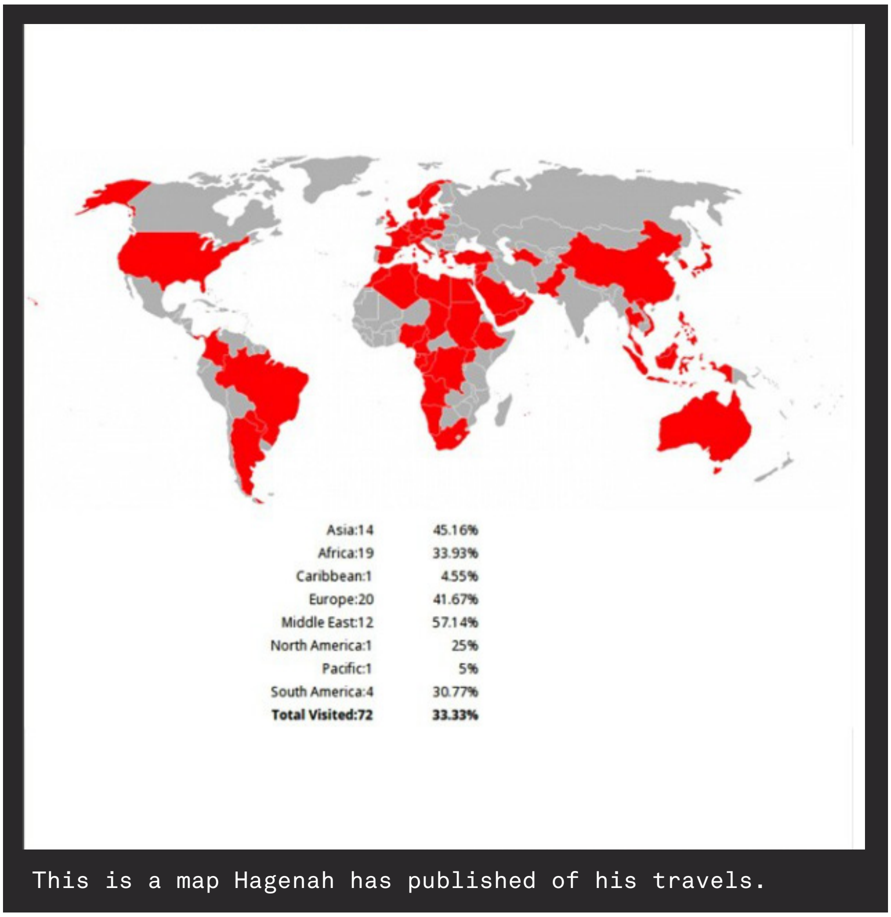
[61] Oluka self-identified as "Mr. Oluka Charles, Director of Technical Support Services, Government of the Republic of Uganda". Documents obtained by PI.

[62] According to the Wikileaks Counterintelligence Unit, September 2013, https://wikileaks.org/spyfiles3map.html

Alexander Hagenah: Senior Security Specialist at Gamma International GmbH (2012)

Alexander Hagenah was a senior security specialist at Gamma International GmbH in 2012. In January 2012 he travelled to Uganda with Gamma colleague Stephan Oelkers to present the capabilities of the FinFisher package.

Hagenah was responsible for fixing technical problems for FinFisher clients worldwide. Hagenah previously worked for other defence technology companies including Advanced German Technology (AGT), a Dubai-based surveillance technology reseller with a shell office in Germany, according to information obtained by Privacy International. Hagenah is currently a senior security specialist and consultant for law enforcement and intelligence agencies globally based in Dubai, United Arab Emirates. As part of his job, he has travelled extensively in Africa, including to Equatorial Guinea and Ethiopia.



Asia:14	45.16%
Africa:19	33.93%
Caribbean:1	4.55%
Europe:20	41.67%
Middle East:12	57.14%
North America:1	25%
Pacific:1	5%
South America:4	30.77%
Total Visited:72	**33.33%**

This is a map Hagenah has published of his travels.

Systematising Surveillance

By mid-2012, Walk to Work had lost its momentum and much of its popular support, though its leadership, which included many prominent opposition MPs, were still vocal.[63]

Uganda is now preparing for a new round of presidential and parliamentary elections in 2016. The Police has been breaking up 'illegal' meetings of Presidential candidates, including of former Minister of Security Amama Mbabazi. The Police is reportedly aiming to deploy two million plain-clothed agents nationwide to conduct counter-espionage and political intelligence under the newly-established Directorate of Intelligence.[64] The Government continues to use excessive force to police assemblies. Two journalists were beaten as they covered a protest march against unemployment in January 2015.[65] Journalists and activists describe a climate of fear and self-censorship as the election approaches.

Communications monitoring centre

The Ugandan Government is also currently in the advanced stages of procuring the central communications monitoring centre that was mandated five years ago by the Regulation of Interception of Communications Act.

The monitoring centre project was conceived as a 'Public Safety Network Project' along with a CCTV surveillance network and National Emergency Call Centre. In early 2013, the inter-agency Joint Security/ICT Technical Committee of the National Security Council invited seven international surveillance technology companies to "make presentations on their solutions", according to a confidential brief to President Museveni obtained by Privacy International, which is included as an annex. These companies included: Verint Systems Ltd. and NICE Systems (Israel); Gamma Group International (UK); ZTE and Huawei (China); Macro System (Poland); and Resi Group (Italy).

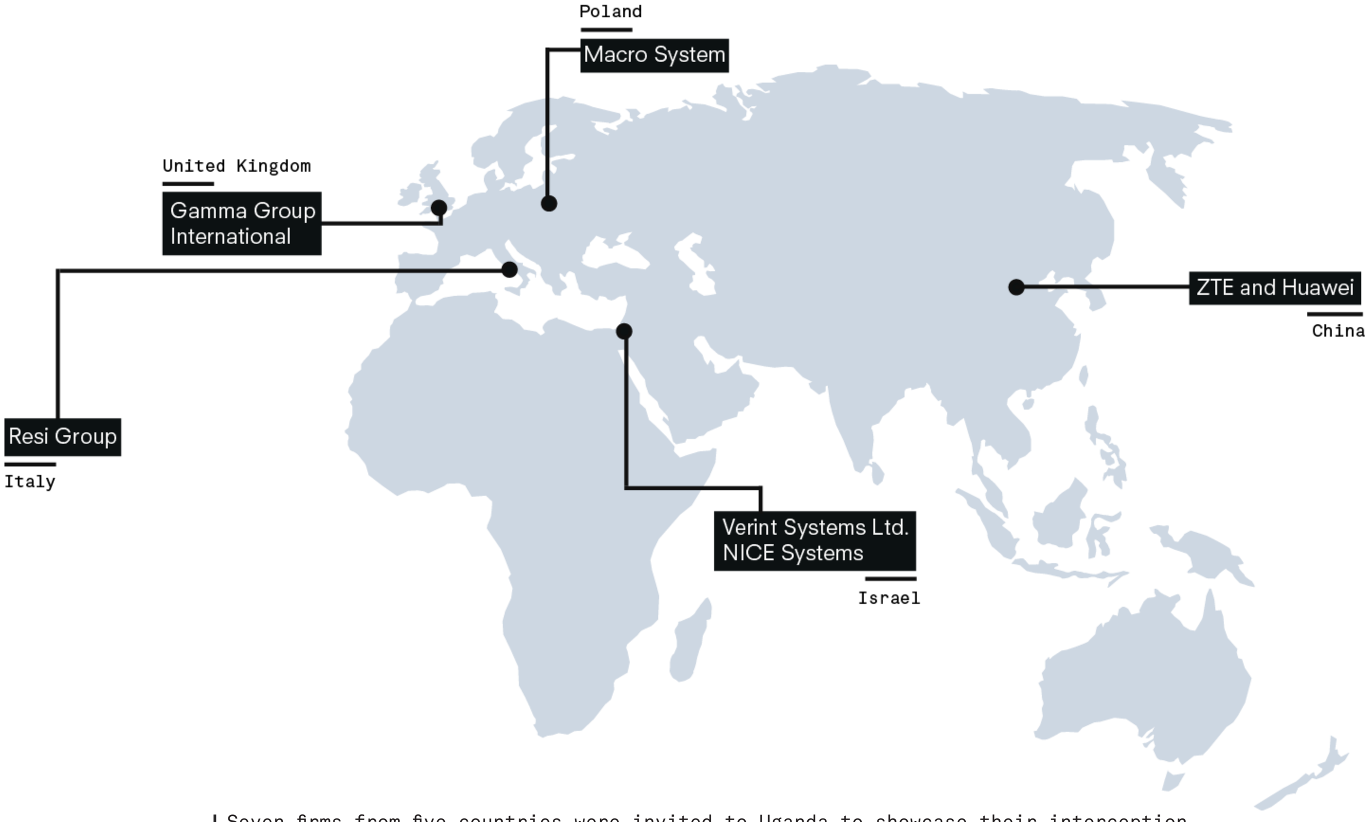
[63] Several had been called in for extensive questioning. "A4C National coordinator Summoned by Special Investigations Unit", Activists for Change, 16 April 2012, http://activists4change.blogspot.co.uk/2012/04/a4c-national-coordinator-summoned-by.html

[64] "Kale Kayihura, Museveni's master spy at work", Africa Intelligence, 13 February 2015, http://www.africaintelligence.com/ION/politics-power/2015/02/13/kale-kayihura-museveni's-master-spy-at-work,108061417-ART?CXT=CANP&country=UGANDA

[65] See for example, "Fears of growing Ugandan police brutality as election looms", Deutsche Welle, 4 March 2015, http://www.dw.com/en/fears-of-growing-ugandan-police-brutality-as-election-looms/a-18290695 and "HRNJ-Uganda alert, another witness pins senior police officer of journalist assault", Human Rights Network for Journalists-Uganda, 14 May 2015, https://hrnjuganda.wordpress.com/2015/05/14/hrnj-uganda-alert-another-witness-pins-senior-police-officer-a-journalist-assault/

Yet the budget for the monitoring centre project was slow to materialise. In 2014, the Office of Security Coordination requested UGX 200 billion (approximately US$ 80 million) to fund it.[66] This request has not been formally granted to date, according to Parliamentary records. Sources differ as to whether the money has been made available for the purchase or already spent.

Procurement was proceeding in 2015. Yet which company, if any, has been contracted for the project is unclear. NICE Systems was one of the frontrunners for the monitoring centre project, according to internal emails of surveillance technology company Hacking Team. In April 2015, a NICE Vice President contacted colleagues at Italian malware company Hacking Team regarding a "new opportunity" it had been negotiating with the Office of the President.[67] NICE expected the evaluation process for the tenders for the "integrated intelligence solution" to be completed in mid-May 2015.



Seven firms from five countries were invited to Uganda to showcase their interception solutions in 2013. Source: Briefing memo obtained by Privacy International

[66] "Budget Framework Paper, Vote:001 Office of the President, 2014-2015."

[67] "RE: [Warning: This mail can include a virus/worm] RE: New opportunity – Uganda", email from NICE to Hacking Team, 8 May 2015, https://wikileaks.org/hackingteam/emails/emailid/431692

Delays and problems

At the time of writing, the monitoring centre project is not operational. It has been delayed in part because service providers have contested Government orders that they pay to connect to the future system, according to sources in the technology industry. The Regulation of Interception of Communications Act requires service providers to foot the bill of connecting to the new centre or otherwise complying with the Act, a considerable cost.[68]

One telecoms expert remembers that his company received a letter in 2011 requesting that it fund the cost of the company's compliance with the Act. Companies stalled, claiming it was not in their budget to do so. "The willingness is not there," he said. "The telecommunications sector is driving the economy, it's very lucrative. They have sunk huge investments into the sector".

The Uganda Communications Commission (UCC), the national telecommunications regulatory body, has reportedly been reluctant to force these service providers to comply. The UCC receives 2-2.5% of service providers' gross annual revenue and they are a major source of the UCC's funding.[69]

Without support from the service providers, it would be difficult to implement such an expensive project – estimated by experts to cost far more than the UGX 200 billion (US$ 80 million) requested in 2014. The monitoring centre project is an expensive and technically complex one. It is unclear whether the Government will be able to implement the project along their stated timeline, in advance of next year's presidential election.

Hacking Team and the Business Mogul

The Government has been looking to purchase intrusion malware in parallel to the monitoring centre project. In early May 2015, the Ugandan Police was considering an offer from Hacking Team. Hacking Team is an Italian company and rival to Gamma that also sells an intrusion malware suite. Ugandan officials had shown interest in the Remote Control System (RCS) since 2011.

Hacking Team was eager to showcase their products to Ugandan Government officials at the ISS World surveillance trade show in late July 2015 in South Africa – but the Ugandans were not forthcoming. By late June the deal

[68] Art 11(4), Regulation of Interception of Communications Act (2010).

[69] The UCC has previously attempted to force service providers' compliance with unpopular government directives with mixed success. In April 2011, during the Walk to Work protests, the UCC wrote to internet service providers to request that they block access to social media sites including Facebook and Twitter. Major networks refused to comply and the UCC retracted its demand claiming it had been sent out in error.

appeared to have stalled. "I contacted them, but they have not responded yet," said Zakiruddin Chowdury of Sraban BD, a technology consultancy company based in Bangladesh, who was liaising between Hacking Team and their potential Ugandan client.[70]

"Can you please provide more information and details, specifically in how your product matches up to Gamma products (specifically FinFisher)... We have been operating here [Uganda] for law enforcement and Security Agencies since 2007.

We also successfully deployed active LE equipment for law enforcement here... We are due to present proposals for the next CapEx [capital expenditure] round for product acquisition in 10 days and would appreciate if you could forward more details as requested above."

"Peter" of Ugandan IT firm IT Doc24 Ltd, to Hacking Team CEO David Vincenzetti, 2 December 2011.[70]

Negotiations over surveillance projects are likely to remain close to the President's inner circle. The local contact for the Hacking Team potential deal was Kin Kariisa, a business executive considered among Museveni's close contacts, according to documentation obtained by Privacy International and included as an annex. Kariisa was the President's special advisor on ICT from 2000 to 2009.

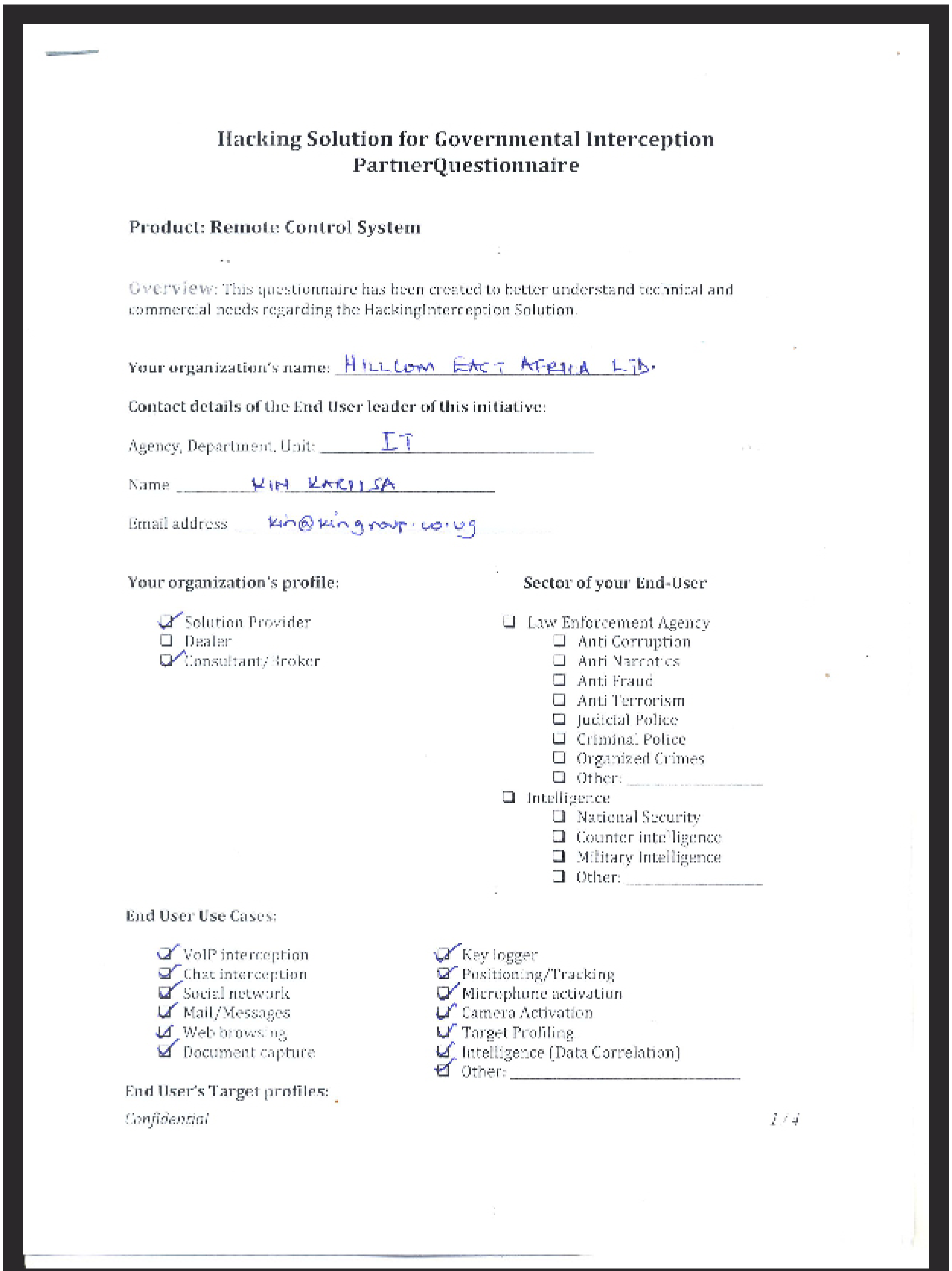
Kariisa has also been the Chairman of NBS Television Limited from 2007 and Vice Chairman of the National Association of Broadcasters since 2011. He is also Executive Chairman of Kin Group Ltd, the holding company that owns the companies including NBS Television Ltd and Director of the Ugandan branch of Ecobank, a major African bank. Kariisa was listed as the 'end user leader' of the Hacking Team procurement initiative through Hillcom East Africa Limited ('Hillcom'). Hillcom was incorporated in May 2010 as a company to "deal in supply of broadcasting equipment" and other audiovisual and data recording equipment. It has been approached by international companies seeking to tender lawful interception projects in Uganda. It is majority owned by Kin Kariisa, also its sole signatory on its Ecobank account. Kin Group's Legal Officer was also liaising on behalf of the Uganda Police Force on the Hacking Team project. Kin Group's response is included as an annex.

"Unofficially my local contact promised to get required budget allocation for this [Hacking Team's RCS intrusion malware suite]."

Zakiruddin Chowdury, consultant at Sraban BD, email to Hacking Team, 18 May 2015

[70] "Re: Re: Re: R: I: Uganda Police", email from Sraban BD to Hacking Team, 30 June 2015 https://wikileaks.org/hackingteam/emails/emailid/1081608

> **"I would be very careful with this one. there are all the dangerous signs, and given that they seem to want confidential information, maybe behind there is Gamma"**
>
> Hacking Team CEO David Vincenzetti, email to colleagues, 2 December 2011. The Chieftaincy of Military Intelligence procured Gamma's FinFisher spyware three days later.



Hacking Solution for Governmental Interception
PartnerQuestionnaire

Product: Remote Control System

Overview: This questionnaire has been created to better understand technical and commercial needs regarding the HackingInterception Solution.

Your organization's name: HILLCOM EAST AFRICA LTD.

Contact details of the End User leader of this initiative:

Agency, Department, Unit: IT

Name KIM KARIISA

Email address kim@kingroup.co.ug

Your organization's profile:

- ☑ Solution Provider
- □ Dealer
- ☑ Consultant/Broker

Sector of your End-User

- □ Law Enforcement Agency
  - □ Anti Corruption
  - □ Anti Narcotics
  - □ Anti Fraud
  - □ Anti Terrorism
  - □ Judicial Police
  - □ Criminal Police
  - □ Organized Crimes
  - □ Other: ____________
- □ Intelligence
  - □ National Security
  - □ Counter intelligence
  - □ Military Intelligence
  - □ Other: ____________

End User Use Cases:

- ☑ VoIP interception
- ☑ Chat interception
- ☑ Social network
- ☑ Mail/Messages
- ☑ Web browsing
- ☑ Document capture
- ☑ Key logger
- ☑ Positioning/Tracking
- ☑ Microphone activation
- ☑ Camera Activation
- ☑ Target Profiling
- ☑ Intelligence (Data Correlation)
- ☑ Other: ____________

End User's Target profiles:

Confidential 1 / 4

The local contact questionnaire submitted to Hacking Team shows the Ugandan government's broad ambitions to target various forms of communication. Source: Document obtained by Privacy International from data publicly available.

Surveillance culture

State authorities have proactively cultivated the popular perception that surveillance is systematic, centralised and technically sophisticated. This is not the case; not yet, at least.

The attributes that have made Uganda's human intelligence network strong and allowed it to infiltrate opposition and other circles considered threatening to the Government are poorly suited to conducting communications surveillance on a large and automated scale. Poor levels of technical training, low pay and a culture of bribe-taking has alienated the few educated and technically competent engineers that would be required to operate a nationwide surveillance system beyond monitoring a relatively small number of high-value targets, according to industry and Government sources.

Despite procuring advanced hacking technology, the Ugandan police and intelligence agencies' forensic skills remain rudimentary, according to industry insiders. Photo: Privacy International, 2015

"The way that they get it [communications data] is basically by walking in to an engineering centre with the Police," said one industry source. "They get a headset and listen to it live." The Government has also reportedly placed agents within the telecommunications switching centres, but their skills vary and assignments are relatively simple – for example, the generation of call and contact lists, the location of callers using cell tower data, and audio recordings of specific lines based on human intelligence.[71]

Police and CMI officials can also obtain call data by presenting formal requests, or by requesting print-outs of call data. These requests are often fabricated and the process is often abused. Journalists with whom Privacy International spoke discussed how plainclothes CMI agents would present them with call records as a warning when working on sensitive stories. CMI agents can also be enlisted – for a fee – to track down stolen phones using location data.

In recent years the security services have invested heavily in cyber defence. In 2013, a new forensic lab for the analysis of computer crime was opened in Kampala[72] and the UCC launched a Computer Emergency Response Team to investigate cyber crimes.[73] In 2014, the UCC opened a media monitoring centre with "digital logger surveillance equipment",[74] though it appears to be targeted at recording and analysing public radio, television and print media rather than private communications. Police have also signed an accord with the UCC to cooperate more closely on the investigation of cyber crimes.

Despite these developments, the Police's ability to actually conduct forensic analysis on devices and trace cybercrimes is rudimentary.

The Police acquired tools to conduct advanced cyber forensic investigations in the past two to three years, but, according to one industry expert, the "Police force still do not have the skillset. They have some tools and training, doing incident reporting and the like, but moving towards expertise and analysis is difficult".

The Police and investigating agencies often turn to private forensic companies to assist in complex investigations. "Really good programmers know how

[71] Nevertheless, elite cadres perceived as loyal to the ruling party are sent abroad to train on surveillance techniques, including, as this report has shown, surveillance technology like FinFisher.

[72] "Forensics lab for computer crime opened in Kampala", Daily Monitor, 11 March 2013, http://www.monitor.co.ug/News/National/Forensics-lab-for-computer-crime-opened-in-Kampala/-/688334/1716526/-/1590cm1z/-/index.html

[73] "UCC launches response team to curb cyber crime", The Observer, 12 June 2013, http://www.observer.ug/business/38-business/25817-ucc-launches-response-team-to-curb-cyber-crime

[74] "Report facts only, Kayihura tells journalists," The Observer, 11 January 2015, http://www.observer.ug/index.php?option=com_content&view=article&id=35887:report-facts-only-kayihura-tells-journalists&catid=34:news&Itemid=114

much people are making from app[lication] development. Unless you're going to throw real money at it, they're not going to do it [work for the police]", said another industry expert. "The police and political leadership generally have no appreciation of the technology, so they undervalue it. They don't hire guys with the skills".[75] Instead, loyalty is prized over technical competence. While such patronage networks are useful when it comes to human intelligence, they are counter-productive when carrying out complicated projects that require engineers with strong technical skills.

[75] Even employing private companies for forensic analysis has not addressed the Police's forensic investigation needs. The government has failed on a number of occasions to uncover the identity or identities of 'Tom Voltaire Okwalinga' aka 'TVO', a Facebook personality and government critic. During the most recent arrest of a suspected TVO – cybersecurity expert and US Embassy employee Robert Shaka – TVO continued to post critical comments to its Facebook page while its supposed author was in custody. Police were also unable to break the encryption on Shaka's seized devices.

Conclusion

Ugandan intelligence and law enforcement authorities use technically sophisticated methods like intrusion malware to conduct targeted communications surveillance of political opponents; as well as simple methods, like extracting call data without warrants from service providers.

