PRIVACY INTERNATIONAL

Report

Briefing for the Italian Government on Hacking Team's surveillance exports

Introduction

For more than a decade, Italian surveillance company Hacking Team has sold invasive surveillance technologies to law enforcement and intelligence agencies across the globe.[1] Its flagship product, the "Remote Control System" (RCS), is marketed by Hacking Team as an "effective, easy-to-use offensive technology" that it provides to "worldwide law enforcement and intelligence communities."[2] Hacking Team has a consistent track record of delivering its software, including the RCS, to government agencies with records of human rights abuse and unlawful surveillance, and its products have been repeatedly used to conduct unlawful surveillance of journalists, activists and human rights defenders.

This briefing canvasses Hacking Team's products and customer base. It's release coincides with the publication of new evidence, uncovered by Privacy International, and an independent investigation by VICE Motherboard, that Hacking Team has sold its Remote Control System to the United States Army and the Drug Enforcement Agency (DEA).

Since 2012, Hacking Team software has been identified and associated with attacks on political dissidents, journalists and human rights defenders, and evidence has been published confirming its suspected deployment in at least 21 countries. However, when presented with compelling evidence of the deployment of its products by human rights abusing governments, Hacking Team has consistently chosen to 'neither confirm nor deny' allegations, ignoring demands for transparency about its customer base, and disregarding victims' claims for redress against offenders.

In publishing this briefing, Privacy International consolidates for the first time research on Hacking Team that it has compiled over four years of investigations and campaigning. The release of this briefing is particularly timely as it comes only months after European law was amended to restrict the export of Hacking Team's RCS product, subjecting the Italian company to strict licensing requirements designed to prevent its invasive technologies from falling into the wrong hands.

---

1 http://www.hackingteam.it/index.php/about-us

2 http://www.hackingteam.it/index.php/about-us : http://www.hackingteam.it/index.php/remote-control-system

Origins and growth

Hacking Team traces its beginnings to 2001, when two Italian computer programmers created the Ettercap programme, designed to facilitate man-in-the-middle attack.[3] The Italian Police quickly realized the programme's potential for surveillance operations against common encrypted communication services such as Skype, e-mail, instant messaging, webcams and computer audio systems,[4] and became one of Hacking Team's first customers.

Hacking Team has benefited considerably from its connections with Italian public authorities. The company received over €1 million in public financing from the Region of Lombardy.[5] Recently, the Italian government tabled legislation designed to explicitly empower its agencies to use Remote Control Systems. The counter-terrorism decree was subsequently blocked by opposition in Parliament, but would have become the first European legislation permitting the use of such systems had it been converted into law.[6]

Today, Hacking Team, lead by CEO David Vincenzetti, has over 50 staff, and subsidiaries in Annapolis, United States of America, and in Singapore. It sells its services and products to law enforcement and intelligence agencies across the globe.[7]

Technology and services

Hacking Team's flagship product is the Remote Control System software. In the company's words:

> *RCS (Remote Control System) is a solution that supports investigations by actively and passively tapping data and information from the devices targeted by the investigations. In fact, TCS anonymously, creates, sets and installs software agents that collect data and information, sending the results to the central database to be decrypted and saved.*[8]

3 http://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers

4 http://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers: https://www.privacyinternational.org/?q=node/147

5 https://www.privacyinternational.org/?q=node/147

6 http://in.reuters.com/article/2015/03/26/italy-security-internet-idINKBN0MM24620150326

7 http://www.hackingteam.it/index.php/about-us : https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

8 https://s3.amazonaws.com/s3.documentcloud.org/documents/1348003/rcs-9-admin-final.pdf

The two main RCS systems currently marketed by Hacking Team are the "DaVinci" and "Galileo" solutions.[9] These products are intrusion technologies that can covertly collect, modify and/or extract data from a device through the installation of malicious software on the device. The malware is inserted on the computer as a trojan, or a malicious code disguised in inconspicuous files or attachments, and is executed on the device. The malicious code can run operations in a clandestine manner on the device, making it undetectable by the users of the device.[10]

These solutions are capable of bypassing encryption in common communications services software, and of logging Skype calls, emails, instant messaging, web browsing records, deleted files and shots taken from the computer's own webcam. The company claims that their product not only relays what is happening on a target's computer, but also enables surveillance of anything occurring within the range of the computer's internal camera or microphone. Hacking Team also claims to be able to compromise computers running Mac OS and Windows, in addition to a range of smartphones.[11] The malware is delivered through man-in-the-middle-attacks, i.e. disguised as requests to common updates, and through social engineering, i.e disguised as attachments to e-mails.