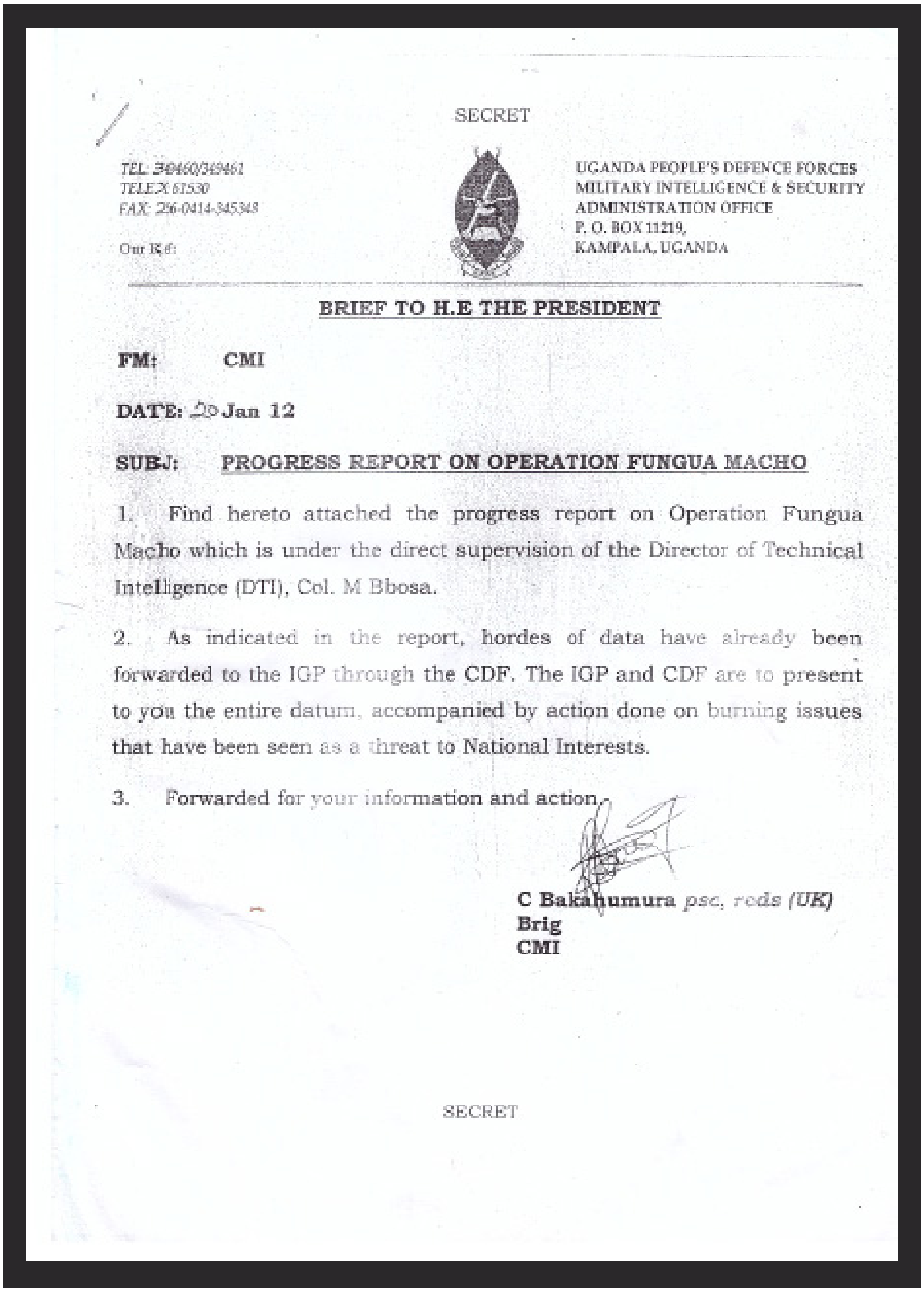
Surveillance operations involving high-level targets are coordinated directly through the Office of the President and involve people perceived as loyal to the President. Surveillance activities for lower-level threats and general control of the media, activists and personal score-settling are haphazard, but no less dangerous for their targets.

In part by using FinFisher spyware, the Ugandan Government under President Museveni's direction dismantled the post-election protest movement.

Along with more heavy-handed tactics, the use of surveillance technology has chilled free speech and legitimate expressions of political dissent. Covert, extrajudicial surveillance projects like those documented in this report have contributed towards making Uganda a less open and democratic country in the name of national security. This situation is unlikely to improve any time soon, particularly with the eventual addition of the centralised communications monitoring centre under the intelligence services' control.

Until and unless this is addressed, claims that Uganda is a burgeoning democracy ring hollow.

Annex 1: Brief to President Museveni on Operation Fungua Macho, 20 January 2012



SECRET

TEL: 349460/349461
TELEX 61530
FAX: 256-0414-345348

Our Ref:

UGANDA PEOPLE'S DEFENCE FORCES
MILITARY INTELLIGENCE & SECURITY
ADMINISTRATION OFFICE
P. O. BOX 11219,
KAMPALA, UGANDA

BRIEF TO H.E THE PRESIDENT

FM: CMI

DATE: 20 Jan 12

SUBJ: PROGRESS REPORT ON OPERATION FUNGUA MACHO

1. Find hereto attached the progress report on Operation Fungua Macho which is under the direct supervision of the Director of Technical Intelligence (DTI), Col. M Bbosa.

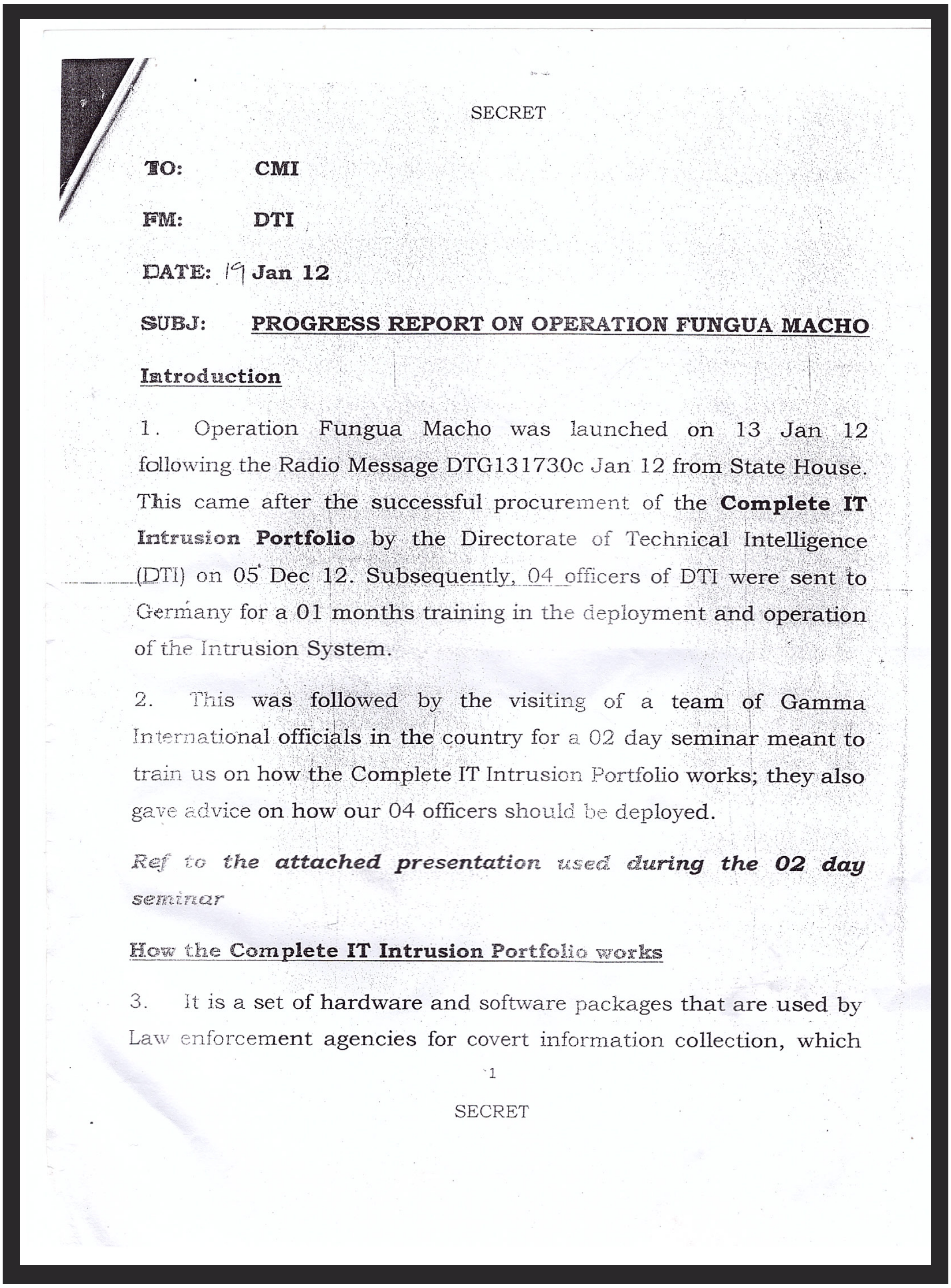
2. As indicated in the report, hordes of data have already been forwarded to the IGP through the CDF. The IGP and CDF are to present to you the entire datum, accompanied by action done on burning issues that have been seen as a threat to National Interests.

3. Forwarded for your information and action.

C Bakahumura *psc, rcds (UK)*
Brig
CMI

SECRET

Annex 1: Brief to President Museveni on Operation Fungua Macho, 20 January 2012



SECRET

TO: **CMI**

FM: **DTI**

DATE: 19 **Jan 12**

SUBJ: **PROGRESS REPORT ON OPERATION FUNGUA MACHO**

Introduction

1. Operation Fungua Macho was launched on 13 Jan 12 following the Radio Message DTG131730c Jan 12 from State House. This came after the successful procurement of the **Complete IT Intrusion Portfolio** by the Directorate of Technical Intelligence (DTI) on 05 Dec 12. Subsequently, 04 officers of DTI were sent to Germany for a 01 months training in the deployment and operation of the Intrusion System.

2. This was followed by the visiting of a team of Gamma International officials in the country for a 02 day seminar meant to train us on how the Complete IT Intrusion Portfolio works; they also gave advice on how our 04 officers should be deployed.

Ref to the attached presentation used during the 02 day seminar

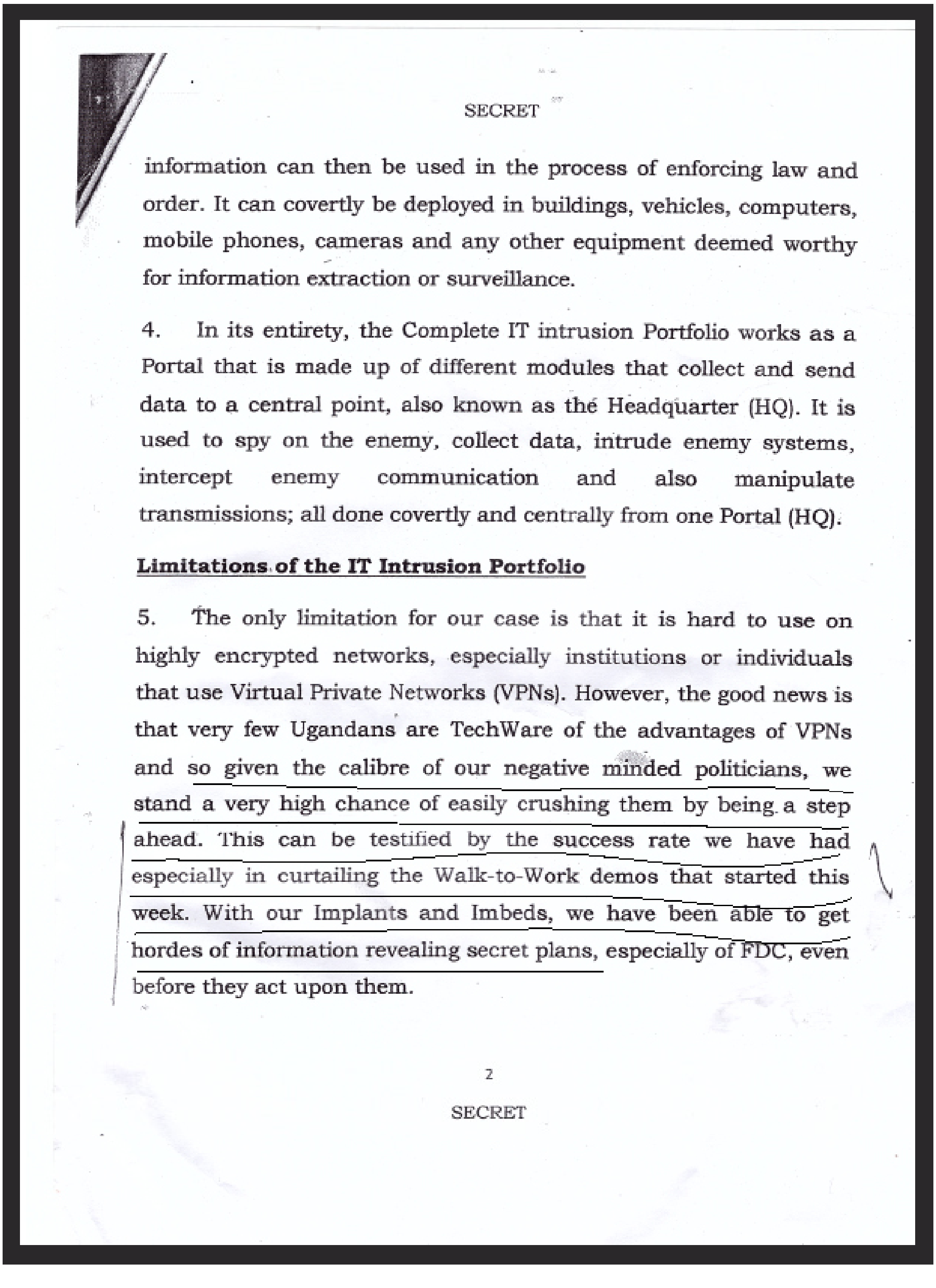
How the Complete IT Intrusion Portfolio works

3. It is a set of hardware and software packages that are used by Law enforcement agencies for covert information collection, which

1

SECRET

Annex 1: Brief to President Museveni on Operation Fungua Macho, 20 January 2012



SECRET

information can then be used in the process of enforcing law and order. It can covertly be deployed in buildings, vehicles, computers, mobile phones, cameras and any other equipment deemed worthy for information extraction or surveillance.

4. In its entirety, the Complete IT intrusion Portfolio works as a Portal that is made up of different modules that collect and send data to a central point, also known as the Headquarter (HQ). It is used to spy on the enemy, collect data, intrude enemy systems, intercept enemy communication and also manipulate transmissions; all done covertly and centrally from one Portal (HQ).

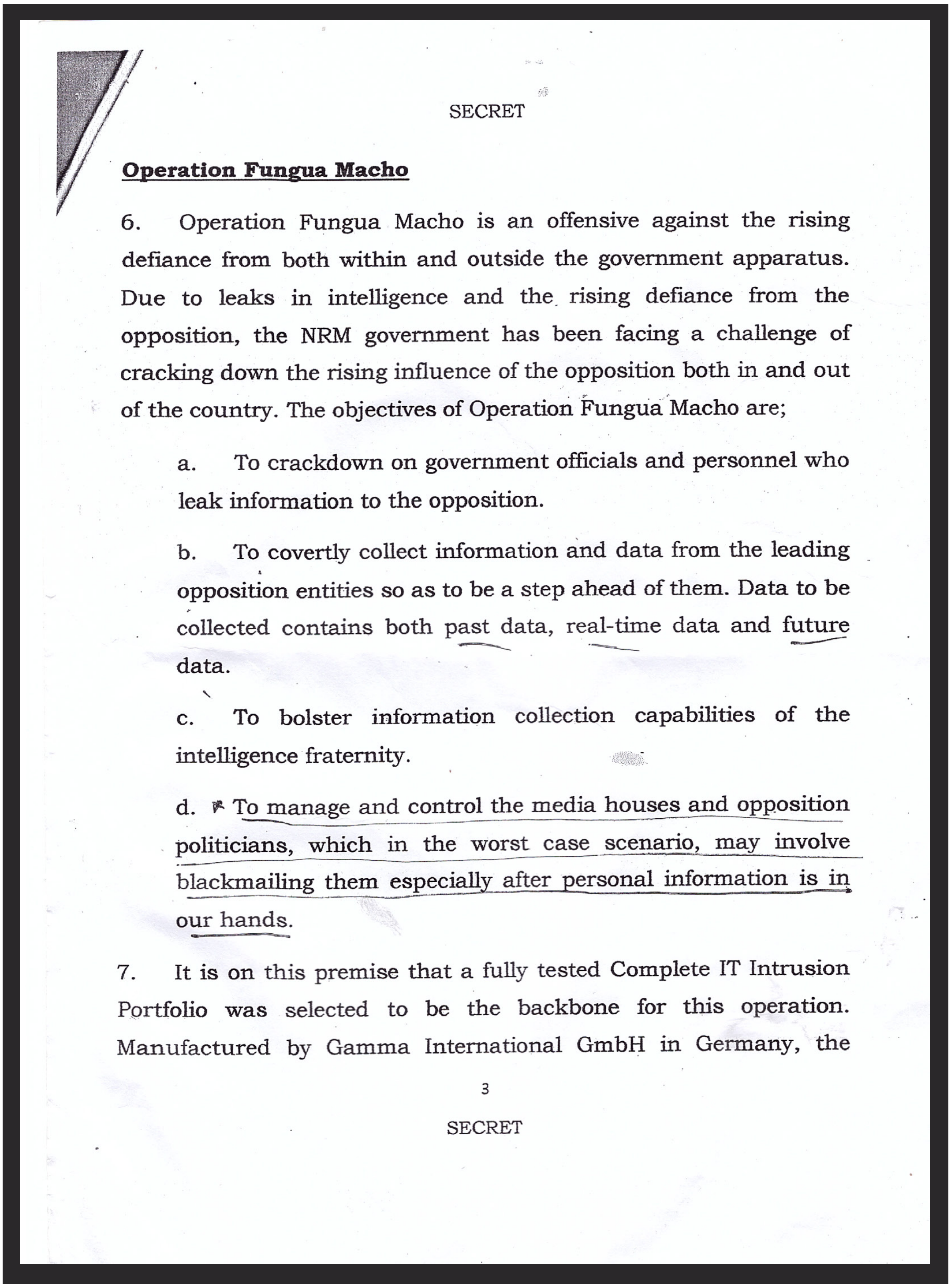
Limitations of the IT Intrusion Portfolio

5. The only limitation for our case is that it is hard to use on highly encrypted networks, especially institutions or individuals that use Virtual Private Networks (VPNs). However, the good news is that very few Ugandans are TechWare of the advantages of VPNs and so given the calibre of our negative minded politicians, we stand a very high chance of easily crushing them by being a step ahead. This can be testified by the success rate we have had especially in curtailing the Walk-to-Work demos that started this week. With our Implants and Imbeds, we have been able to get hordes of information revealing secret plans, especially of FDC, even before they act upon them.

2

SECRET

Annex 1: Brief to President Museveni on Operation Fungua Macho, 20 January 2012



SECRET

Operation Fungua Macho

6. Operation Fungua Macho is an offensive against the rising defiance from both within and outside the government apparatus. Due to leaks in intelligence and the rising defiance from the opposition, the NRM government has been facing a challenge of cracking down the rising influence of the opposition both in and out of the country. The objectives of Operation Fungua Macho are;

a. To crackdown on government officials and personnel who leak information to the opposition.

b. To covertly collect information and data from the leading opposition entities so as to be a step ahead of them. Data to be collected contains both past data, real-time data and future data.

c. To bolster information collection capabilities of the intelligence fraternity.

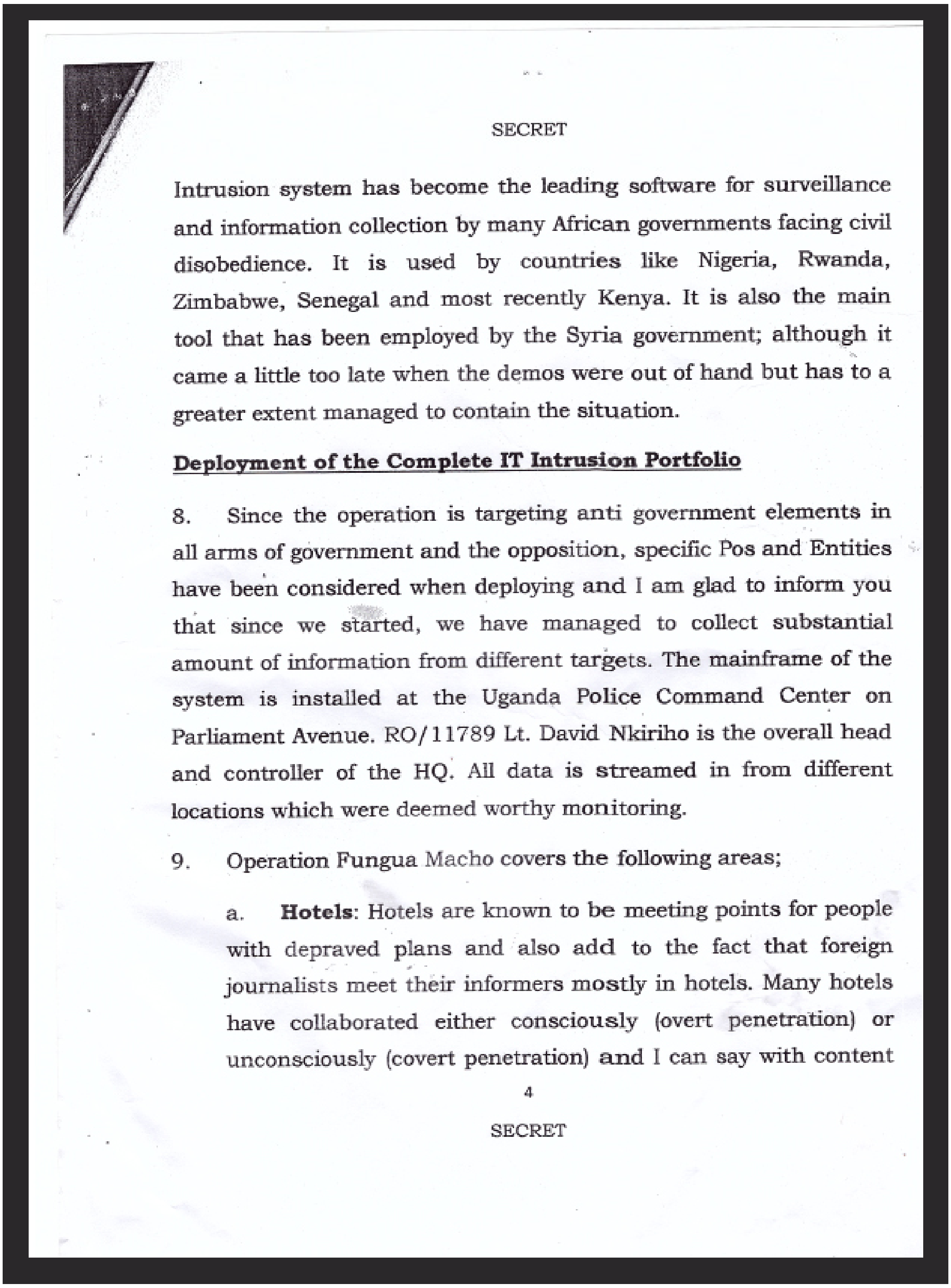
d. To manage and control the media houses and opposition politicians, which in the worst case scenario, may involve blackmailing them especially after personal information is in our hands.

7. It is on this premise that a fully tested Complete IT Intrusion Portfolio was selected to be the backbone for this operation. Manufactured by Gamma International GmbH in Germany, the

3

SECRET

Annex 1: Brief to President Museveni on Operation Fungua Macho, 20 January 2012



Intrusion system has become the leading software for surveillance and information collection by many African governments facing civil disobedience. It is used by countries like Nigeria, Rwanda, Zimbabwe, Senegal and most recently Kenya. It is also the main tool that has been employed by the Syria government; although it came a little too late when the demos were out of hand but has to a greater extent managed to contain the situation.