Contribution to human rights abuses

Evidence suggests that Hacking Team's RCS is one of the most popular intrusion technologies on the market, and is used widely by countries with poor human rights records. However, when presented with compelling evidence of the deployment of its products by human rights abusing governments, Hacking Team has consistently chosen to 'neither confirm nor deny' allegations, ignoring demands for transparency about its customer base, and disregarding victims' claims for redress against offenders.

Since 2012, Hacking Team software has been identified and associated with attacks on political dissidents, journalists and human rights defenders, and evidence has been published confirming its suspected deployment in at least 21 governments, spanning six

9 http://www.hackingteam.it/index.php/remote-control-system

10 https://www.privacyinternational.org/?q=node/73

11 http://www.cso.com.au/article/431882/_crisis_os_x_trojan_made_by_lawful_intercept_vendor_hackingteam/

contents.[12] It is suspected, however, that Hacking Team's customer base is actually much larger, and the company's intelligence tools may be in use in more than 60 countries.[13]

Citizen Lab at the University of Toronto has, in cooperation with Claudio Guarnieri, identified the following governments as suspected users[14] of Hacking Team software:

Azerbaijan	Colombia	Egypt	Ethiopia
Hungary	Italy	Kazakhstan	Malaysia
Mexico	Morocco	Nigeria	Oman
Panama	Poland	Saudi Arabia	South Korea
Sudan	Thailand	Turkey	United Arab Emirates
Uzbekistan			

Three of Hacking Team's clients – Uzbekistan, Saudi Arabia and Sudan – are ranked as "the worst of the worst" in terms of freedom, Freedom House's 2015 Freedom in the World index.[15] Another three of the clients – Colombia, Mexico and Turkey – are on the Committee for the Protection of Journalists "20 Deadliest Countries" list in ranking attacks on journalists.[16] Additionally, several of Hacking Team's clients have a history of human rights abuse linked to surveillance and intelligence technologies, as detailed below.

Azerbaijan

Citizen Lab "identified an RCS endpoint in Azerbaijan (Azertelekom: 109.235.193.83) that was active between June and November 2013."[17]

Azerbaijan is one of the Central Asian states with the most serious history of arresting bloggers, and those using information and communications technologies.[18] Freedom House observes that Azerbaijani authorities rely on sweeping investigatory powers that

12 A Citizen lab map of hacking Team proliferation is annexed to this report. See Annex III https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/
13 http://www.wired.com/2014/06/remote-control-system-phone-surveillance/
14 https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/
15 https://freedomhouse.org/report/freedom-world/freedom-world-2015#.VSaUezvF8Yc
16 https://cpj.org/killed/
17 https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/
18 https://freedomhouse.org/report/freedom-net/2012/azerbaijan#.VSenQTvF8Yd

leaving substantial leeway for abuse of powers:

> *"The law "On operative-search activity" (Article 10, section IV) authorizes law enforcement agencies to conduct surveillance without a court order in cases regarded as necessary "to prevent serious crimes against the person or especially dangerous crimes against the state." The unclear parameters for what constitutes preventive action leave the law open to abuse."*[19]

Government agencies in Azerbaijan have increasingly invested in surveillance technologies, while implementing methods of blanket surveillance on mobile phone users, and consistently targeting foreigners and activists with invasive surveillance tools.[20]

Ethiopia

In 2014, investigations by Citizen Lab revealed that an independent Ethiopian media outlet in the United States, the Ethiopian Satellite Television Service, had been attacked with spyware on several occasions.[21] Citizen Lab concluded that the attack to obtain "files and passwords, and intercept Skype calls and instant messages" could be attributed to the use of software "sold exclusively to governments by Milan-based Hacking Team."[22] Both the results of the investigations and the Ethiopian Government's previous conflicts with the Television Service indicate that Ethiopian intelligence agencies staged the attack, using RCS.