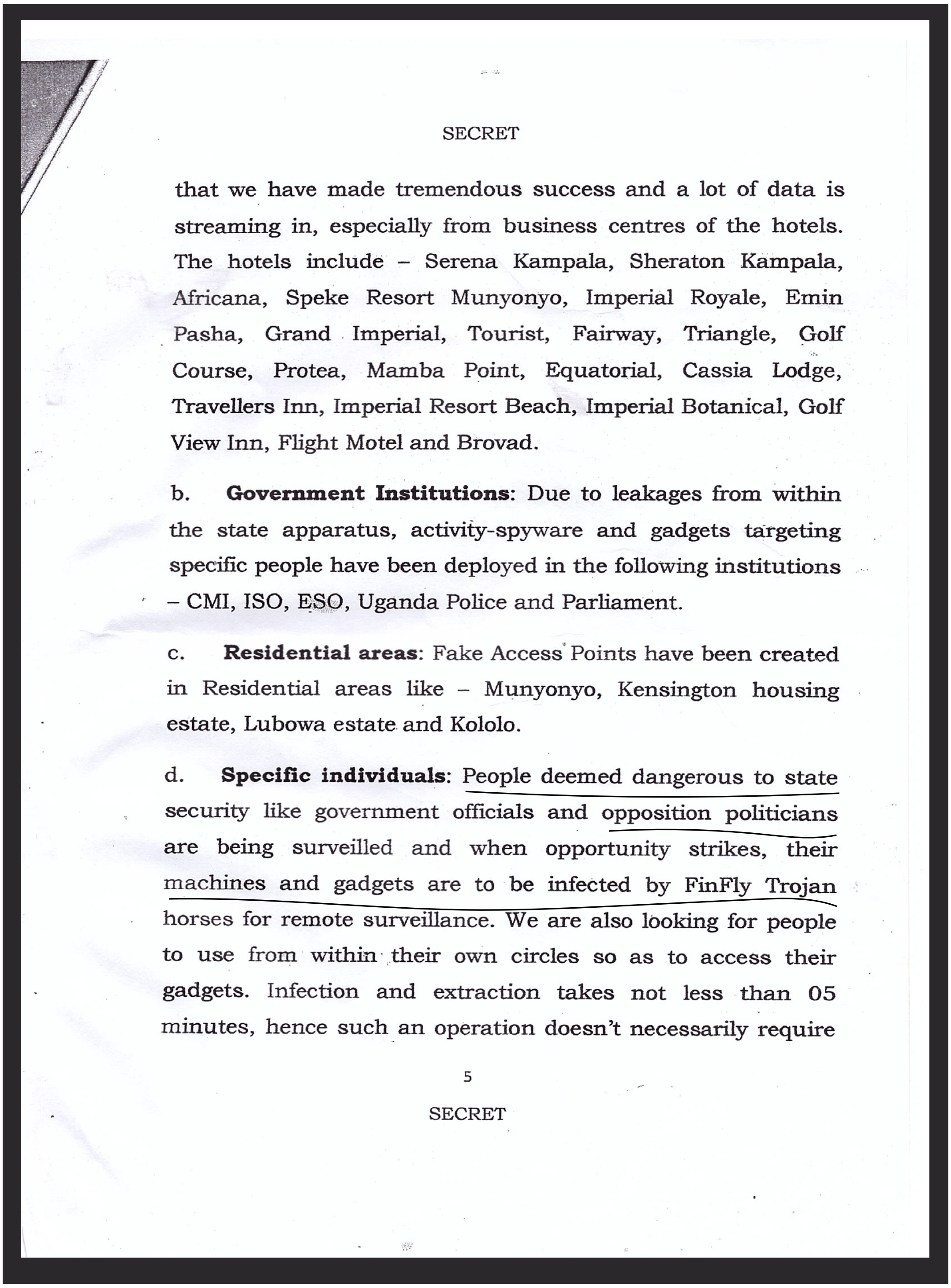
Deployment of the Complete IT Intrusion Portfolio

8. Since the operation is targeting anti government elements in all arms of government and the opposition, specific Pos and Entities have been considered when deploying and I am glad to inform you that since we started, we have managed to collect substantial amount of information from different targets. The mainframe of the system is installed at the Uganda Police Command Center on Parliament Avenue. RO/11789 Lt. David Nkiriho is the overall head and controller of the HQ. All data is streamed in from different locations which were deemed worthy monitoring.

9. Operation Fungua Macho covers the following areas;

a. **Hotels**: Hotels are known to be meeting points for people with depraved plans and also add to the fact that foreign journalists meet their informers mostly in hotels. Many hotels have collaborated either consciously (overt penetration) or unconsciously (covert penetration) and I can say with content

Annex 1: Brief to President Museveni on Operation Fungua Macho, 20 January 2012



SECRET

that we have made tremendous success and a lot of data is streaming in, especially from business centres of the hotels. The hotels include – Serena Kampala, Sheraton Kampala, Africana, Speke Resort Munyonyo, Imperial Royale, Emin Pasha, Grand Imperial, Tourist, Fairway, Triangle, Golf Course, Protea, Mamba Point, Equatorial, Cassia Lodge, Travellers Inn, Imperial Resort Beach, Imperial Botanical, Golf View Inn, Flight Motel and Brovad.

b. **Government Institutions**: Due to leakages from within the state apparatus, activity-spyware and gadgets targeting specific people have been deployed in the following institutions – CMI, ISO, ESO, Uganda Police and Parliament.

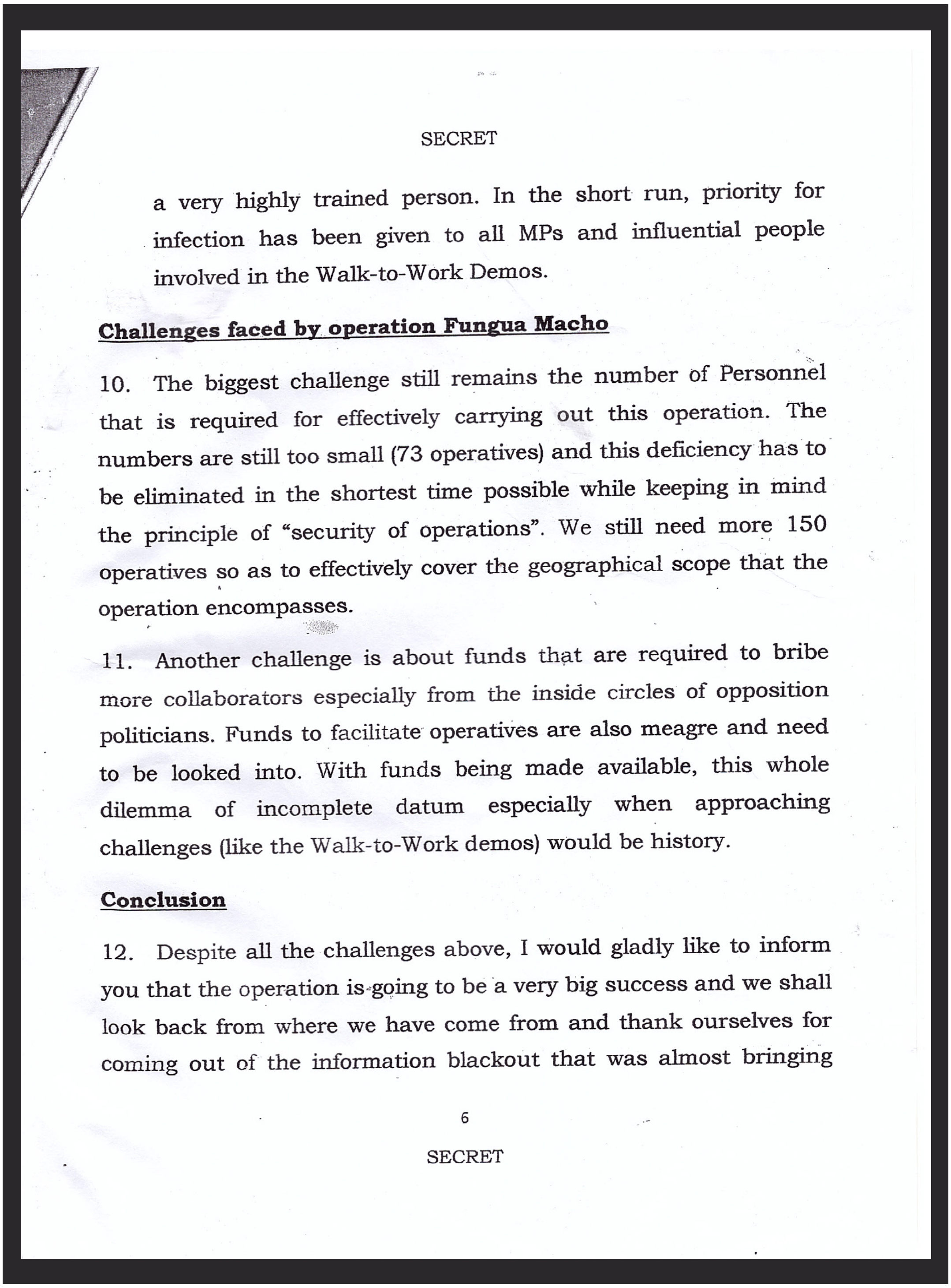
c. **Residential areas**: Fake Access Points have been created in Residential areas like – Munyonyo, Kensington housing estate, Lubowa estate and Kololo.

d. **Specific individuals**: People deemed dangerous to state security like government officials and opposition politicians are being surveilled and when opportunity strikes, their machines and gadgets are to be infected by FinFly Trojan horses for remote surveillance. We are also looking for people to use from within their own circles so as to access their gadgets. Infection and extraction takes not less than 05 minutes, hence such an operation doesn't necessarily require

5

SECRET

Annex 1: Brief to President Museveni on Operation Fungua Macho, 20 January 2012



SECRET

a very highly trained person. In the short run, priority for infection has been given to all MPs and influential people involved in the Walk-to-Work Demos.

Challenges faced by operation Fungua Macho

10. The biggest challenge still remains the number of Personnel that is required for effectively carrying out this operation. The numbers are still too small (73 operatives) and this deficiency has to be eliminated in the shortest time possible while keeping in mind the principle of "security of operations". We still need more 150 operatives so as to effectively cover the geographical scope that the operation encompasses.

11. Another challenge is about funds that are required to bribe more collaborators especially from the inside circles of opposition politicians. Funds to facilitate operatives are also meagre and need to be looked into. With funds being made available, this whole dilemma of incomplete datum especially when approaching challenges (like the Walk-to-Work demos) would be history.

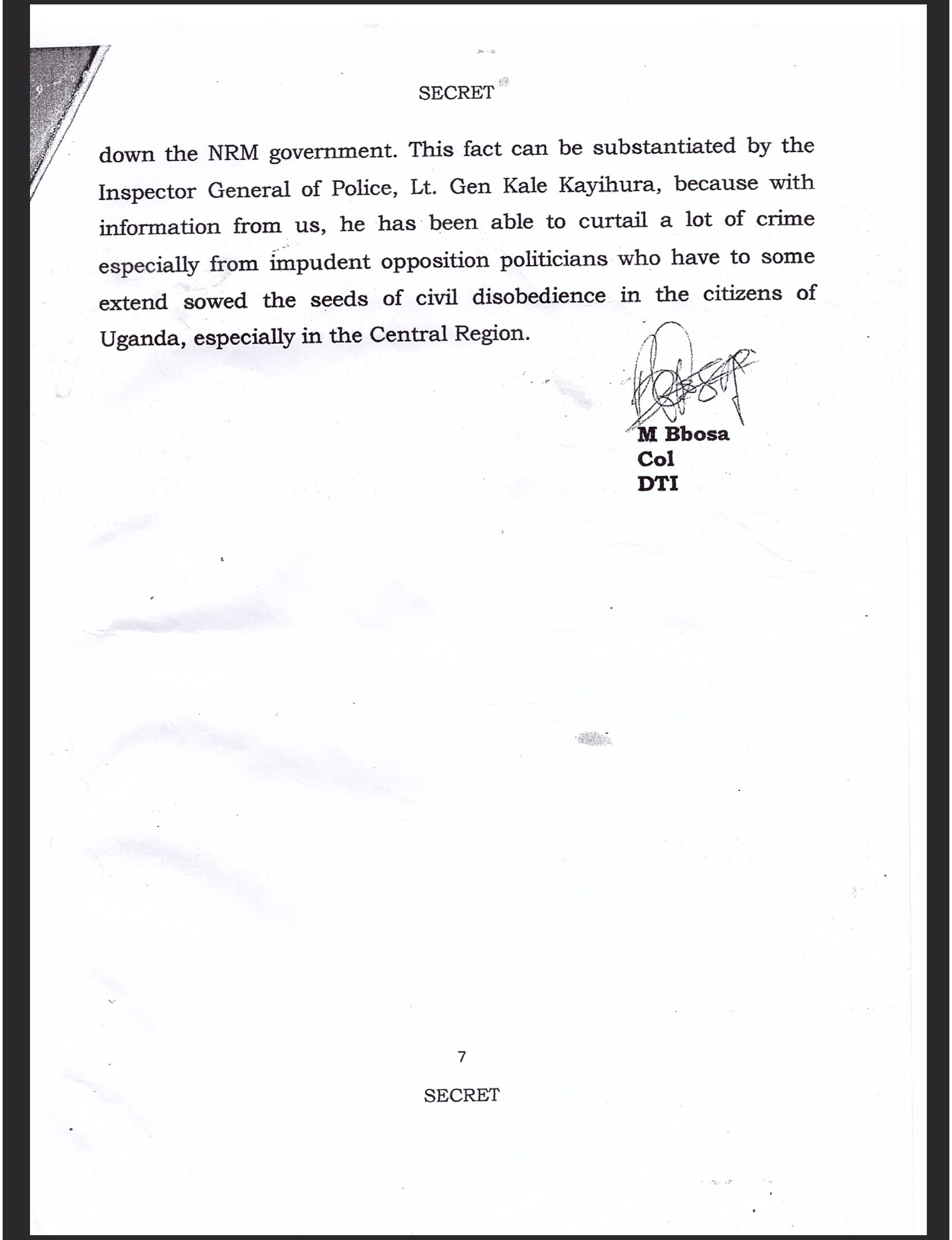
Conclusion

12. Despite all the challenges above, I would gladly like to inform you that the operation is going to be a very big success and we shall look back from where we have come from and thank ourselves for coming out of the information blackout that was almost bringing

6

SECRET

Annex 1: Brief to President Museveni on Operation Fungua Macho, 20 January 2012



SECRET

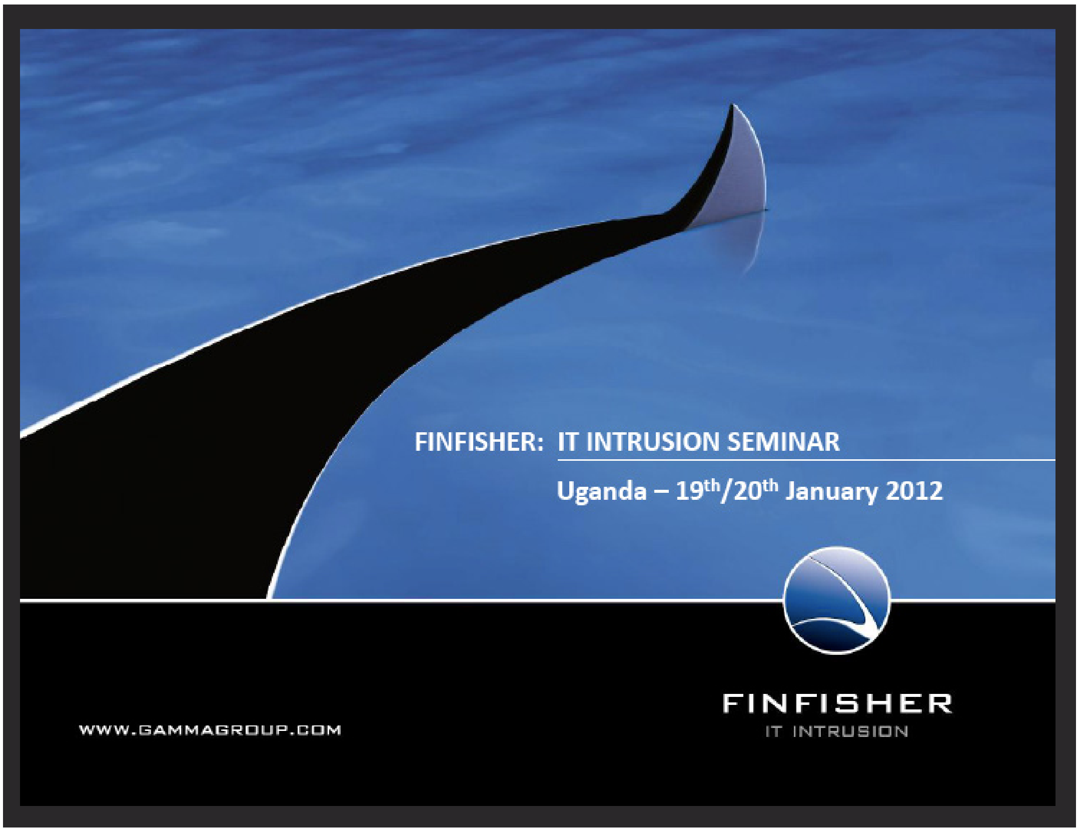
down the NRM government. This fact can be substantiated by the Inspector General of Police, Lt. Gen Kale Kayihura, because with information from us, he has been able to curtail a lot of crime especially from impudent opposition politicians who have to some extend sowed the seeds of civil disobedience in the citizens of Uganda, especially in the Central Region.

M Bbosa
Col
DTI

7

SECRET

Annex 2: Slides 1-6 of 96 slide presentation by Gamma officials to Uganda government officials, 2012



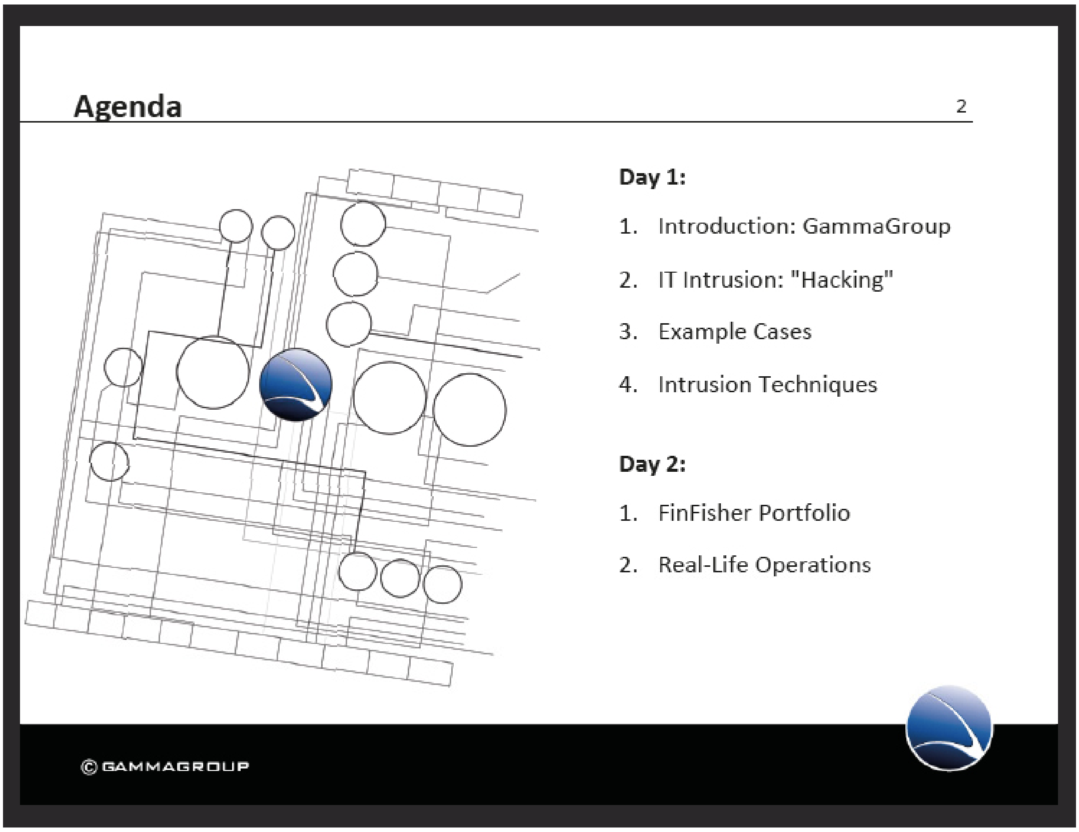
FINFISHER: IT INTRUSION SEMINAR

Uganda – 19th/20th January 2012

WWW.GAMMAGROUP.COM

FINFISHER
IT INTRUSION

Annex 2: Slides 1-6 of 96 slide presentation by Gamma officials to Uganda government officials, 2012



Agenda

2

Day 1:

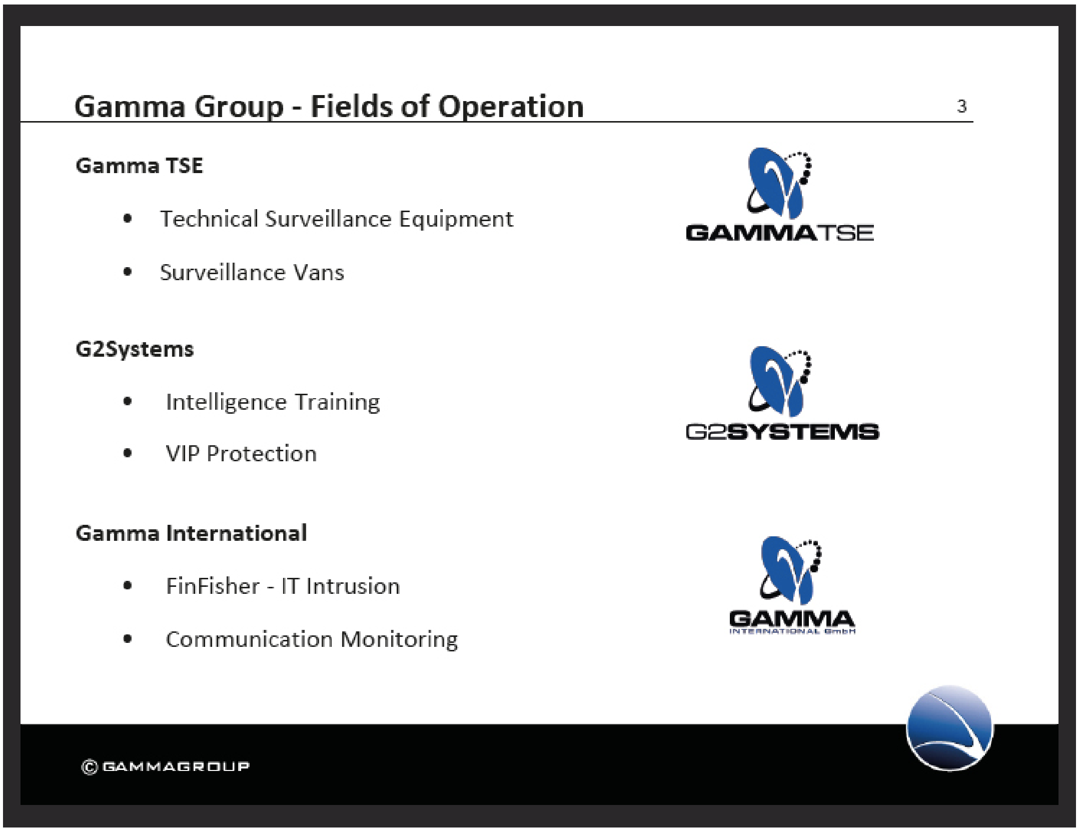
1. Introduction: GammaGroup
2. IT Intrusion: "Hacking"
3. Example Cases
4. Intrusion Techniques

Day 2:

1. FinFisher Portfolio
2. Real-Life Operations

© GAMMAGROUP

Annex 2: Slides 1-6 of 96 slide presentation by Gamma officials to Uganda government officials, 2012