Kazakhstan

RCS technology has been traced to telecommunications company JSC Kazakhtelecom Slyzhebnyi.[23] In at 2014 report, Human Rights Watch noted that "Kazakhstan's poor human rights record continued to deteriorate in 2013,"[24] citing as a cause overly broad laws that allow for the suppression of free speech, dissent, and freedom of assembly and religion. In 2011, national unrest triggered a crack-down from security forces where civil society activists and prominent members of the political opposition were

19 https://freedomhouse.org/report/freedom-net/2012/azerbaijan#.VS5gfxOUdHg
20 See also https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/#12
21 https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/; https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/
22 https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/
23 https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/#12
24 "Human Rights Watch World Report 2014", Human Rights Watch, 2014, available at http://www.hrw.org/sites/default/files/wr2014_web_0.pdf

imprisoned. Opposition groups and independent media outlets and journalists were harassed, and often forced to close.[25] Torture remains commonplace in the country.[26] As recently as 2014, testimonies were submitted to the UN Committee Against Torture, alleging that Kazakh intelligence agencies have perpetrated 37 counts of ill-treatment and coerced testimonies.[27]

Morocco

The Economist's Intelligence Units 2014 Democracy Index classifies Morocco as an authoritarian regime. In a recent report by Privacy International, *Their eyes on me: stories of surveillance in Morocco,*[28] it has been found that Morocco has aggressively increased its surveillance capacity since 2011.[29] The report includes testimonies from several journalists and human rights workers who have been subject to attacks from "hacking militias" that are suspected to have connections with the Moroccan intelligence community. As recently as 2012, the "Mamkfinch" website and Global Voices (a citizen media platform) staff were targeted with Hacking Team software.[30]

United Arab Emirates

Reporters Without Borders has observed that the UAE has been implementing internet surveillance and censorship programs since 2008,[31] underpinned by legislation suppressing communications "'opposing Islam,' 'insulting any religion recognised by the state' or 'contravening family values and principles.'"[32] Specifically, UAE use of RCS technology has been tied to the arrest of blogger Ahmad Mansoor in 2011 on charges of insulting the President and Crown Prince.[33]

---

25 "Amnesty International Report 2013: The state of the world's human rights", Amnesty International, 2013, available at http://files.amnesty.org/air13/AmnestyInternational_AnnualReport2013_complete_en.pdf

26 "Human Rights Watch World Report 2014", Human Rights Watch, 2014, available at http://www.hrw.org/sites/default/files/wr2014_web_0.pdf

27 "Kazakhstan: Submission to the UN Committee Against Torture", Human Rights Watch, October 2014, available at http://www.hrw.org/news/2014/10/20/kazakhstan-submission-un-committee-against-torture

28 https://www.privacyinternational.org/?q=node/554

29 https://www.privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English_0.pdf

30 Pg 16-19 https://www.privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English_0.pdf

31 http://en.rsf.org/surveillance-united-arab-emirates,39760.html

32 http://en.rsf.org/surveillance-united-arab-emirates,39760.html

33 https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

Uzbekistan

Digital forensic investigations suggest the deployment of Hacking Team technologies at Sarkor Telecom, in Uzbekistan.[34]

Numerous journalists and activists living in Uzbekistan and outside of it, in exile, report that their communications have been monitored. Uzbek authorities appear to be monitoring phones calls and emails of Uzbeks working on what state authorities perceive to be politically sensitive topics, often using transcripts of private communications in criminal proceedings against them. In some cases, authorities also appear to have obtained access to VoIP communications such as Skype. While the methods and stories vary, the accounts evidence the politically-motivated nature of surveillance in Uzbekistan. Human rights activists and journalists are targeted where they are considered a viable threat to the regime.[35]

Privacy International's recent report *Private Interests: Monitoring Central Asia*[36]) details testimonies of individuals that suggest that the Uzbek intelligence community has targeted persons communicating human rights concerns to UN bodies and the international human rights community on numerous occasions since 2005. As late as 2013, Uzbek intelligence agencies spied on private and confidential communications, carried over encrypted Skype links, between families of arrested dissidents and human rights lawyers.[37]

Saudi Arabia

Citizen Lab has traced the use of RCS software in Saudi Arabia to Etihad Etisalat and Al-Khomasia Shipping & Maintenance Co Ltd.[38]

According to Freedom House, Saudi Arabia has implemented surveillance and censorship programmes resulting in "notable political censorship".[39] A Freedom House report notes:

34 https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/#12
35 PG 68-70 https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf
36 https://www.privacyinternational.org/?q=node/293
37 https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf
38 https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/#12
39 https://freedomhouse.org/report/freedom-net/2012/saudi-arabia#.VSfPtzvF8Yc

> *"Surveillance is rampant in Saudi Arabia. Anyone who uses communication technology is subject to government monitoring, which is officially justified under the auspices of protecting national security and maintaining social order. The authorities regularly monitor websites, blogs, chat rooms, social media sites, and the content of email and mobile phone text messages."*[40]

Surveillance technologies have also been used to identify and detain women's rights activists.[41] In 2014, Citizen Lab uncovered that Hacking Team malware had been packaged with news applications aimed at the Shia minority in Saudi Arabia.[42]

Sudan

Investigations by Citizen Lab has traced the use of RCS software to VisionValley in Sudan.[43]

The Association for Progressive Communications has observed that Sudan uses censorship and surveillance technologies with an aim of suppressing non-Islamic norms and government opposition.[44] Hacking Team technologies have been used by the Sudanese Government's "Cyber Jihadist Unit" since 2011 to target "government opponents, journalists, human rights activists and various youth groups."[45]

Complicity in potentially unlawful US surveillance

Investigations by Privacy International, published today by VICE, reveal that Hacking Team has sold its Remote Control System to the Drug Enforcement Agency and US military via a front company based in the US.[46]

Records show that in 2011, a company called Cicom, with a registered address identical to that at which Hacking Team's US office is registered (1997 Annapolis Exchange Parkway Suite 30x), sold a "Remote Control System", originating in Italy, to the US Army for USD $350,000.[47]

---

40 https://freedomhouse.org/report/freedom-net/2012/saudi-arabia#.VSfPtzvF8Yc
41 https://freedomhouse.org/report/freedom-net/2012/saudi-arabia#.VSfPtzvF8Yc
42 https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/
43 https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/#12
44 http://www.apc.org/en/blog/online-surveillance-and-censorship-sudan
45 http://www.apc.org/en/blog/online-surveillance-and-censorship-sudan
46 https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.4.4&s=FPDSNG.COM&q=CICOM
47 Annex IV

Only months later, in March 2012, the DEA released a call for tender for a "Remote Control Host Based Interception System":

> *"The DEA is seeking information from potential sources with a fully functional and operational product proven to be capable of providing a Remote Control Host Based Interception System for device or target specific collection pursuant to authorized law enforcement use."*[48]

In August 2012, the DEA's Office of Investigative Technology paid an initial USD$575,000 of an All Options Value of USD$2,410,000 to Cicom, and has continued to pay annual installments to the company. The most recent record shows a transaction, effective in August 2014 and to be completed in August 2015, for a "*Remote Control Host Based Interception System and support services*".[49] The transactions are due to end in 2017.

The transfers come in the wake of recent revelations of the DEA's mass surveillance programme, through which the agency has been collecting and storing the telephone records of ordinary Americans for more than two decades.[50] It is now clear that, in addition to such bulk collection practices, the DEA also possesses the technical capacity to conduct intrusive surveillance on individuals across the globe, using Hacking Team's products. Whether law enforcement use of intrusive surveillance is lawful in the US is not clear, as some courts have refused to issue warrants authorising such activities.

Internal due diligence – is it enough?

Privacy International believes that under no circumstances should Hacking Team provide its products and services to government end-users when there is a likelihood that those products will be used for unlawful surveillance or other human rights abuses. Nor should products such as the RCS ever be deployed by, and thus sold to, government agencies in the absence of rigorous legal frameworks and oversight regimes.

48 https://www.fbo.gov/index?s=opportunity&mode=form&id=7eb60b154c178c5a0abd3d5dfbba2709&tab=core&_cview=0

49 Annex V

50 https://firstlook.org/theintercept/2015/04/08/dea-surveillance-phone-records-crisscross-nsa/

Export of a product like the RCS to the United States raises a number of critical questions about the role of companies like Hacking Team in facilitating unlawful surveillance. There is unclear statutory authority authorising the deployment of spyware by US federal or law enforcement agencies, meaning that deployment of the RCS by the DEA or the Army is potentially unlawful under US law. Furthermore, because RCS is designed to be usable against targets even while they are outside of the end-user's legal jurisdiction, it raises serious legal questions concerning the ability of US agencies and the military to target individuals based outside of the United States. Companies' internal due diligence policies that do not take into account that their customer cannot lawfully use their products are inherently problematic, and ultimately inadequate to properly prevent against human rights violations.