GAMMATSE
G2SYSTEMS
GAMMA INTERNATIONAL GmbH

Gamma Group - Fields of Operation

3

Gamma TSE

- Technical Surveillance Equipment
- Surveillance Vans

G2Systems

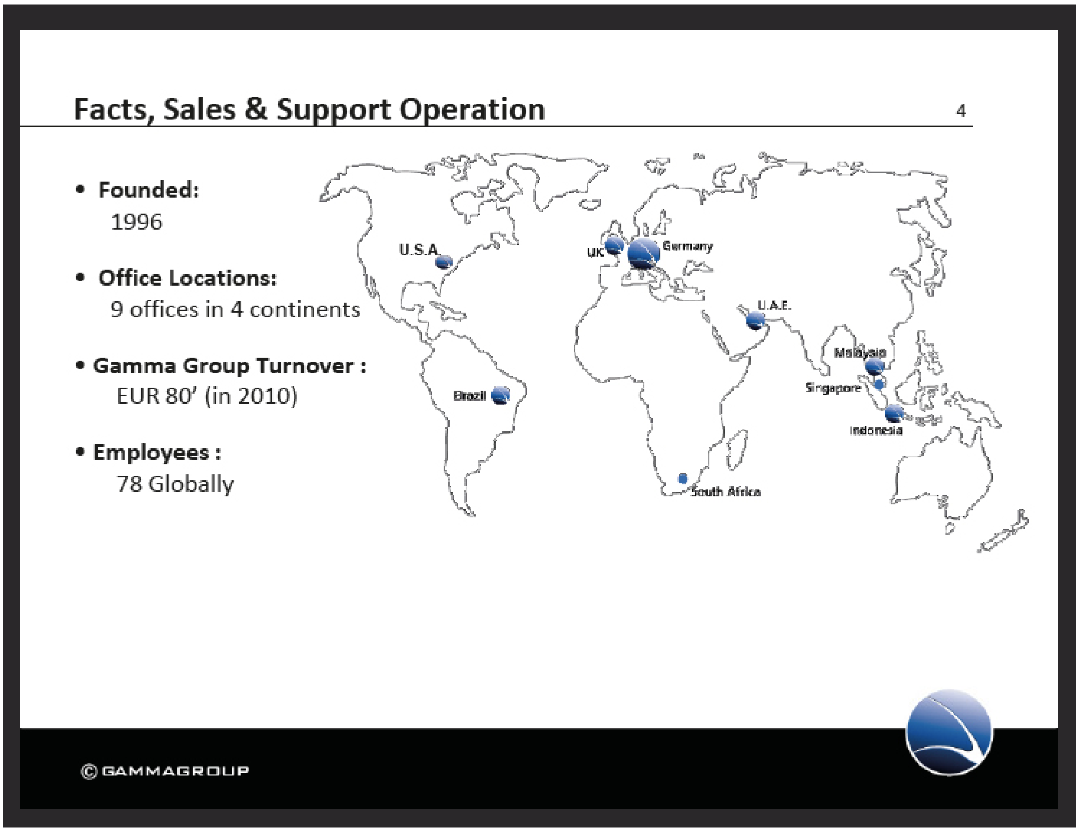
- Intelligence Training
- VIP Protection

Gamma International

- FinFisher - IT Intrusion
- Communication Monitoring

© GAMMAGROUP

Annex 2: Slides 1-6 of 96 slide presentation by Gamma officials to Uganda government officials, 2012



Facts, Sales & Support Operation

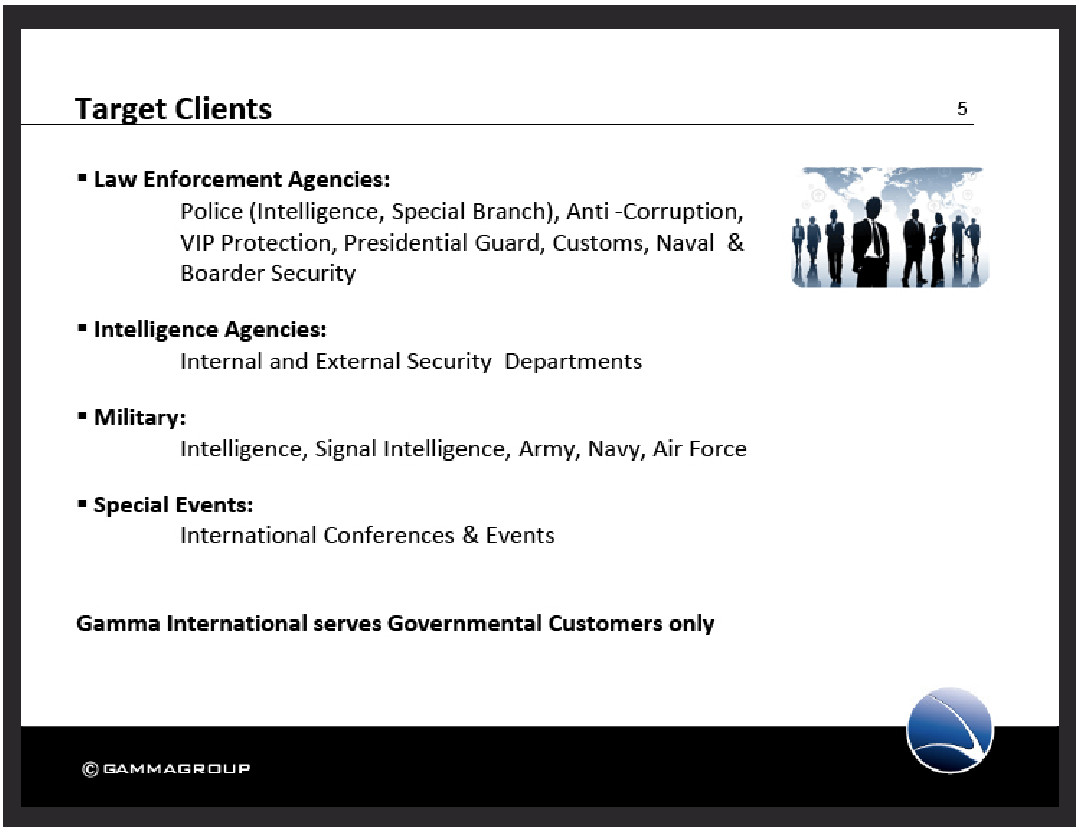
4

- **Founded:**
  1996
- **Office Locations:**
  9 offices in 4 continents
- **Gamma Group Turnover :**
  EUR 80' (in 2010)
- **Employees :**
  78 Globally

U.S.A.
UK
Germany
U.A.E.
Malaysia
Singapore
Indonesia
Brazil
South Africa

© GAMMAGROUP

Annex 2: Slides 1-6 of 96 slide presentation by Gamma officials to Uganda government officials, 2012



Target Clients

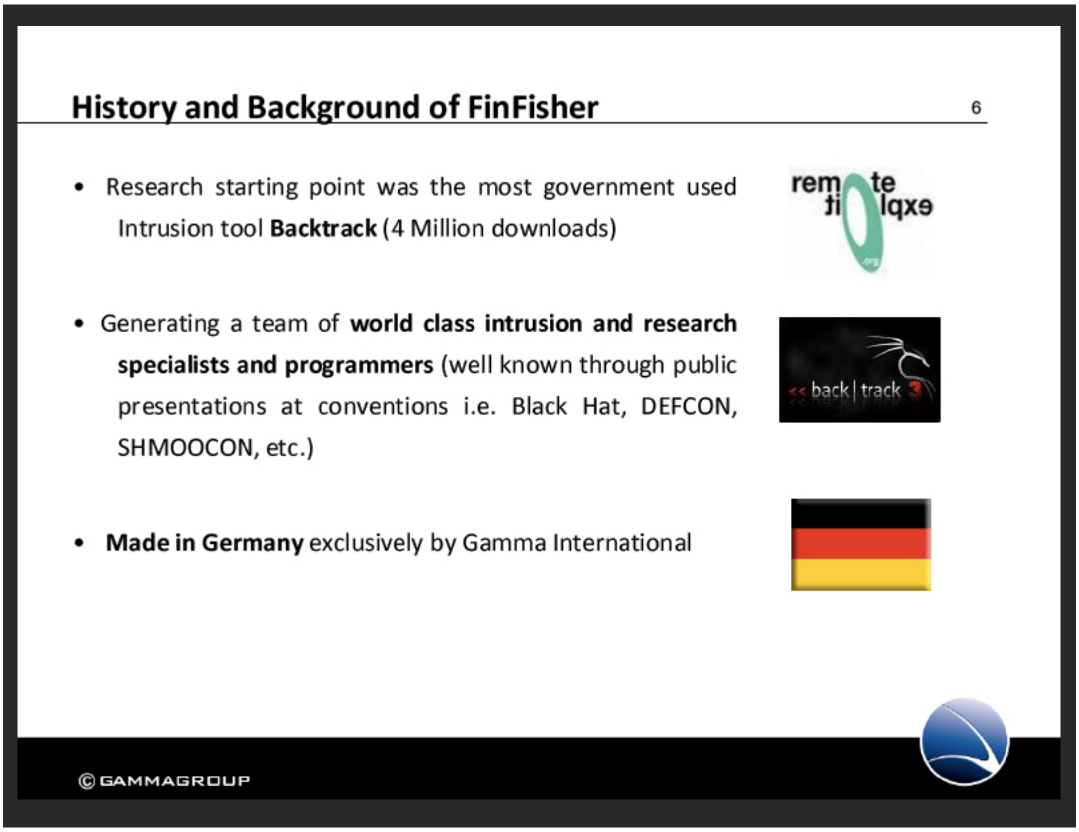
5

- **Law Enforcement Agencies:**
  Police (Intelligence, Special Branch), Anti -Corruption, VIP Protection, Presidential Guard, Customs, Naval & Boarder Security
- **Intelligence Agencies:**
  Internal and External Security Departments
- **Military:**
  Intelligence, Signal Intelligence, Army, Navy, Air Force
- **Special Events:**
  International Conferences & Events

Gamma International serves Governmental Customers only

© GAMMAGROUP

Annex 2: Slides 1-6 of 96 slide presentation by Gamma officials to Uganda government officials, 2012



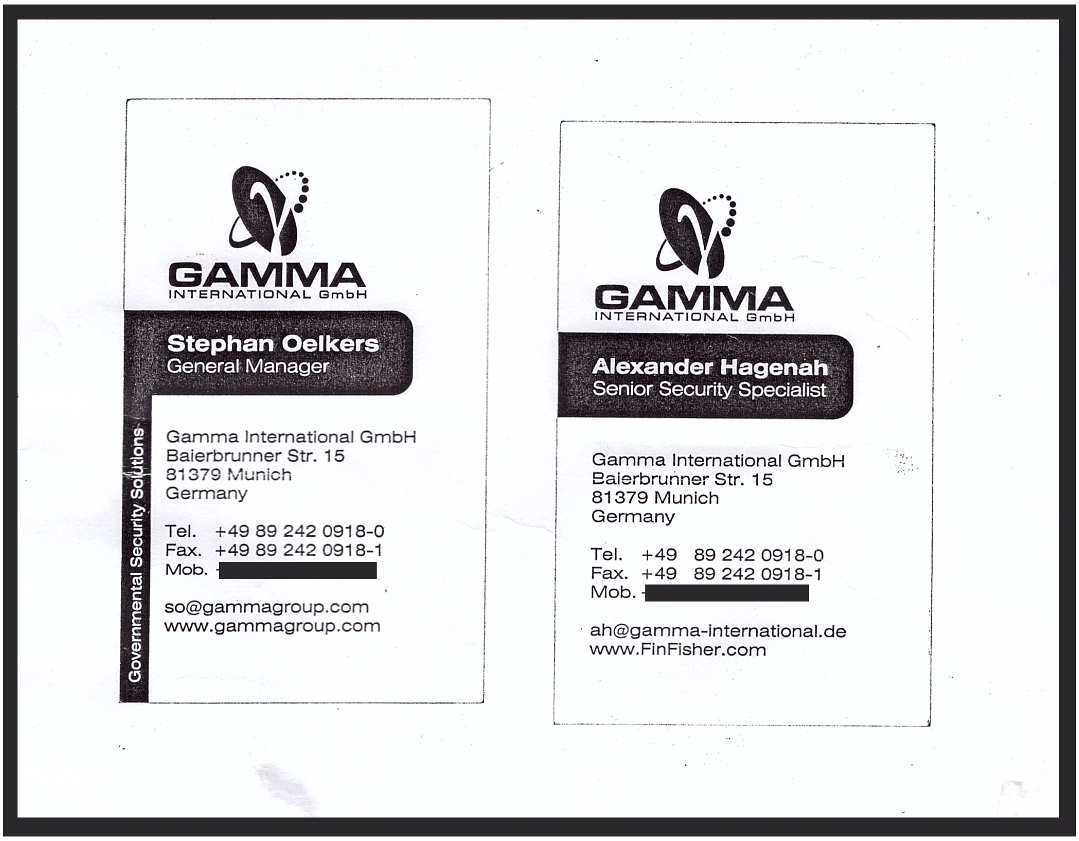
History and Background of FinFisher

6

- Research starting point was the most government used Intrusion tool **Backtrack** (4 Million downloads)
- Generating a team of **world class intrusion and research specialists and programmers** (well known through public presentations at conventions i.e. Black Hat, DEFCON, SHMOOCON, etc.)
- **Made in Germany** exclusively by Gamma International

© GAMMAGROUP

Annex 3: Business cards of Stephan Oelkers and Alexander Hagenah, Gamma International GmbH, 2011



GAMMA
INTERNATIONAL GmbH

Stephan Oelkers
General Manager

Governmental Security Solutions

Gamma International GmbH
Baierbrunner Str. 15
81379 Munich
Germany

Tel. +49 89 242 0918-0
Fax. +49 89 242 0918-1
Mob. [redacted]

so@gammagroup.com
www.gammagroup.com

GAMMA
INTERNATIONAL GmbH

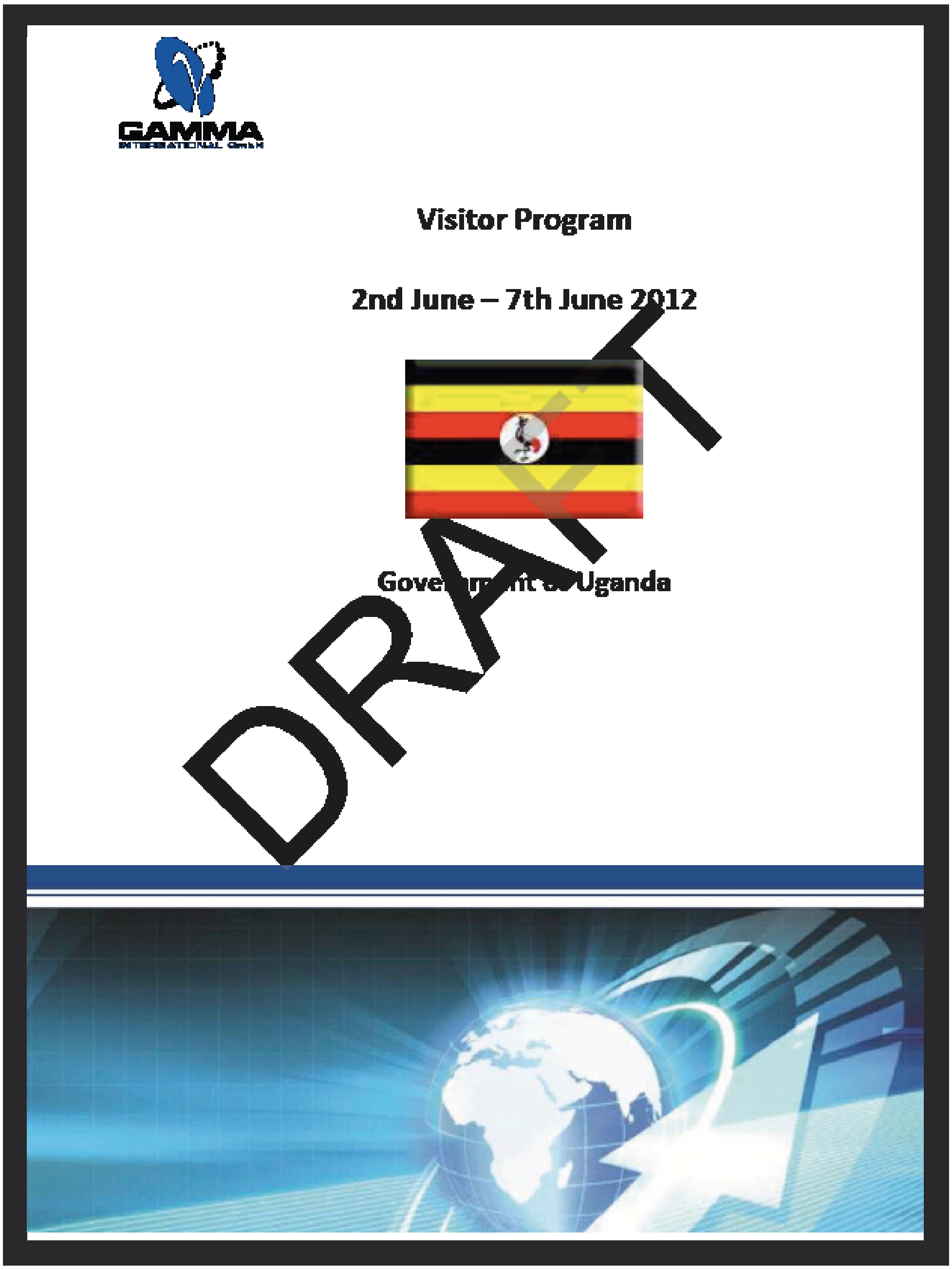
Alexander Hagenah
Senior Security Specialist

Gamma International GmbH
Baierbrunner Str. 15
81379 Munich
Germany

Tel. +49 89 242 0918-0
Fax. +49 89 242 0918-1
Mob. [redacted]

ah@gamma-international.de
www.FinFisher.com

Annex 4: Draft Visitor Program, visit of Ugandan officials to Gamma International GmbH, June 2012



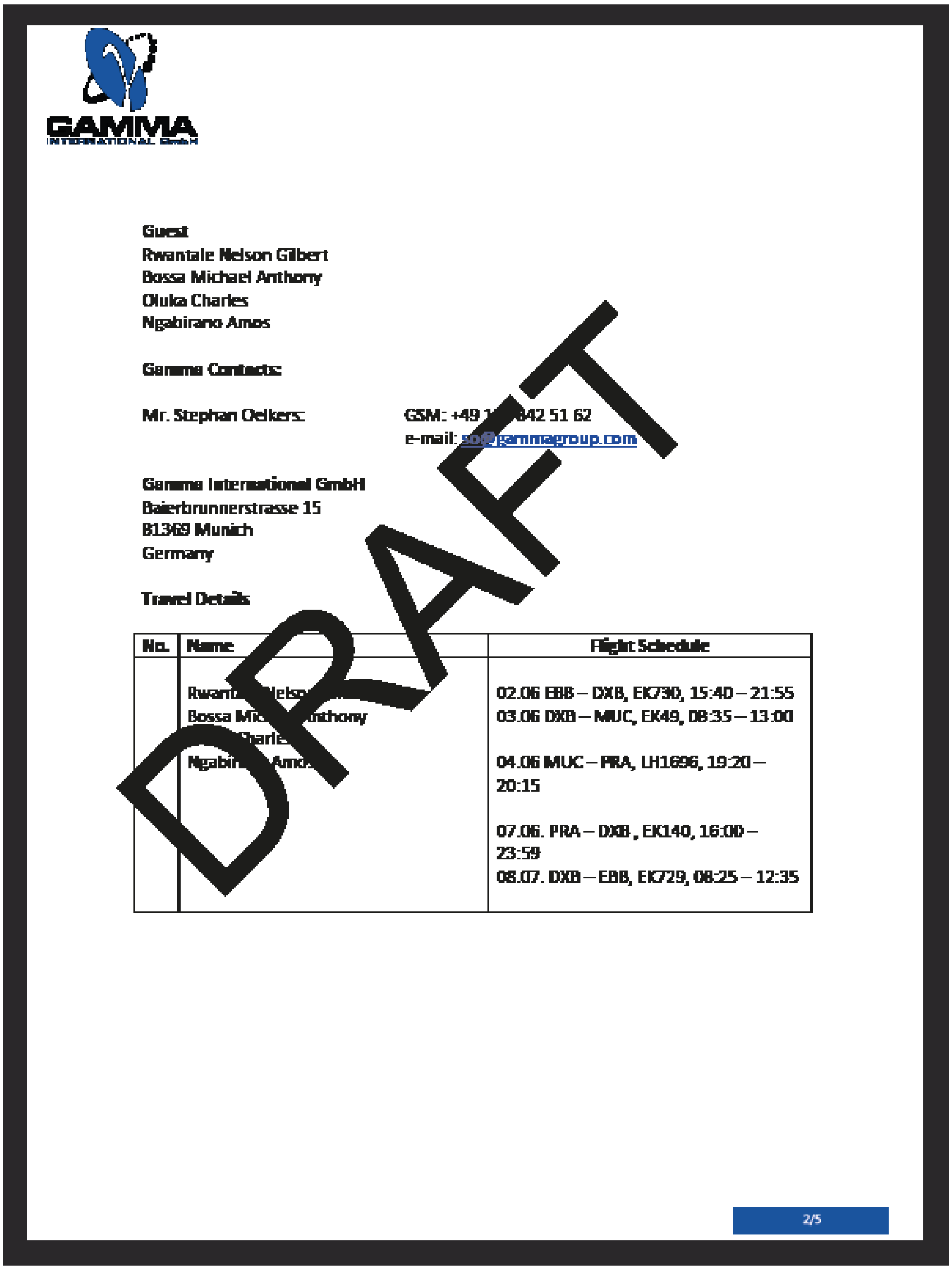
GAMMA INTERNATIONAL GmbH

Visitor Program

2nd June – 7th June 2012

Government of Uganda

Annex 4: Draft Visitor Program, visit of Ugandan officials to Gamma International GmbH, June 2012



GAMMA
INTERNATIONAL GmbH

Guest
Rwantale Nelson Gilbert
Bossa Michael Anthony
Oluka Charles
Ngabirano Amos

Gamma Contacts:

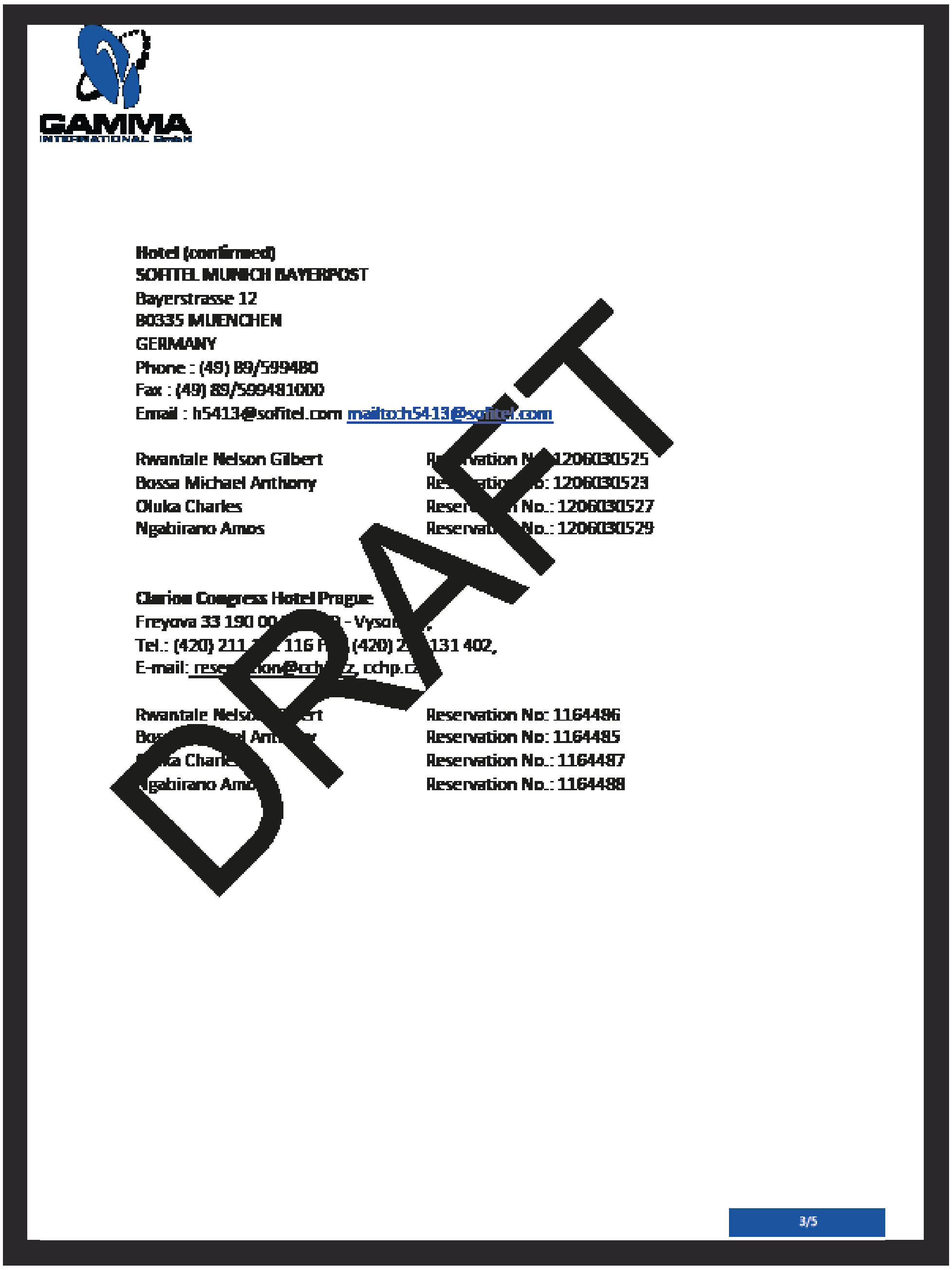
Mr. Stephan Oelkers:	GSM: +49 1[illegible]842 51 62 e-mail: so@gammagroup.com

Gamma International GmbH
Baierbrunnerstrasse 15
81369 Munich
Germany

Travel Details

No.	Name	Flight Schedule
	Rwant[illegible] Nelso[illegible] Bossa Mic[illegible]nthony [illegible]Charle[illegible] Ngabir[illegible] Amo[illegible]	02.06 EBB – DXB, EK730, 15:40 – 21:55 03.06 DXB – MUC, EK49, 08:35 – 13:00 04.06 MUC – PRA, LH1696, 19:20 – 20:15 07.06. PRA – DXB , EK140, 16:00 – 23:59 08.07. DXB – EBB, EK729, 08:25 – 12:35

Annex 4: Draft Visitor Program, visit of Ugandan officials to Gamma International GmbH, June 2012



GAMMA INTERNATIONAL GmbH

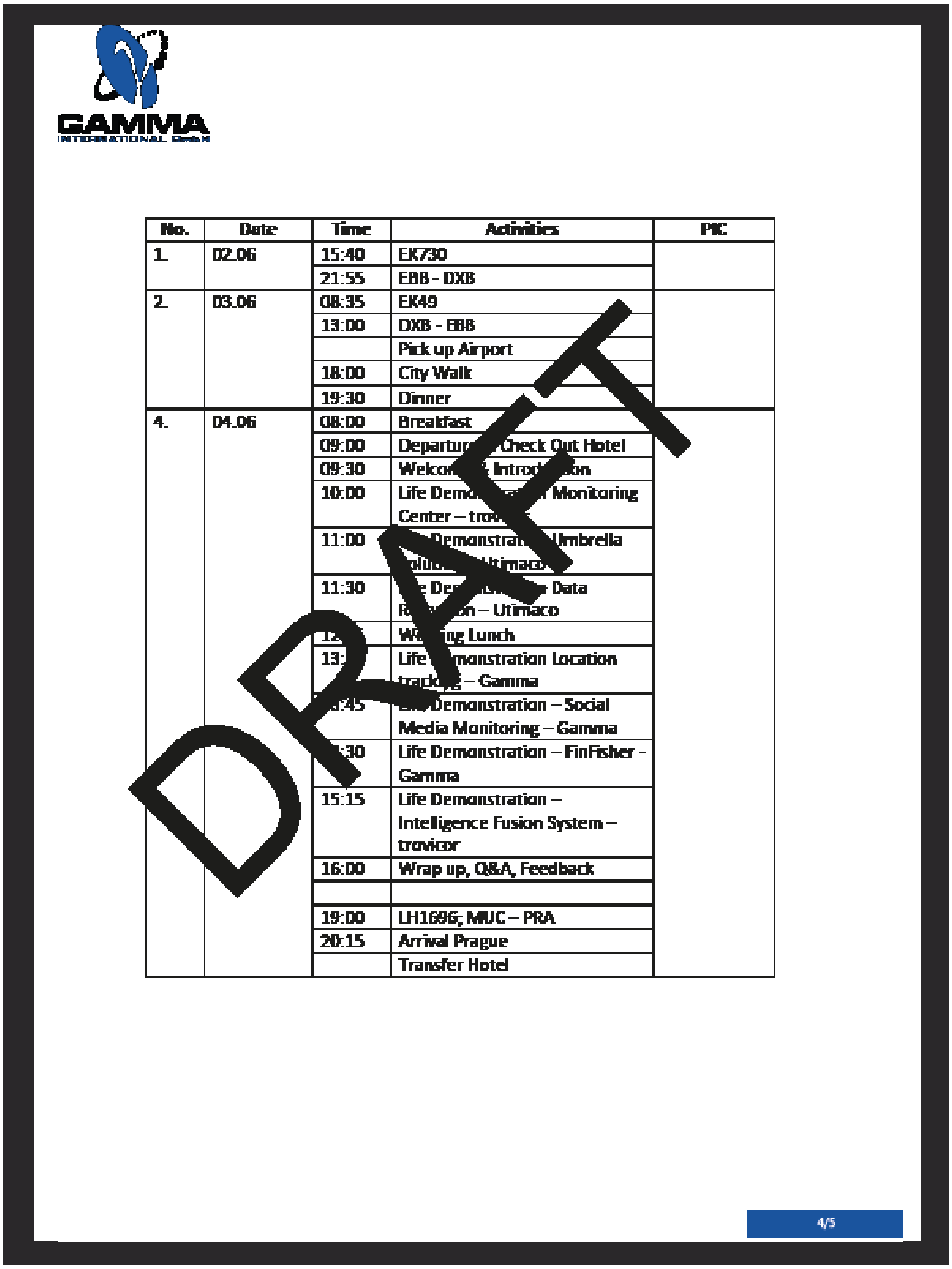
Hotel (confirmed)
SOFITEL MUNICH BAYERPOST
Bayerstrasse 12
80335 MUENCHEN
GERMANY
Phone : (49) 89/599480
Fax : (49) 89/599481000
Email : h5413@sofitel.com mailto:h5413@sofitel.com

Rwantale Nelson Gilbert	Reservation No: 1206030525
Bossa Michael Anthony	Reservation No: 1206030523
Oluka Charles	Reservation No.: 1206030527
Ngabirano Amos	Reservation No.: 1206030529

Clarion Congress Hotel Prague
Freyova 33 190 00 Praha 9 - Vysočany,
Tel.: (420) 211 131 116 Fax (420) 211 131 402,
E-mail: reservation@cchp.cz, cchp.cz

Rwantale Nelson Gilbert	Reservation No: 1164486
Bossa Michael Anthony	Reservation No: 1164485
Oluka Charles	Reservation No.: 1164487
Ngabirano Amos	Reservation No.: 1164488

Annex 4: Draft Visitor Program, visit of Ugandan officials to Gamma International GmbH, June 2012

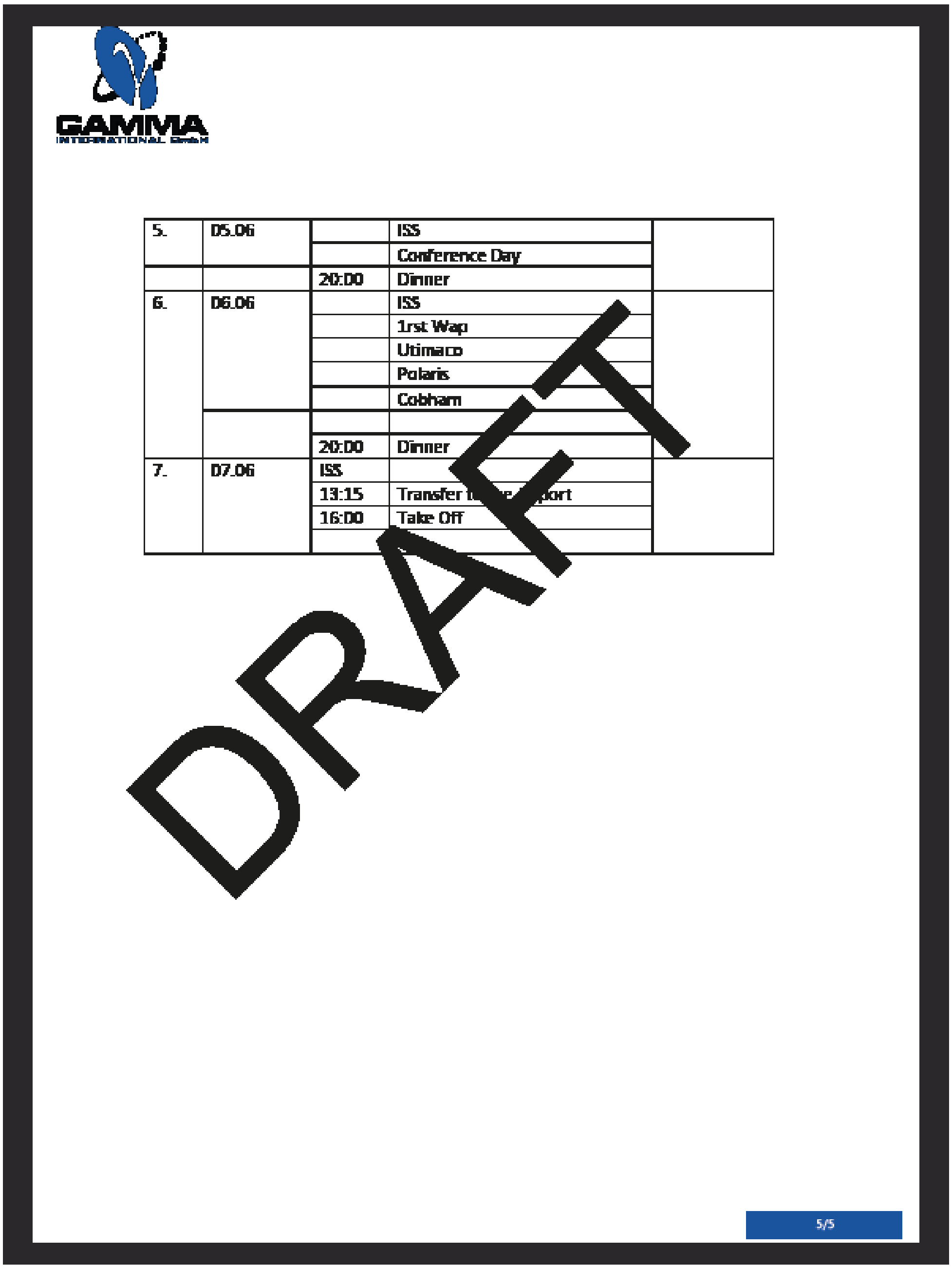


GAMMA INTERNATIONAL GmbH

No.	Date	Time	Activities	PIC
1.	02.06	15:40	EK730	
		21:55	EBB - DXB	
2.	03.06	08:35	EK49	
		13:00	DXB - EBB	
			Pick up Airport	
		18:00	City Walk	
		19:30	Dinner	
4.	04.06	08:00	Breakfast	
		09:00	Departure – Check Out Hotel	
		09:30	Welcome & Introduction	
		10:00	Life Demonstration Monitoring Center – trovicor	
		11:00	Life Demonstration Umbrella Solution – Utimaco	
		11:30	Life Demonstration Data Retention – Utimaco	
		12:[illegible]	Working Lunch	
		13:[illegible]	Life Demonstration Location tracking – Gamma	
		[illegible]:45	Life Demonstration – Social Media Monitoring – Gamma	
		[illegible]:30	Life Demonstration – FinFisher - Gamma	
		15:15	Life Demonstration – Intelligence Fusion System – trovicor	
		16:00	Wrap up, Q&A, Feedback	
		19:00	LH1696; MUC – PRA	
		20:15	Arrival Prague	
			Transfer Hotel	

4/5

Annex 4: Draft Visitor Program, visit of Ugandan officials to Gamma International GmbH, June 2012

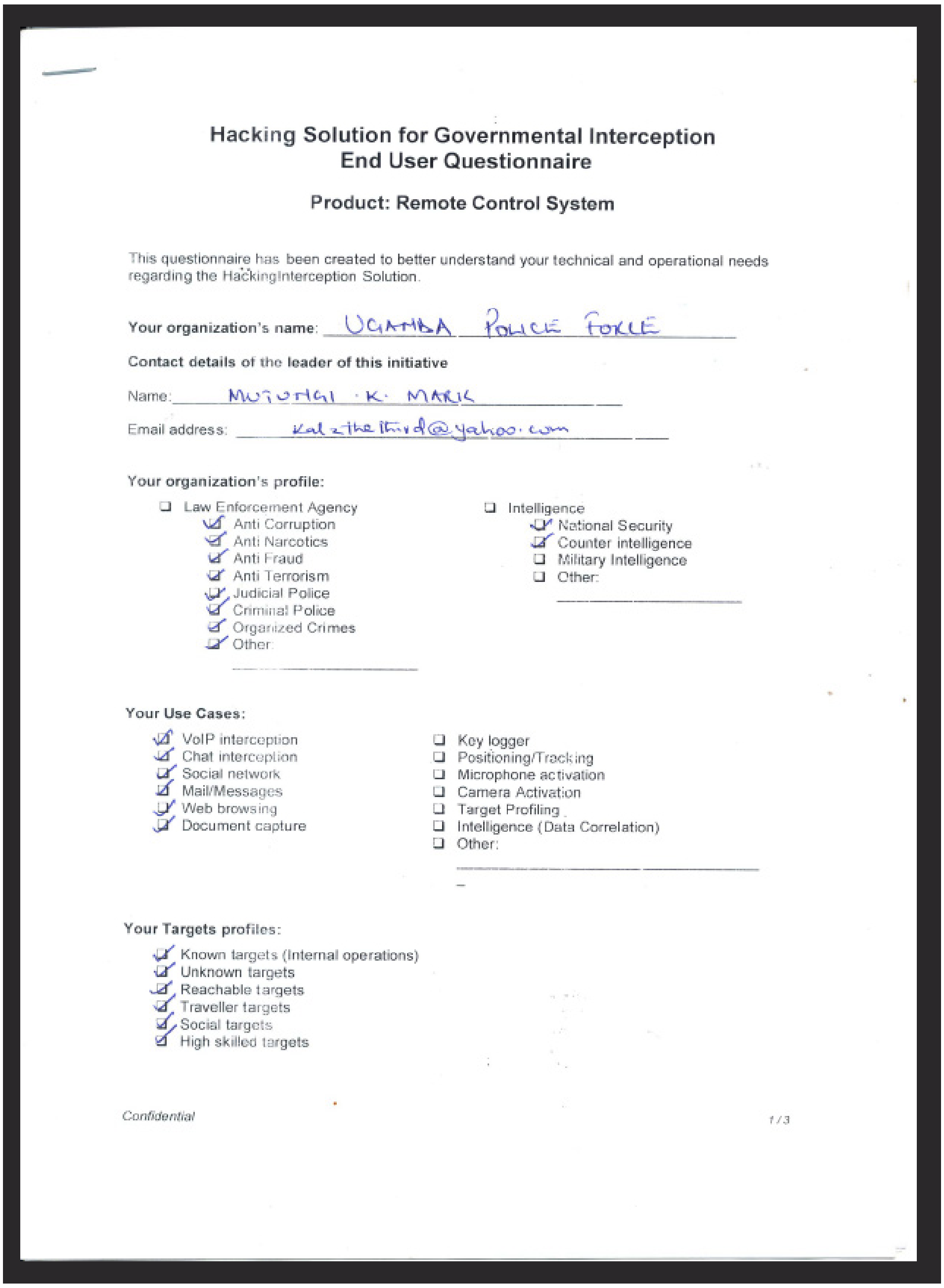


GAMMA
INTERNATIONAL GmbH

5.	05.06		ISS	
			Conference Day	
		20:00	Dinner	
6.	06.06		ISS	
			1rst Wap	
			Utimaco	
			Polaris	
			Cobham	
		20:00	Dinner	
7.	07.06	ISS		
		13:15	Transfer to the airport	
		16:00	Take Off	

5/5

Annex 5: Uganda Customer and Uganda Local Contact forms provided to Hacking Team, May 2015



Hacking Solution for Governmental Interception
End User Questionnaire

Product: Remote Control System

This questionnaire has been created to better understand your technical and operational needs regarding the HackingInterception Solution.

Your organization's name: UGANDA POLICE FORCE

Contact details of the leader of this initiative

Name: MUJUNGI · K · MARK

Email address: kal2thethird@yahoo.com

Your organization's profile:

- □ Law Enforcement Agency
  - ☑ Anti Corruption
  - ☑ Anti Narcotics
  - ☑ Anti Fraud
  - ☑ Anti Terrorism
  - ☑ Judicial Police
  - ☑ Criminal Police
  - ☑ Organized Crimes
  - ☑ Other: ____________
- □ Intelligence
  - ☑ National Security
  - ☑ Counter intelligence
  - □ Military Intelligence
  - □ Other: ____________

Your Use Cases:

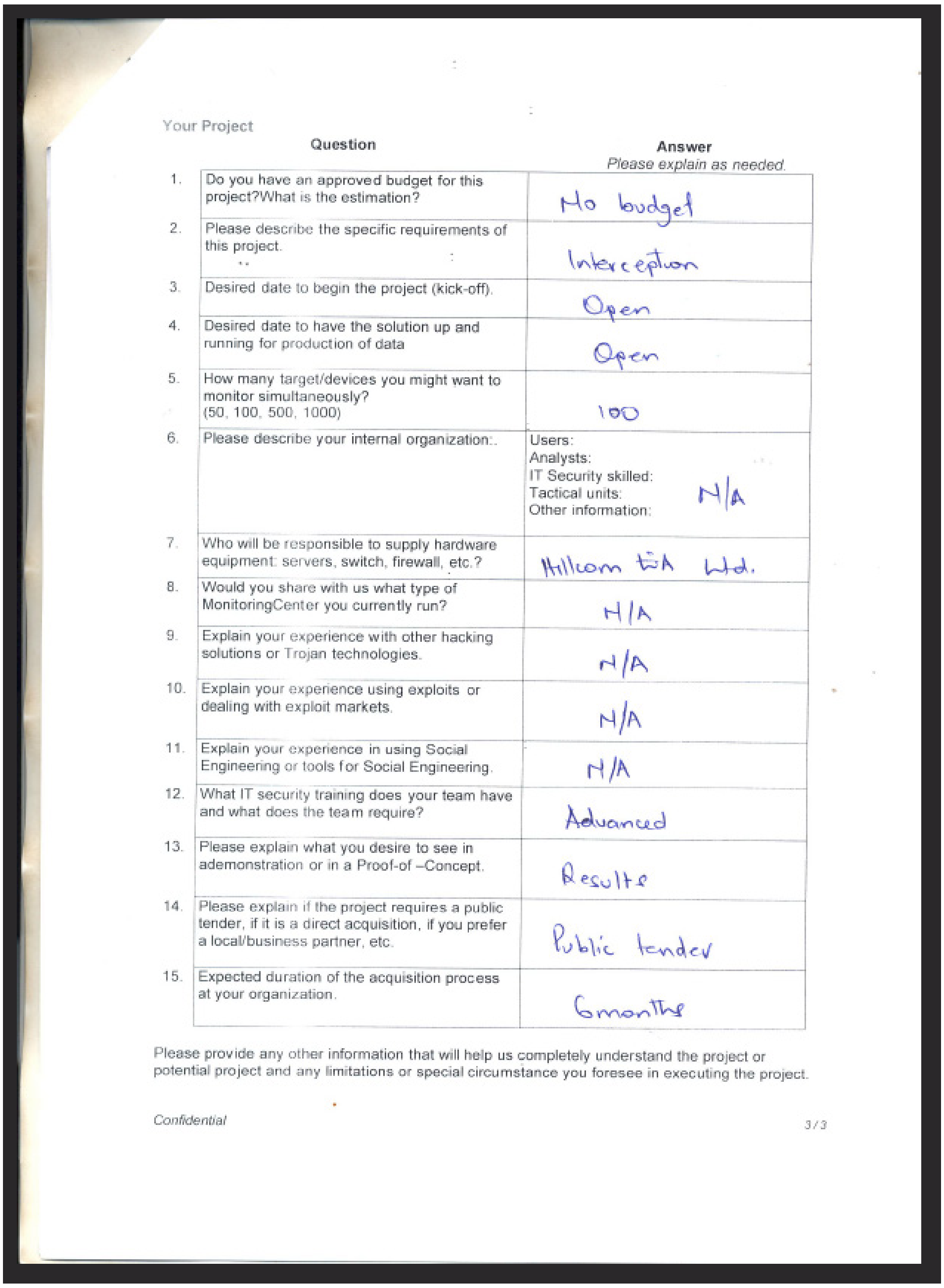
- ☑ VoIP interception
- ☑ Chat interception
- ☑ Social network
- ☑ Mail/Messages
- ☑ Web browsing
- ☑ Document capture
- □ Key logger
- □ Positioning/Tracking
- □ Microphone activation
- □ Camera Activation
- □ Target Profiling
- □ Intelligence (Data Correlation)
- □ Other: ____________

Your Targets profiles:

- ☑ Known targets (Internal operations)
- ☑ Unknown targets
- ☑ Reachable targets
- ☑ Traveller targets
- ☑ Social targets
- ☑ High skilled targets

Confidential 1 / 3

Annex 5: Uganda Customer and Uganda Local Contact forms provided to Hacking Team, May 2015



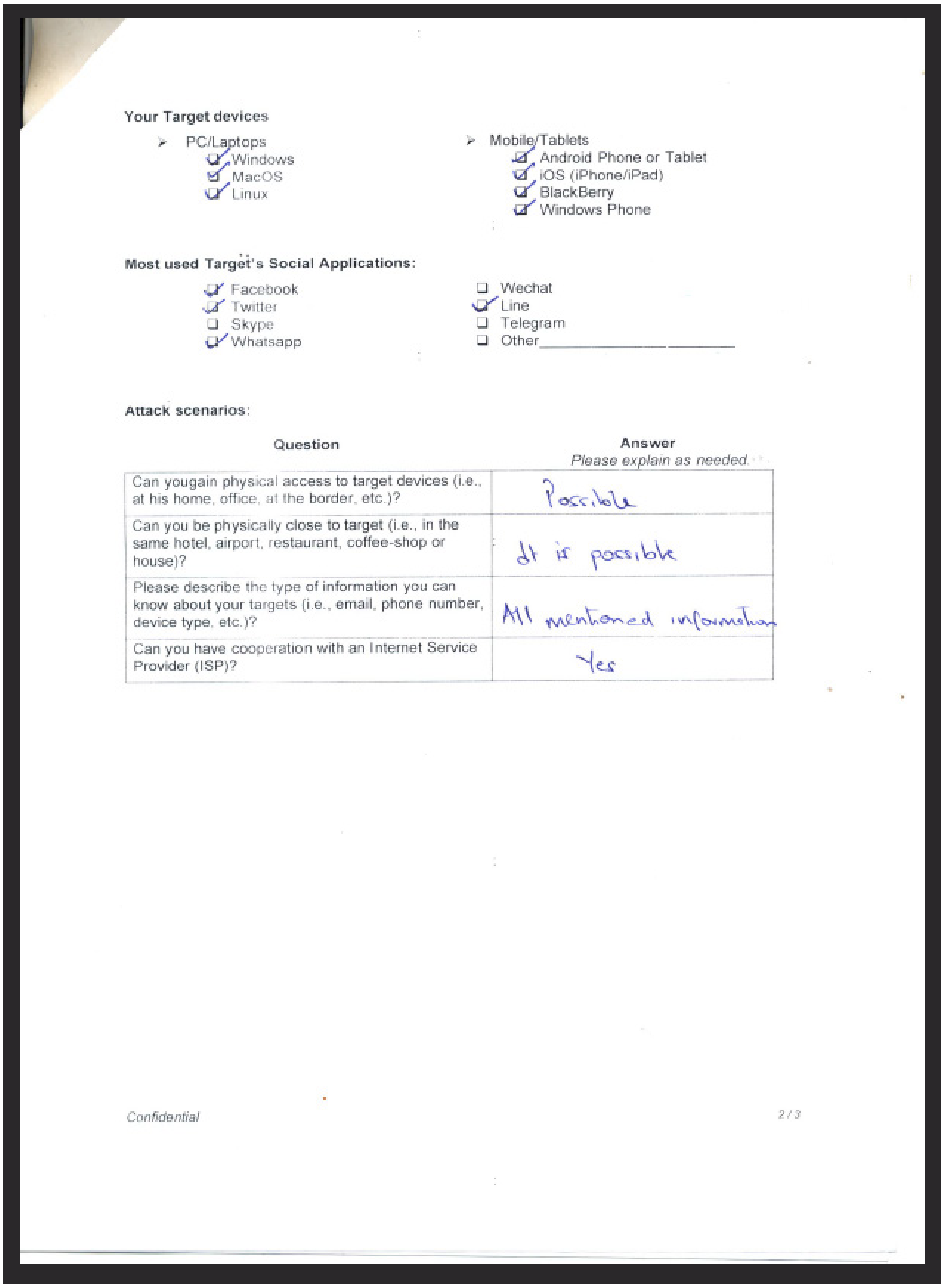
Your Project

	Question	Answer *Please explain as needed.*
1.	Do you have an approved budget for this project?What is the estimation?	No budget
2.	Please describe the specific requirements of this project.	Interception
3.	Desired date to begin the project (kick-off).	Open
4.	Desired date to have the solution up and running for production of data	Open
5.	How many target/devices you might want to monitor simultaneously? (50, 100, 500, 1000)	100
6.	Please describe your internal organization:.	Users: Analysts: IT Security skilled: Tactical units: Other information: N/A
7.	Who will be responsible to supply hardware equipment: servers, switch, firewall, etc.?	Hillcom EA Ltd.
8.	Would you share with us what type of MonitoringCenter you currently run?	N/A
9.	Explain your experience with other hacking solutions or Trojan technologies.	N/A
10.	Explain your experience using exploits or dealing with exploit markets.	N/A
11.	Explain your experience in using Social Engineering or tools for Social Engineering.	N/A
12.	What IT security training does your team have and what does the team require?	Advanced
13.	Please explain what you desire to see in ademonstration or in a Proof-of –Concept.	Results
14.	Please explain if the project requires a public tender, if it is a direct acquisition, if you prefer a local/business partner, etc.	Public tender
15.	Expected duration of the acquisition process at your organization.	6months

Please provide any other information that will help us completely understand the project or potential project and any limitations or special circumstance you foresee in executing the project.