In its branding and communications materials, Hacking Team claims to have understanding of the "potential for abuse of the surveillance technologies" and asserts that it enforces a precautionary approach in managing its services.[51] Eric Rabe, Hacking Team's Chief Marketing and Communications Officer has asserted that Hacking Team goes "further than any other company to address the concerns of human rights organizations and Citizen Lab not only through our own policies but also by complying with international standards including the Wassenaar Arrangement protocols."[52]

The Hacking Team Customer Policy details a number of measures[53] to minimize the risk of human rights abuse, including conducting sales reviews with a "panel of technical experts and legal advisors" and monitoring the human rights record of potential clients; implementing training that allows Hacking Team employees identify "red flags" according to the U.S. Commerce and Foreign Trade "Know Your Customer" Guidance;[54] and inserting conditionality clauses in sales agreements requiring legal compliance with applicable laws. Nevertheless, these internal processes are not by themselves sufficient to prevent the sale of invasive products such as the RCS to

51 http://www.hackingteam.it/index.php/customer-policy

52 HackingTeam Response to Citizen Lab Report of March 9, 2015: http://www.hackingteam.it/index.php/about-us

53 The complete Customer Policy is appended to this report. See also Customer Policy http://www.hackingteam.it/index.php/customer-policy

54 http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=b598042103e95c10c396b0140e0620b7&rgn=div9&view=text&node=15:2.1.3.4.21.0.1.7.22&idno=15

government agencies with a history of potentially unlawful surveillance, nor to stop the sale of such systems to governments with grave histories of human rights abuse. Thus, Hacking Team's internal due diligence process, to the extent they exist, are woefully inadequate to ensure that the company is not complicit in human rights violations.

A first step: regulation of exports

The profit model of companies such as Hacking Team is the provision of incredibly intrusive products and services to law enforcement and intelligence agencies across the world, who use them for both legitimate, and unlawful, surveillance of their populations. Although the company has basic internal due diligence policies, these policies appear not to have prevented the export of intrusion technology to some of the world's worst human rights abusers, and to government agencies with histories of unlawful surveillance. Key to controlling the proliferation of this technology, therefore, are regulations which require companies such as Hacking Team to obtain licences prior to exporting their products and services.

As an Italian company, Hacking Team's technologies are now subject to European Union export restrictions. As of 1 January 2015, the EU Dual-Use Regulation 429/2008 restricts the export of intrusion software, defined in a manner that captures the RCS. The EU developments are grounded in agreements made at a 2013 convening of States parties to the Wassenaar Arrangement, an intergovernmental export control regime used to determine which items should be subjected to export licensing by its participatory states in order to foster international security.[55] The inclusion of the category relating to intrusion software was instigated by the United Kingdom in 2012, after campaigning by Privacy International and others, motivated by increasing evidence that intrusion technologies were being exported to authoritarian states with poor human rights records and being used to target activists.

As of January 2015, Hacking Team has asserted its immediate compliance with the EU regulation, and has undertaken to seek authorization for exports under the Italian Ministry of Economic Development.[56] However, although the technology is now subject to

55 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF

56 The complete Hacking team news release on its compliance with export regimes is appended to this report. See also: HackingTeam Complies with Wassenaar Arrangement Export Controls on Surveillance and Law Enforcement/Intelligence Gathering Tools http://www.hackingteam.it/index.php/about-us

licensing, it is incumbant on the Italian authorities to appropriately assess whether or not a transfer should be authorised. As a first step, the authorities should consider the eight common criteria for arms exports already in place within the EU common position on arms exports.[57]

In addition to this, the authorities must also look at the legal framework which regulates the use of the technology in question in the destination country, the record of the end-user and how it uses intelligence, as well as the potential of the proposed technology to be used against the principles established within the European Covenant on Human Rights.

Conclusion

Hacking Team's RCS is one of the most widely documented and reported surveillance technologies on the market. While the company has repeatedly stipulated that it respects human rights and has internal procedures in place to ensure that their products are not used for human rights violations, it is not enough to rely on self-regulation. The imposition of effective export regulations with appropriate and strong human rights provisions is an essential step in ensuring that the sale of RCS and similar technology is accountable, more transparent, and that it ultimately does not lead to human rights abuses.