Confidential 3/3

Annex 5: Uganda Customer and Uganda Local Contact forms provided to Hacking Team, May 2015



Your Target devices

- PC/Laptops
  - ☑ Windows
  - ☑ MacOS
  - ☑ Linux
- Mobile/Tablets
  - ☑ Android Phone or Tablet
  - ☑ iOS (iPhone/iPad)
  - ☑ BlackBerry
  - ☑ Windows Phone

Most used Target's Social Applications:

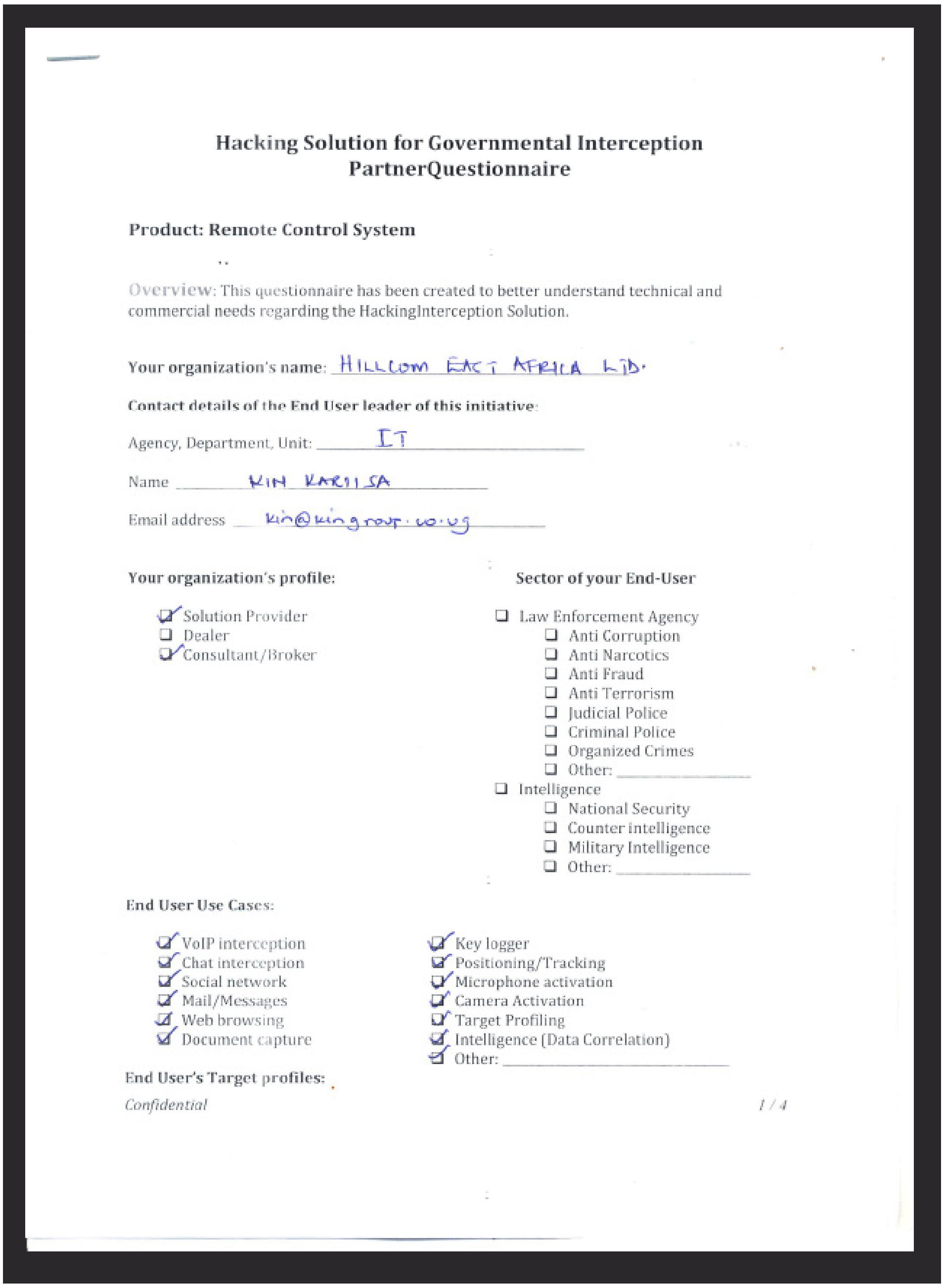
☑ Facebook
☑ Twitter
□ Skype
☑ Whatsapp

□ Wechat
☑ Line
□ Telegram
□ Other________________________

Attack scenarios:

Question	Answer *Please explain as needed.*
Can yougain physical access to target devices (i.e., at his home, office, at the border, etc.)?	Possible
Can you be physically close to target (i.e., in the same hotel, airport, restaurant, coffee-shop or house)?	It is possible
Please describe the type of information you can know about your targets (i.e., email, phone number, device type, etc.)?	All mentioned information
Can you have cooperation with an Internet Service Provider (ISP)?	Yes

Annex 5: Uganda Customer and Uganda Local Contact forms provided to Hacking Team, May 2015



Hacking Solution for Governmental Interception
PartnerQuestionnaire

Product: Remote Control System

Overview: This questionnaire has been created to better understand technical and commercial needs regarding the HackingInterception Solution.

Your organization's name: HILLCOM EAST AFRICA LTD.

Contact details of the End User leader of this initiative:

Agency, Department, Unit: IT

Name KIN KARIISA

Email address kin@kingroup.co.ug

Your organization's profile:

- ☑ Solution Provider
- □ Dealer
- ☑ Consultant/Broker

Sector of your End-User

- □ Law Enforcement Agency
  - □ Anti Corruption
  - □ Anti Narcotics
  - □ Anti Fraud
  - □ Anti Terrorism
  - □ Judicial Police
  - □ Criminal Police
  - □ Organized Crimes
  - □ Other: ____________
- □ Intelligence
  - □ National Security
  - □ Counter intelligence
  - □ Military Intelligence
  - □ Other: ____________

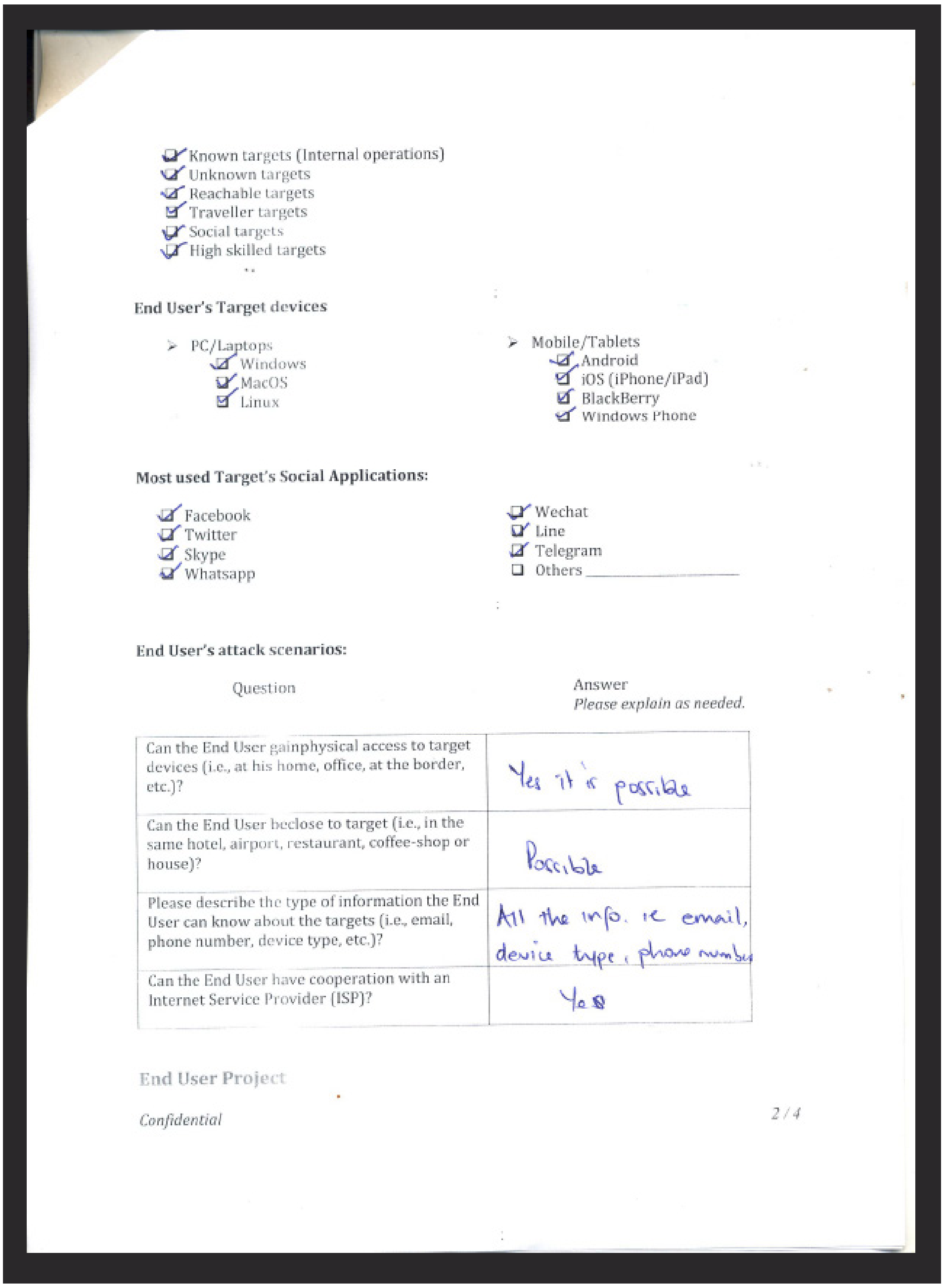
End User Use Cases:

- ☑ VoIP interception
- ☑ Chat interception
- ☑ Social network
- ☑ Mail/Messages
- ☑ Web browsing
- ☑ Document capture
- ☑ Key logger
- ☑ Positioning/Tracking
- ☑ Microphone activation
- ☑ Camera Activation
- ☑ Target Profiling
- ☑ Intelligence (Data Correlation)
- ☑ Other: ____________

End User's Target profiles:

Confidential 1 / 4

Annex 5: Uganda Customer and Uganda Local Contact forms provided to Hacking Team, May 2015



☑ Known targets (Internal operations)
☑ Unknown targets
☑ Reachable targets
☑ Traveller targets
☑ Social targets
☑ High skilled targets

End User's Target devices

- PC/Laptops
  - ☑ Windows
  - ☑ MacOS
  - ☑ Linux
- Mobile/Tablets
  - ☑ Android
  - ☑ iOS (iPhone/iPad)
  - ☑ BlackBerry
  - ☑ Windows Phone

Most used Target's Social Applications:

☑ Facebook
☑ Twitter
☑ Skype
☑ Whatsapp
☑ Wechat
☑ Line
☑ Telegram
□ Others ______________

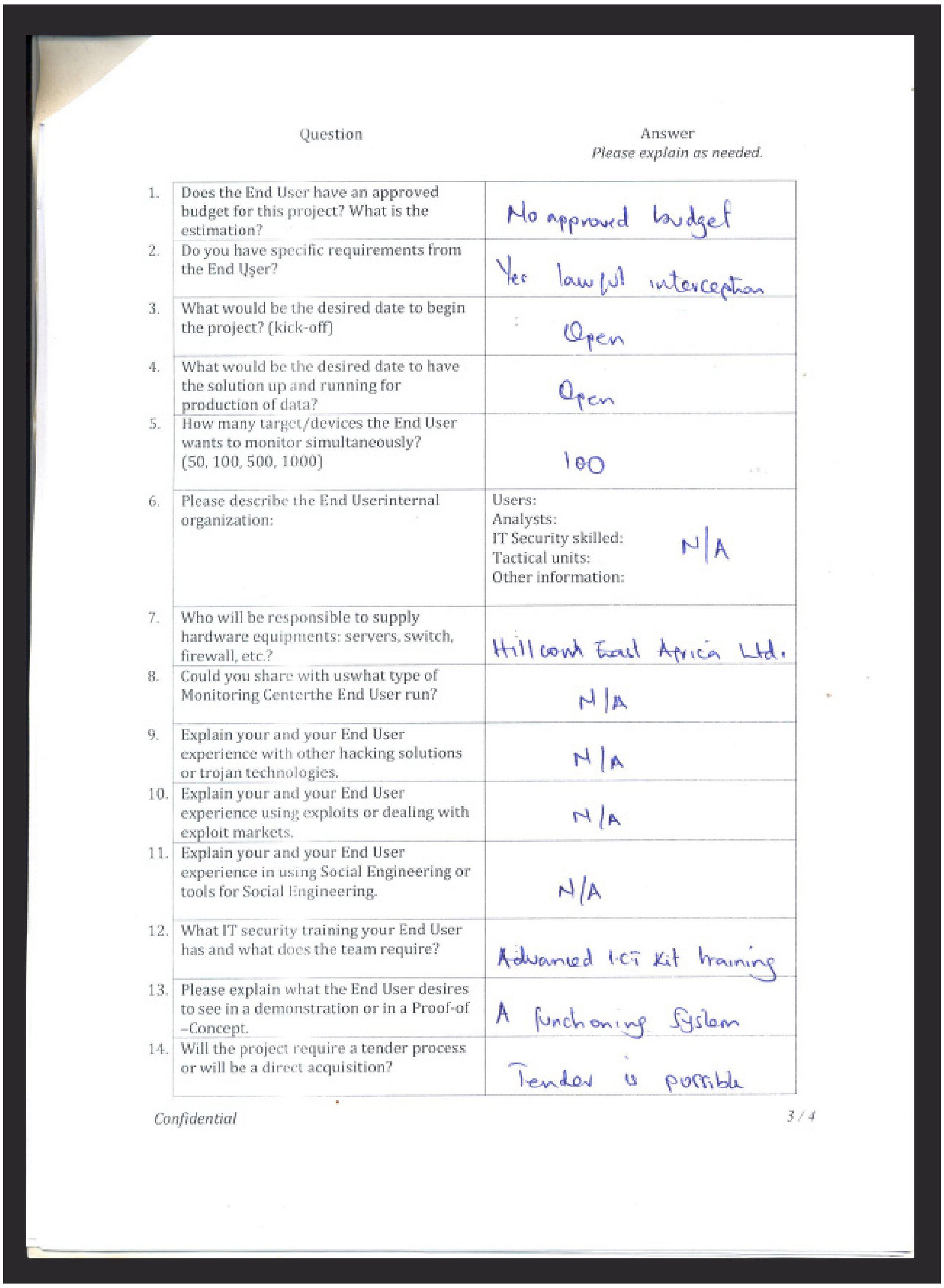
End User's attack scenarios:

Question	Answer *Please explain as needed.*
Can the End User gainphysical access to target devices (i.e., at his home, office, at the border, etc.)?	Yes it is possible
Can the End User beclose to target (i.e., in the same hotel, airport, restaurant, coffee-shop or house)?	Possible
Please describe the type of information the End User can know about the targets (i.e., email, phone number, device type, etc.)?	All the info. ie email, device type, phone number
Can the End User have cooperation with an Internet Service Provider (ISP)?	Yes

End User Project

Confidential 2 / 4

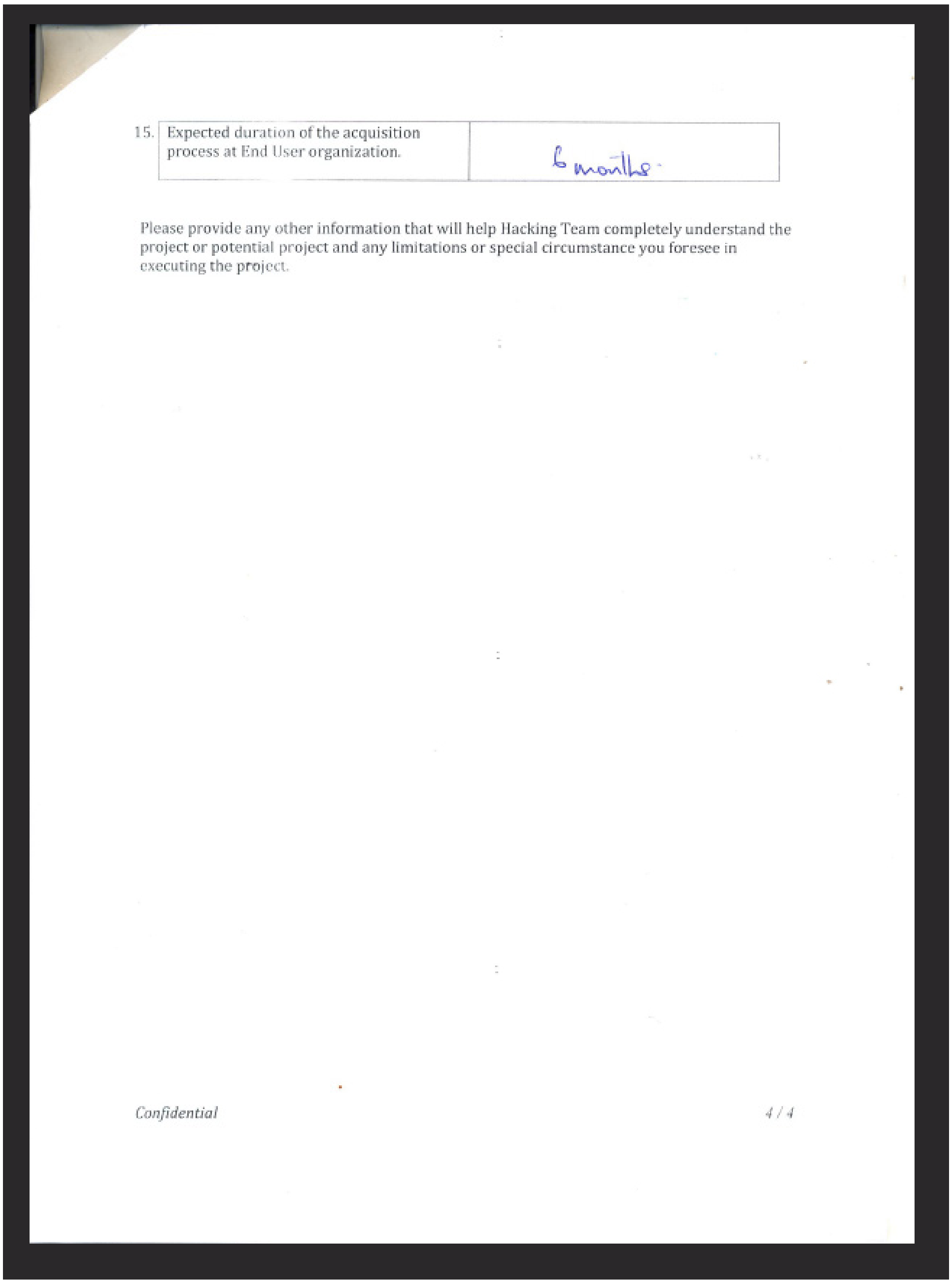
Annex 5: Uganda Customer and Uganda Local Contact forms provided to Hacking Team, May 2015



	Question	Answer *Please explain as needed.*
1.	Does the End User have an approved budget for this project? What is the estimation?	No approved budget
2.	Do you have specific requirements from the End User?	Yes lawful interception
3.	What would be the desired date to begin the project? (kick-off)	Open
4.	What would be the desired date to have the solution up and running for production of data?	Open
5.	How many target/devices the End User wants to monitor simultaneously? (50, 100, 500, 1000)	100
6.	Please describe the End Userinternal organization:	Users: Analysts: IT Security skilled: Tactical units: Other information: N/A
7.	Who will be responsible to supply hardware equipments: servers, switch, firewall, etc.?	Hillcom East Africa Ltd.
8.	Could you share with uswhat type of Monitoring Centerthe End User run?	N/A
9.	Explain your and your End User experience with other hacking solutions or trojan technologies.	N/A
10.	Explain your and your End User experience using exploits or dealing with exploit markets.	N/A
11.	Explain your and your End User experience in using Social Engineering or tools for Social Engineering.	N/A
12.	What IT security training your End User has and what does the team require?	Advanced I.C.T Kit training
13.	Please explain what the End User desires to see in a demonstration or in a Proof-of -Concept.	A functioning system
14.	Will the project require a tender process or will be a direct acquisition?	Tender is possible

Confidential 3 / 4

Annex 5: Uganda Customer and Uganda Local Contact forms provided to Hacking Team, May 2015

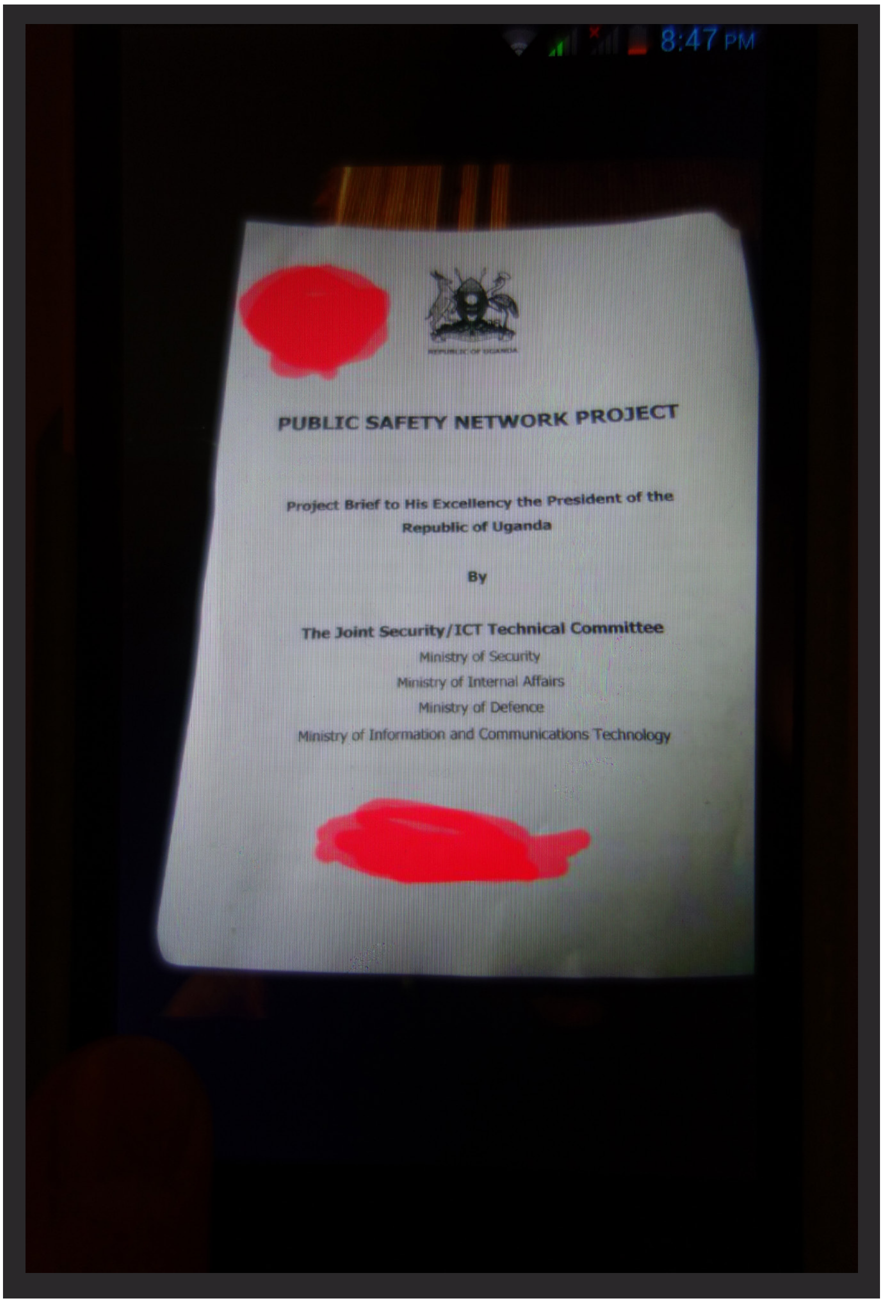


15.	Expected duration of the acquisition process at End User organization.	6 months.

Please provide any other information that will help Hacking Team completely understand the project or potential project and any limitations or special circumstance you foresee in executing the project.

Confidential *4 / 4*

Annex 6: Exerpt From Project Brief on Public Safety Network Project, 2013



[redacted]

REPUBLIC OF UGANDA

PUBLIC SAFETY NETWORK PROJECT

Project Brief to His Excellency the President of the Republic of Uganda

By

The Joint Security/ICT Technical Committee

Ministry of Security

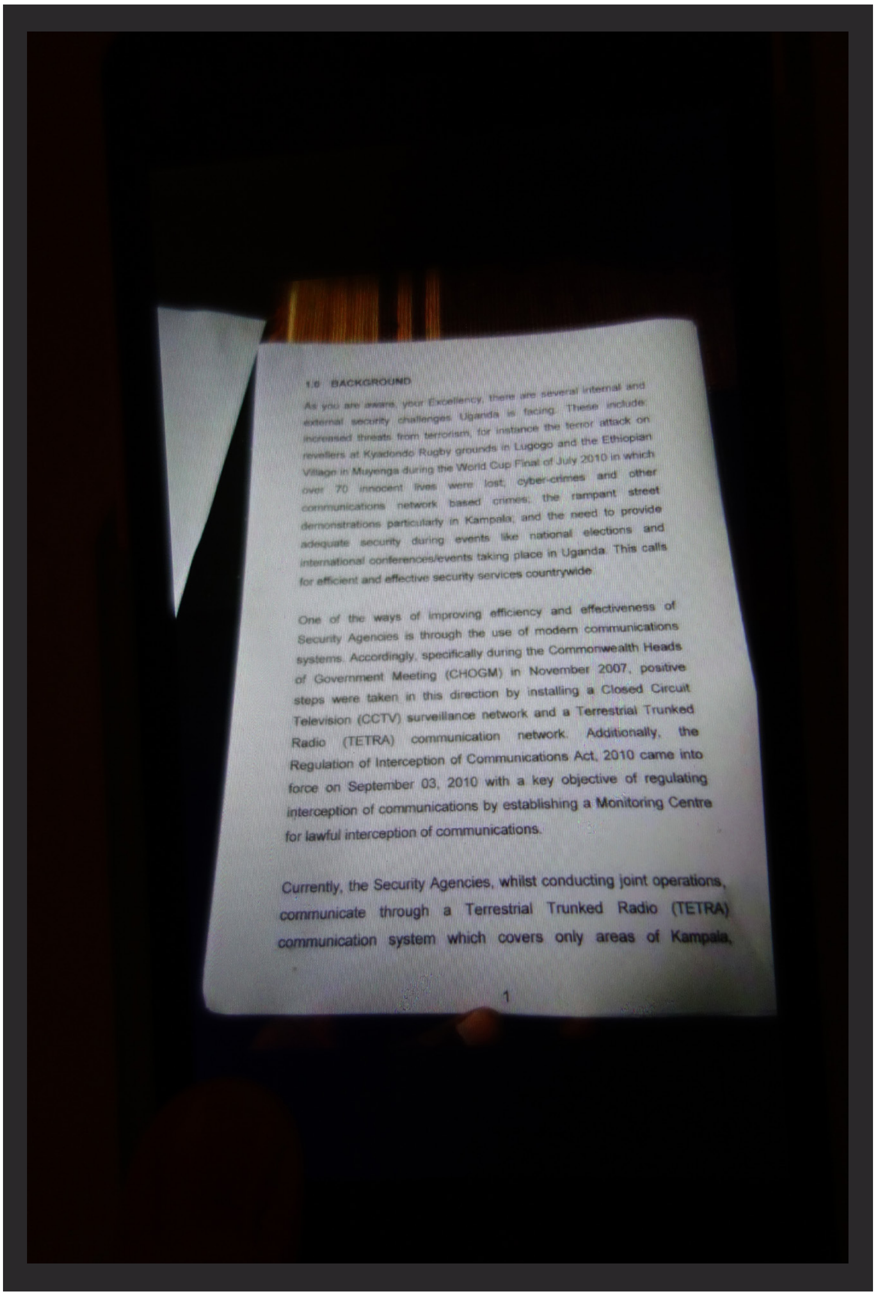
Ministry of Internal Affairs

Ministry of Defence

Ministry of Information and Communications Technology

[redacted]

Annex 6: Excerpt From Project Brief on Public Safety Network Project, 2013



1.0 BACKGROUND

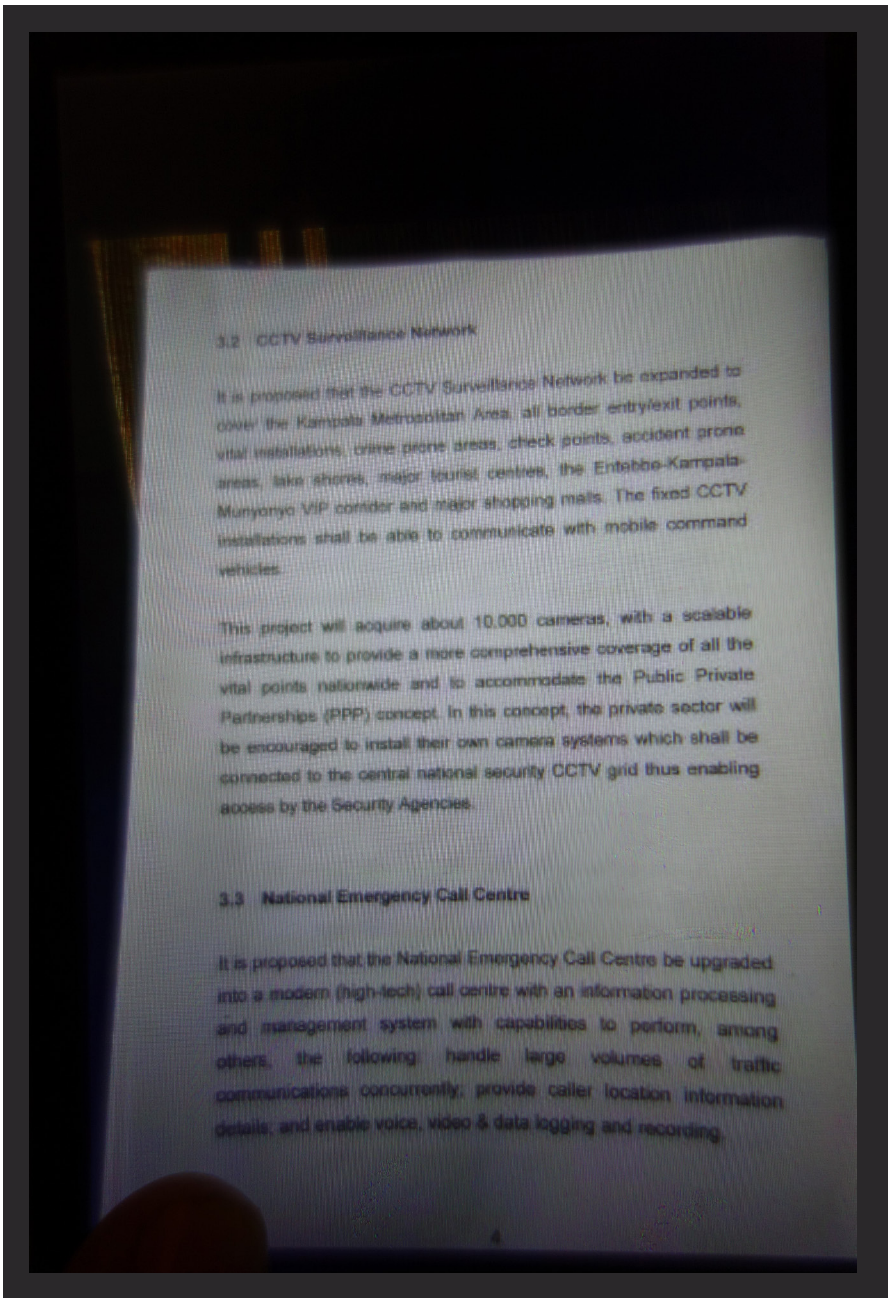
As you are aware, your Excellency, there are several internal and external security challenges Uganda is facing. These include: increased threats from terrorism, for instance the terror attack on revellers at Kyadondo Rugby grounds in Lugogo and the Ethiopian Village in Muyenga during the World Cup Final of July 2010 in which over 70 innocent lives were lost; cyber-crimes and other communications network based crimes; the rampant street demonstrations particularly in Kampala; and the need to provide adequate security during events like national elections and international conferences/events taking place in Uganda. This calls for efficient and effective security services countrywide.

One of the ways of improving efficiency and effectiveness of Security Agencies is through the use of modern communications systems. Accordingly, specifically during the Commonwealth Heads of Government Meeting (CHOGM) in November 2007, positive steps were taken in this direction by installing a Closed Circuit Television (CCTV) surveillance network and a Terrestrial Trunked Radio (TETRA) communication network. Additionally, the Regulation of Interception of Communications Act, 2010 came into force on September 03, 2010 with a key objective of regulating interception of communications by establishing a Monitoring Centre for lawful interception of communications.

Currently, the Security Agencies, whilst conducting joint operations, communicate through a Terrestrial Trunked Radio (TETRA) communication system which covers only areas of Kampala,

1

Annex 6: Excerpt From Project Brief on Public Safety Network Project, 2013



3.2 CCTV Surveillance Network

It is proposed that the CCTV Surveillance Network be expanded to cover the Kampala Metropolitan Area, all border entry/exit points, vital installations, crime prone areas, check points, accident prone areas, lake shores, major tourist centres, the Entebbe-Kampala-Munyonyo VIP corridor and major shopping malls. The fixed CCTV installations shall be able to communicate with mobile command vehicles.

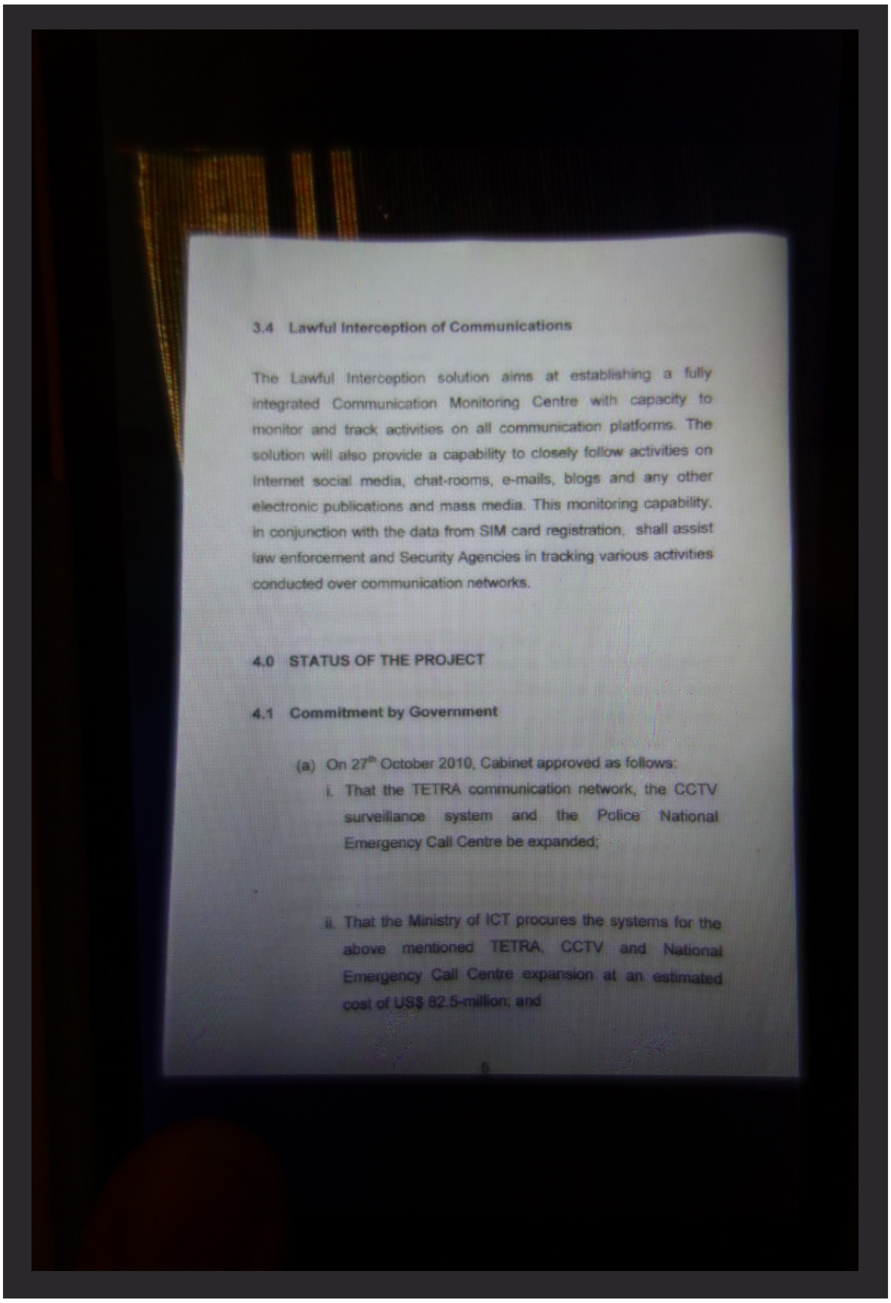
This project will acquire about 10,000 cameras, with a scalable infrastructure to provide a more comprehensive coverage of all the vital points nationwide and to accommodate the Public Private Partnerships (PPP) concept. In this concept, the private sector will be encouraged to install their own camera systems which shall be connected to the central national security CCTV grid thus enabling access by the Security Agencies.

3.3 National Emergency Call Centre

It is proposed that the National Emergency Call Centre be upgraded into a modern (high-tech) call centre with an information processing and management system with capabilities to perform, among others, the following: handle large volumes of traffic communications concurrently; provide caller location information details; and enable voice, video & data logging and recording.

4

Annex 6: Excerpt From Project Brief on Public Safety Network Project, 2013



3.4 Lawful Interception of Communications

The Lawful Interception solution aims at establishing a fully integrated Communication Monitoring Centre with capacity to monitor and track activities on all communication platforms. The solution will also provide a capability to closely follow activities on Internet social media, chat-rooms, e-mails, blogs and any other electronic publications and mass media. This monitoring capability, in conjunction with the data from SIM card registration, shall assist law enforcement and Security Agencies in tracking various activities conducted over communication networks.

4.0 STATUS OF THE PROJECT

4.1 Commitment by Government

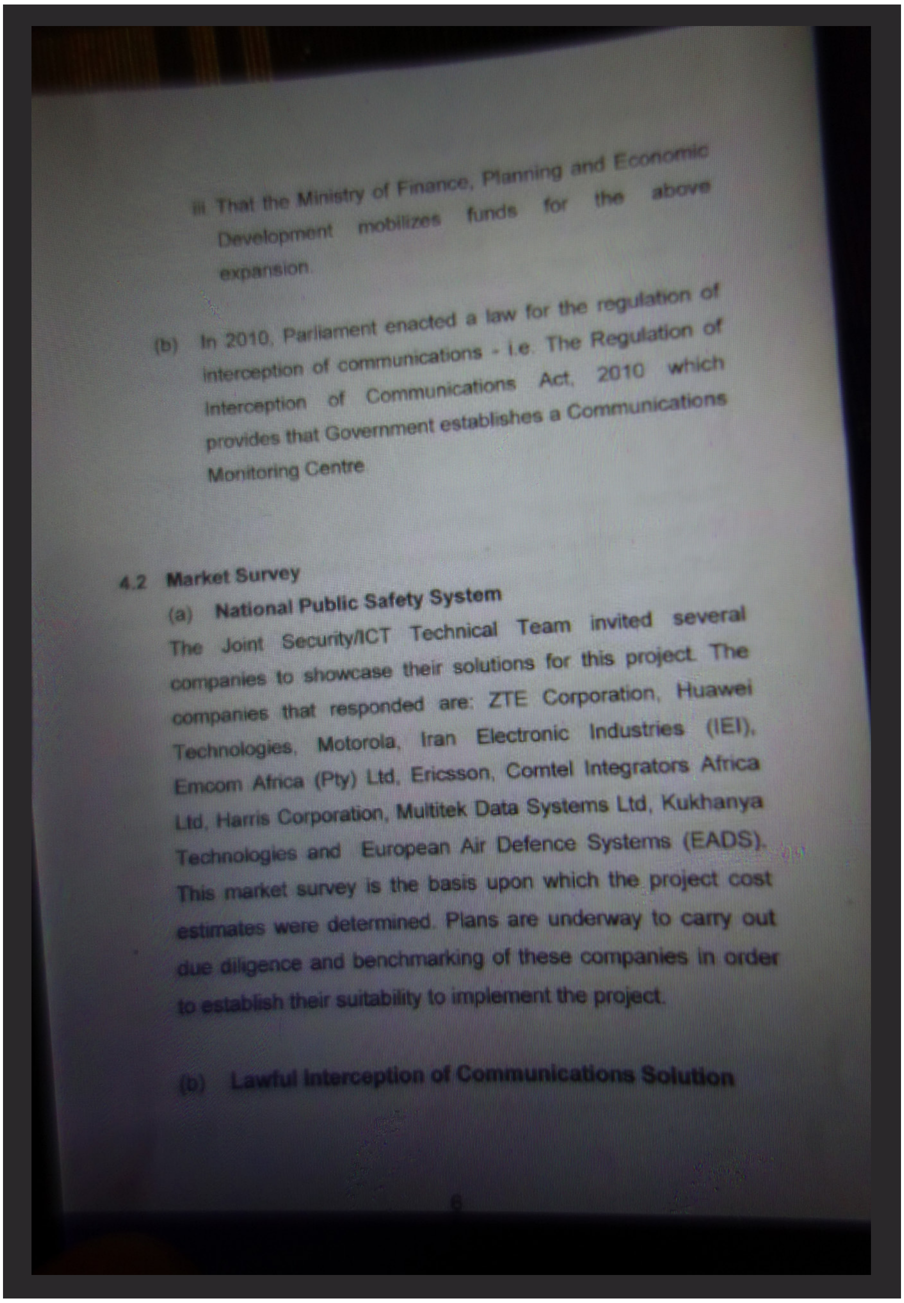
(a) On 27th October 2010, Cabinet approved as follows:

i. That the TETRA communication network, the CCTV surveillance system and the Police National Emergency Call Centre be expanded;

ii. That the Ministry of ICT procures the systems for the above mentioned TETRA, CCTV and National Emergency Call Centre expansion at an estimated cost of US$ 82.5-million; and

5

Annex 6: Excerpt From Project Brief on Public Safety Network Project, 2013



iii. That the Ministry of Finance, Planning and Economic Development mobilizes funds for the above expansion.

(b) In 2010, Parliament enacted a law for the regulation of interception of communications - i.e. The Regulation of Interception of Communications Act, 2010 which provides that Government establishes a Communications Monitoring Centre

4.2 **Market Survey**

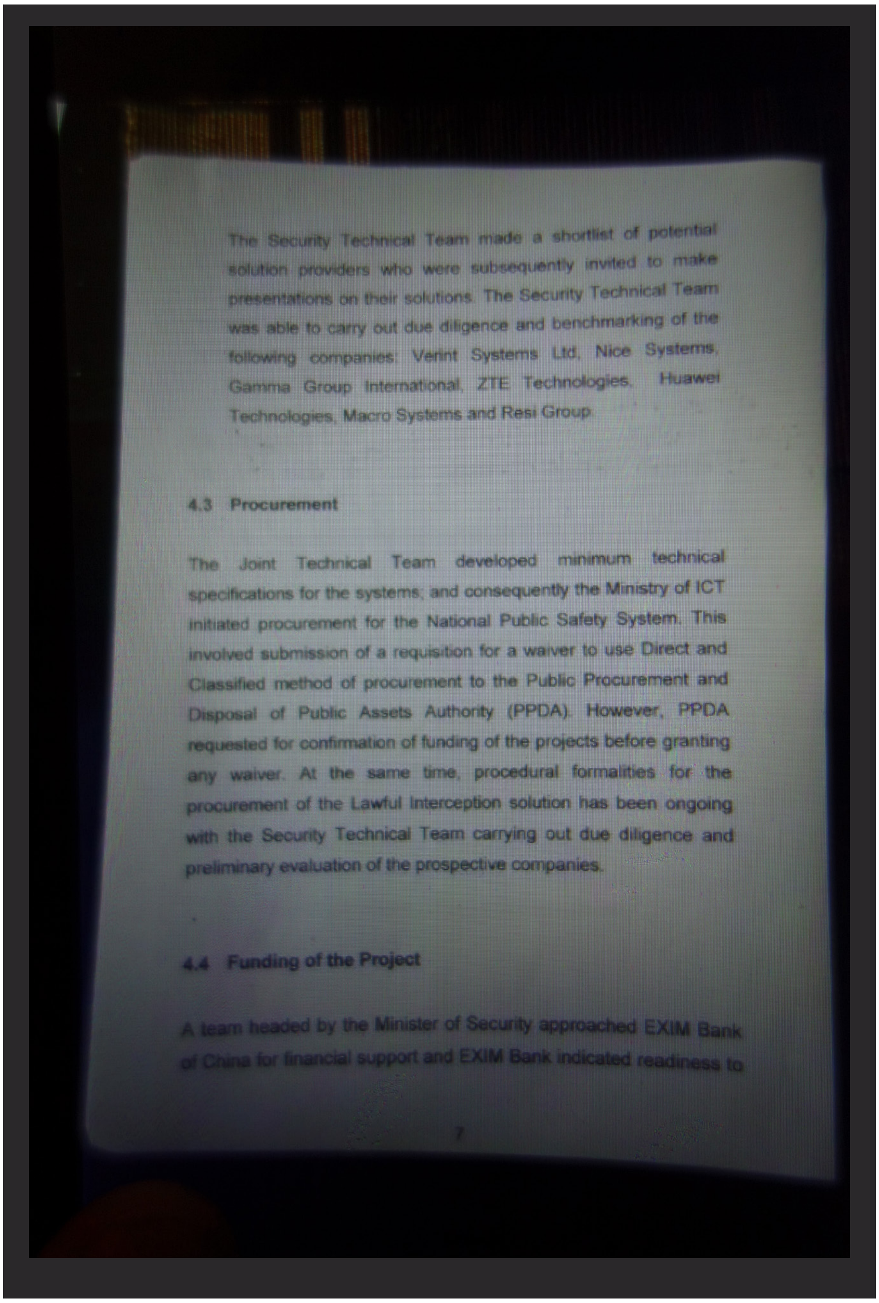
(a) **National Public Safety System**

The Joint Security/ICT Technical Team invited several companies to showcase their solutions for this project. The companies that responded are: ZTE Corporation, Huawei Technologies, Motorola, Iran Electronic Industries (IEI), Emcom Africa (Pty) Ltd, Ericsson, Comtel Integrators Africa Ltd, Harris Corporation, Multitek Data Systems Ltd, Kukhanya Technologies and European Air Defence Systems (EADS). This market survey is the basis upon which the project cost estimates were determined. Plans are underway to carry out due diligence and benchmarking of these companies in order to establish their suitability to implement the project.

(b) **Lawful Interception of Communications Solution**

6

Annex 6: Excerpt From Project Brief on Public Safety Network Project, 2013



The Security Technical Team made a shortlist of potential solution providers who were subsequently invited to make presentations on their solutions. The Security Technical Team was able to carry out due diligence and benchmarking of the following companies: Verint Systems Ltd, Nice Systems, Gamma Group International, ZTE Technologies, Huawei Technologies, Macro Systems and Resi Group.

4.3 Procurement

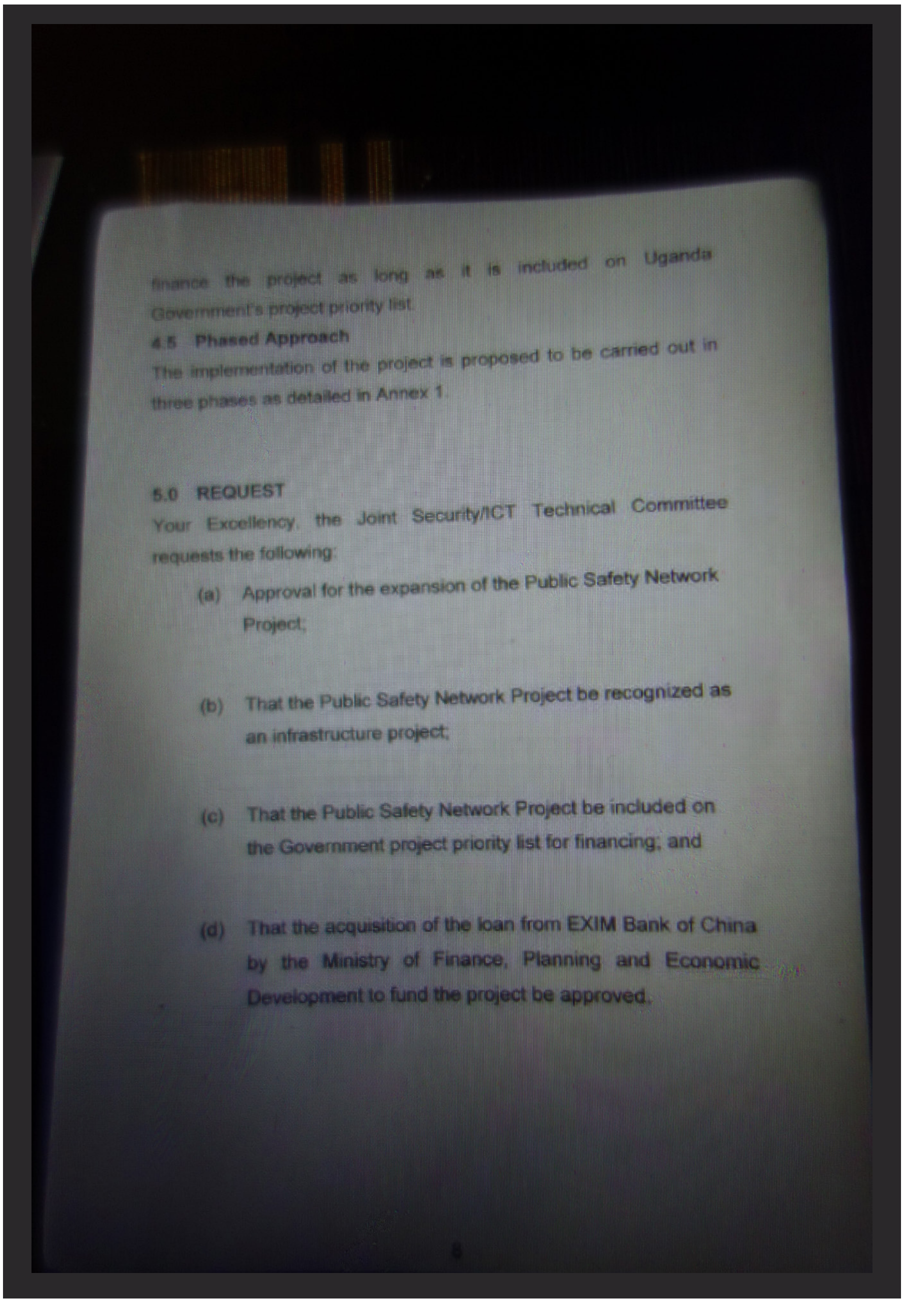
The Joint Technical Team developed minimum technical specifications for the systems; and consequently the Ministry of ICT initiated procurement for the National Public Safety System. This involved submission of a requisition for a waiver to use Direct and Classified method of procurement to the Public Procurement and Disposal of Public Assets Authority (PPDA). However, PPDA requested for confirmation of funding of the projects before granting any waiver. At the same time, procedural formalities for the procurement of the Lawful Interception solution has been ongoing with the Security Technical Team carrying out due diligence and preliminary evaluation of the prospective companies.

4.4 Funding of the Project

A team headed by the Minister of Security approached EXIM Bank of China for financial support and EXIM Bank indicated readiness to

7

Annex 6: Excerpt From Project Brief on Public Safety Network Project, 2013



finance the project as long as it is included on Uganda Government's project priority list.

4.5 Phased Approach

The implementation of the project is proposed to be carried out in three phases as detailed in Annex 1.

5.0 REQUEST

Your Excellency, the Joint Security/ICT Technical Committee requests the following:

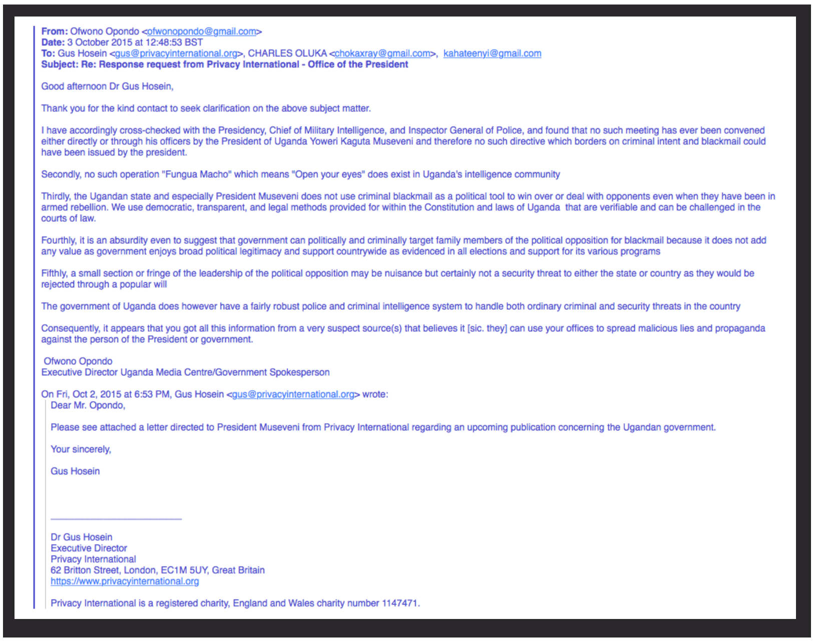
(a) Approval for the expansion of the Public Safety Network Project;

(b) That the Public Safety Network Project be recognized as an infrastructure project;

(c) That the Public Safety Network Project be included on the Government project priority list for financing; and

(d) That the acquisition of the loan from EXIM Bank of China by the Ministry of Finance, Planning and Economic Development to fund the project be approved.

Annex 7: Response from Ofwono Opondo, Uganda Media Centre to Privacy International, October 2015



From: Ofwono Opondo <ofwonopondo@gmail.com>
Date: 3 October 2015 at 12:48:53 BST
To: Gus Hosein <gus@privacyinternational.org>, CHARLES OLUKA <chokaxray@gmail.com>, kahateenyi@gmail.com
Subject: Re: Response request from Privacy International - Office of the President

Good afternoon Dr Gus Hosein,

Thank you for the kind contact to seek clarification on the above subject matter.

I have accordingly cross-checked with the Presidency, Chief of Military Intelligence, and Inspector General of Police, and found that no such meeting has ever been convened either directly or through his officers by the President of Uganda Yoweri Kaguta Museveni and therefore no such directive which borders on criminal intent and blackmail could have been issued by the president.

Secondly, no such operation "Fungua Macho" which means "Open your eyes" does exist in Uganda's intelligence community

Thirdly, the Ugandan state and especially President Museveni does not use criminal blackmail as a political tool to win over or deal with opponents even when they have been in armed rebellion. We use democratic, transparent, and legal methods provided for within the Constitution and laws of Uganda that are verifiable and can be challenged in the courts of law.

Fourthly, it is an absurdity even to suggest that government can politically and criminally target family members of the political opposition for blackmail because it does not add any value as government enjoys broad political legitimacy and support countrywide as evidenced in all elections and support for its various programs

Fifthly, a small section or fringe of the leadership of the political opposition may be nuisance but certainly not a security threat to either the state or country as they would be rejected through a popular will

The government of Uganda does however have a fairly robust police and criminal intelligence system to handle both ordinary criminal and security threats in the country

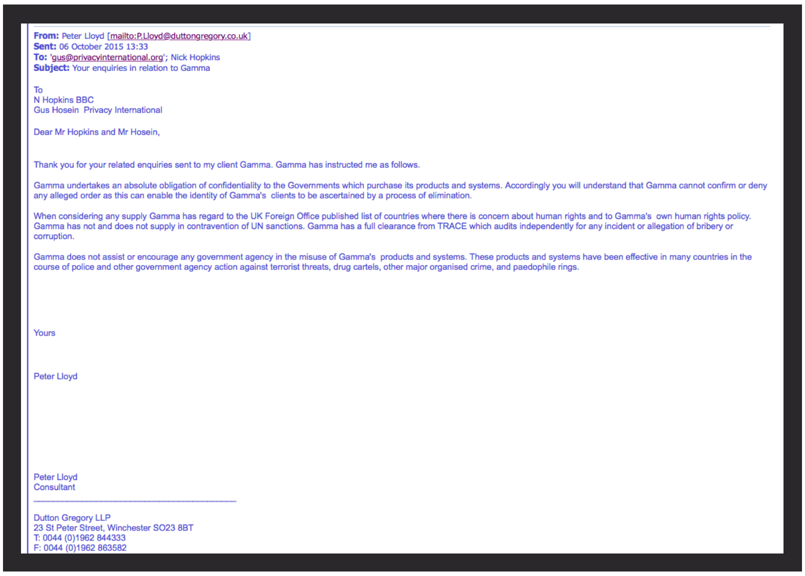
Consequently, it appears that you got all this information from a very suspect source(s) that believes it [sic. they] can use your offices to spread malicious lies and propaganda against the person of the President or government.

Ofwono Opondo
Executive Director Uganda Media Centre/Government Spokesperson

On Fri, Oct 2, 2015 at 6:53 PM, Gus Hosein <gus@privacyinternational.org> wrote:

> Dear Mr. Opondo,
>
> Please see attached a letter directed to President Museveni from Privacy International regarding an upcoming publication concerning the Ugandan government.
>
> Your sincerely,
>
> Gus Hosein
>
> ______________________
>
> Dr Gus Hosein
> Executive Director
> Privacy International
> 62 Britton Street, London, EC1M 5UY, Great Britain
> https://www.privacyinternational.org
>
> Privacy International is a registered charity, England and Wales charity number 1147471.

Annex 8: Response from Gamma Group to Privacy International, October 2015



From: Peter Lloyd [mailto:P.Lloyd@duttongregory.co.uk]
Sent: 06 October 2015 13:33
To: 'gus@privacyinternational.org'; Nick Hopkins
Subject: Your enquiries in relation to Gamma

To
N Hopkins BBC
Gus Hosein Privacy International

Dear Mr Hopkins and Mr Hosein,

Thank you for your related enquiries sent to my client Gamma. Gamma has instructed me as follows.

Gamma undertakes an absolute obligation of confidentiality to the Governments which purchase its products and systems. Accordingly you will understand that Gamma cannot confirm or deny any alleged order as this can enable the identity of Gamma's clients to be ascertained by a process of elimination.

When considering any supply Gamma has regard to the UK Foreign Office published list of countries where there is concern about human rights and to Gamma's own human rights policy. Gamma has not and does not supply in contravention of UN sanctions. Gamma has a full clearance from TRACE which audits independently for any incident or allegation of bribery or corruption.

Gamma does not assist or encourage any government agency in the misuse of Gamma's products and systems. These products and systems have been effective in many countries in the course of police and other government agency action against terrorist threats, drug cartels, other major organised crime, and paedophile rings.

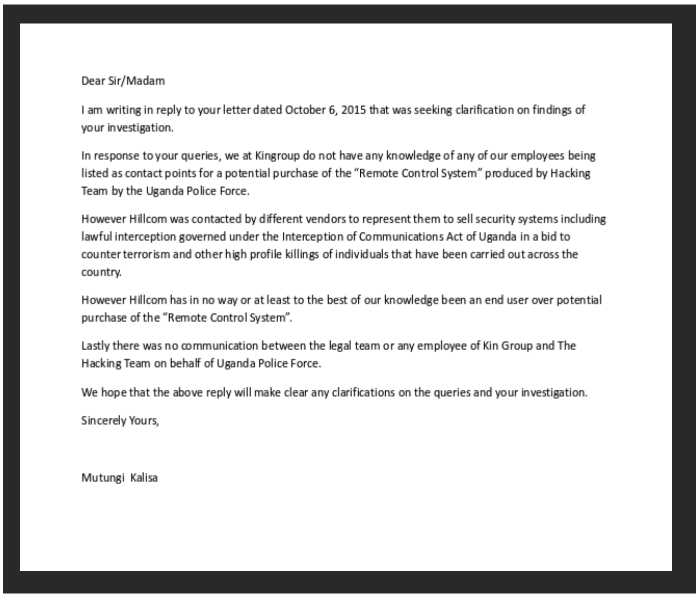
Yours

Peter Lloyd

Peter Lloyd
Consultant
____

Dutton Gregory LLP
23 St Peter Street, Winchester SO23 8BT
T: 0044 (0)1962 844333
F: 0044 (0)1962 863582

Annex 9: Responses from companies contacted by Privacy International, October 2015 | Response from Kin Group



Dear Sir/Madam

I am writing in reply to your letter dated October 6, 2015 that was seeking clarification on findings of your investigation.

In response to your queries, we at Kingroup do not have any knowledge of any of our employees being listed as contact points for a potential purchase of the "Remote Control System" produced by Hacking Team by the Uganda Police Force.

However Hillcom was contacted by different vendors to represent them to sell security systems including lawful interception governed under the Interception of Communications Act of Uganda in a bid to counter terrorism and other high profile killings of individuals that have been carried out across the country.

However Hillcom has in no way or at least to the best of our knowledge been an end user over potential purchase of the "Remote Control System".

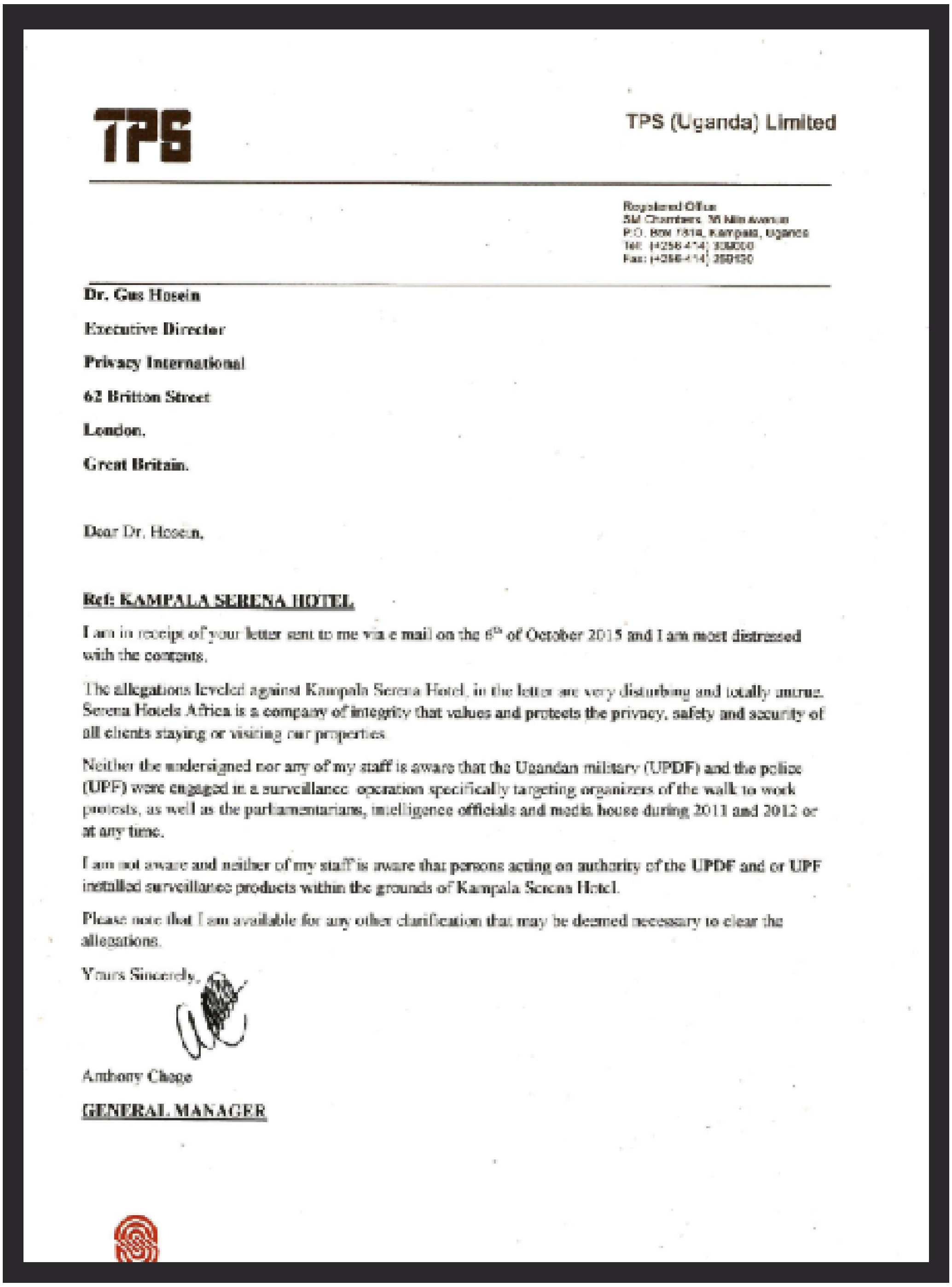
Lastly there was no communication between the legal team or any employee of Kin Group and The Hacking Team on behalf of Uganda Police Force.

We hope that the above reply will make clear any clarifications on the queries and your investigation.

Sincerely Yours,

Mutungi Kalisa

Annex 9: Responses from companies contacted by Privacy International, October 2015 | Response from Serena



TPS

TPS (Uganda) Limited

Registered Office
SM Chambers, 36 Nile Avenue
P.O. Box 7814, Kampala, Uganda
Tel: (+256 414) 309000
Fax: (+256 414) 259130

Dr. Gus Hosein

Executive Director

Privacy International

62 Britton Street

London,

Great Britain.

Dear Dr. Hosein,

<u>Ref: KAMPALA SERENA HOTEL</u>

I am in receipt of your letter sent to me via e mail on the 6th of October 2015 and I am most distressed with the contents.

The allegations leveled against Kampala Serena Hotel, in the letter are very disturbing and totally untrue. Serena Hotels Africa is a company of integrity that values and protects the privacy, safety and security of all clients staying or visiting our properties.

Neither the undersigned nor any of my staff is aware that the Ugandan military (UPDF) and the police (UPF) were engaged in a surveillance operation specifically targeting organizers of the walk to work protests, as well as the parliamentarians, intelligence officials and media house during 2011 and 2012 or at any time.

I am not aware and neither of my staff is aware that persons acting on authority of the UPDF and or UPF installed surveillance products within the grounds of Kampala Serena Hotel.

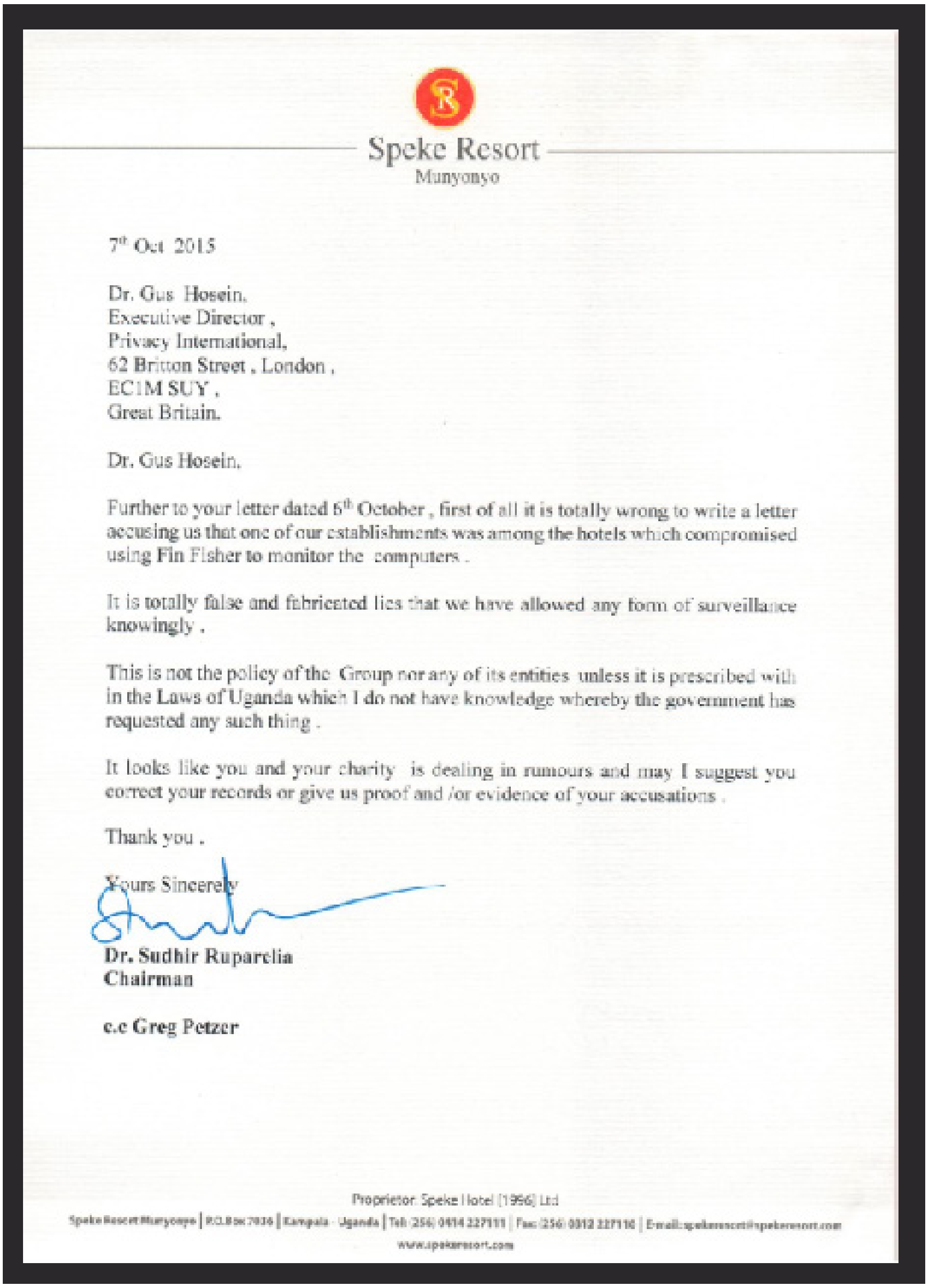
Please note that I am available for any other clarification that may be deemed necessary to clear the allegations.

Yours Sincerely,

Anthony Chege

<u>GENERAL MANAGER</u>

Annex 9: Responses from companies contacted by Privacy International, October 2015 | Response from Ruparelia



Speke Resort
Munyonyo

7th Oct 2015

Dr. Gus Hosein,
Executive Director ,
Privacy International,
62 Britton Street , London ,
EC1M SUY ,
Great Britain.

Dr. Gus Hosein,

Further to your letter dated 6th October , first of all it is totally wrong to write a letter accusing us that one of our establishments was among the hotels which compromised using Fin Fisher to monitor the computers .

It is totally false and fabricated lies that we have allowed any form of surveillance knowingly .

This is not the policy of the Group nor any of its entities unless it is prescribed with in the Laws of Uganda which I do not have knowledge whereby the government has requested any such thing .

It looks like you and your charity is dealing in rumours and may I suggest you correct your records or give us proof and /or evidence of your accusations .

Thank you .

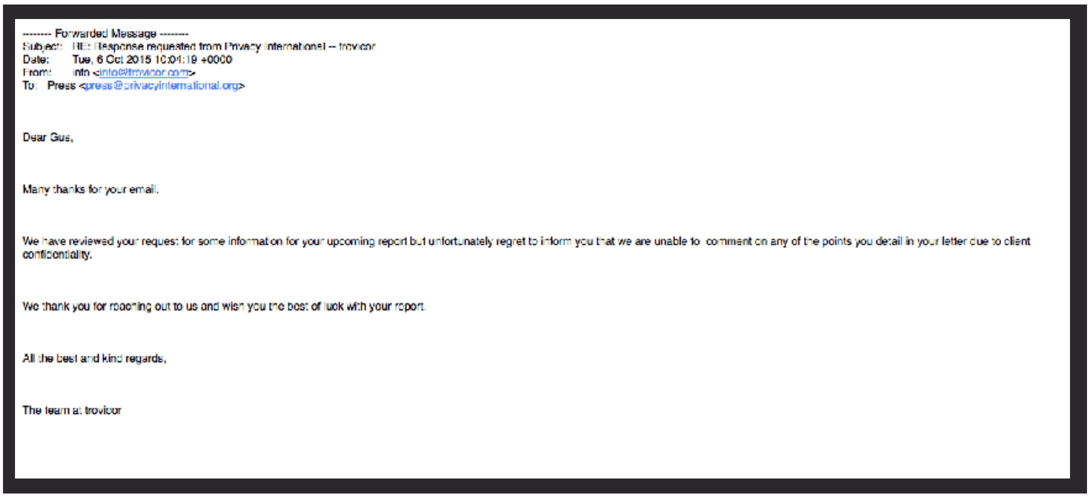
Yours Sincerely

Dr. Sudhir Ruparelia
Chairman

c.c Greg Petzer

Proprietor: Speke Hotel [1996] Ltd
Speke Resort Munyonyo | P.O.Box 7036 | Kampala - Uganda | Tel: (256) 0414 227111 | Fax: (256) 0312 227110 | E-mail: spekeresort@spekeresort.com
www.spekeresort.com

Annex 9: Responses from companies contacted by Privacy International, October 2015 | Response from Trovicor



-------- Forwarded Message --------
Subject: RE: Response requested from Privacy International -- trovicor
Date: Tue, 6 Oct 2015 10:04:19 +0000
From: info <info@trovicor.com>
To: Press <press@privacyinternational.org>

Dear Gus,

Many thanks for your email.

We have reviewed your request for some information for your upcoming report but unfortunately regret to inform you that we are unable to comment on any of the points you detail in your letter due to client confidentiality.

We thank you for reaching out to us and wish you the best of luck with your report.

All the best and kind regards,

The team at trovicor