Privacy International is currently secretariat for an international NGO campaign calling for effective, human rights-based, export controls to be put into place to stop exports of surveillance technology which pose a threat to fundamental human rights. More information on the Coalition Against Unlawful Surveillance Exports can be found at http://www.globalcause.net/.

57 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF

Annex I: Hacking Team "Customer Policy"[58]

Customer Policy
Since we founded Hacking Team, we have understood the power of our software in law enforcement and intelligence investigations.

We also understand the potential for abuse of the surveillance technologies that we produce, and so we take a number of precautions to limit the potential for that abuse. We provide our software only to governments or government agencies. We do not sell products to individuals or private businesses.

We fully comply with dual use and export controls called for in the nineteenth Plenary meeting of the Wassenaar Arrangement.

We do not sell products to governments or to countries blacklisted by the U.S., E.U., U.N., NATO or ASEAN.

We monitor the international geopolitical situation and we review potential customers before a sale to determine whether or not there is objective evidence or credible concerns that Hacking Team technology provided to the customer will be used to facilitate human rights violations.

We have established a panel of technical experts and legal advisors, unique in our industry, that reviews potential sales.

Moreover, in HT contracts, we require customers to abide by applicable law. We reserve the right in our contracts to suspend support for our software if we find terms of our contracts are violated. If we suspend support for HT technology, the product soon becomes useless.

We will refuse to provide or we will stop supporting our technologies to governments or government agencies that:

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

HT policies and procedures are consistent with the U.S. Know Your Customer guidelines. We conduct ongoing employee training to assure that employees know and understand the provisions of these guidelines.

Should we discover "red flags" described in these guidelines while negotiating a sale, we will conduct a detailed inquiry into the matter and raise the issue with the potential customer. If the "red flags" cannot be reasonably explained or justified, we may suspend the transaction.

58 http://www.hackingteam.it/index.php/customer-policy

Our review will include:

- Statements made by the potential customer either to HT or elsewhere that reflect the potential for abuse.
- The potential customer's laws, regulations and practices regarding surveillance including due process requirements.
- Credible government or non-government reports reflecting that a potential customer could use surveillance technologies to facilitate human rights abuses.

Hacking Team encourages anyone with information about apparent misuse or abuse of our systems and solutions to promptly report that information to us at info@hackingteam.comThis e-mail address is being protected from spambots. You need JavaScript enabled to view it .

Hacking Team has established a process of monitoring news media, activist community blogs and other Internet communication, and other available sources for expressed concerns about human rights abuses by customers or potential customers. Should questions be raised about the possible abuse of HT software in human rights cases, HT will investigate to determine the facts to the extent possible. If we believe one of our customers may be involved in an abuse of HT software, we will contact the customer as part of this investigation. Based on the results of such an investigation, HT will take appropriate action.

Annex II: Hacking Team News Release on Compliance with Wassenaar Arrangement Export Controls[59]

HackingTeam Complies With Wassenaar Arrangement Export Controls on Surveillance and Law Enforcement/ Intelligence Gathering Tools

Milan, Italy (Feb. 25, 2015) Hacking Team, the world leader in providing state-of-the-art software tools for surveillance to law enforcement and intelligence agencies, said today it is complying fully with the export controls called for in the nineteenth Plenary meeting of the Wassenaar Arrangement. No other company in the lawful surveillance industry has made this commitment.

These export controls are designed to assure that only appropriate governments or government agencies are able to use surveillance software and that the use of the software in no way threatens international or regional security or stability.
On January 1, 2015 , the European Union (E.U.) implemented the Wassenaar guidance and applicable dual use legislation. Hacking Team instituted the new procedures immediately.

"We designed our system to be used to fight crime and terrorism and we want it to be used for that purpose," said David Vincenzetti, CEO of Hacking Team. "Criminals and terrorists around the world routinely use mobile phones, mobile devices, computers, and the Internet to commit horrific crimes and terrorism. Without HT technology law enforcement is blind to this activity."

"We are now the first in our industry to comply with these latest international laws, and we are doing so because we are committed to assuring that our products are not misused," Vincenzetti said.

Under the procedures agreed to by Hacking Team and the Italian Ministry of Economic Development, HT will request from the Italian Government export authorization for its technologies.

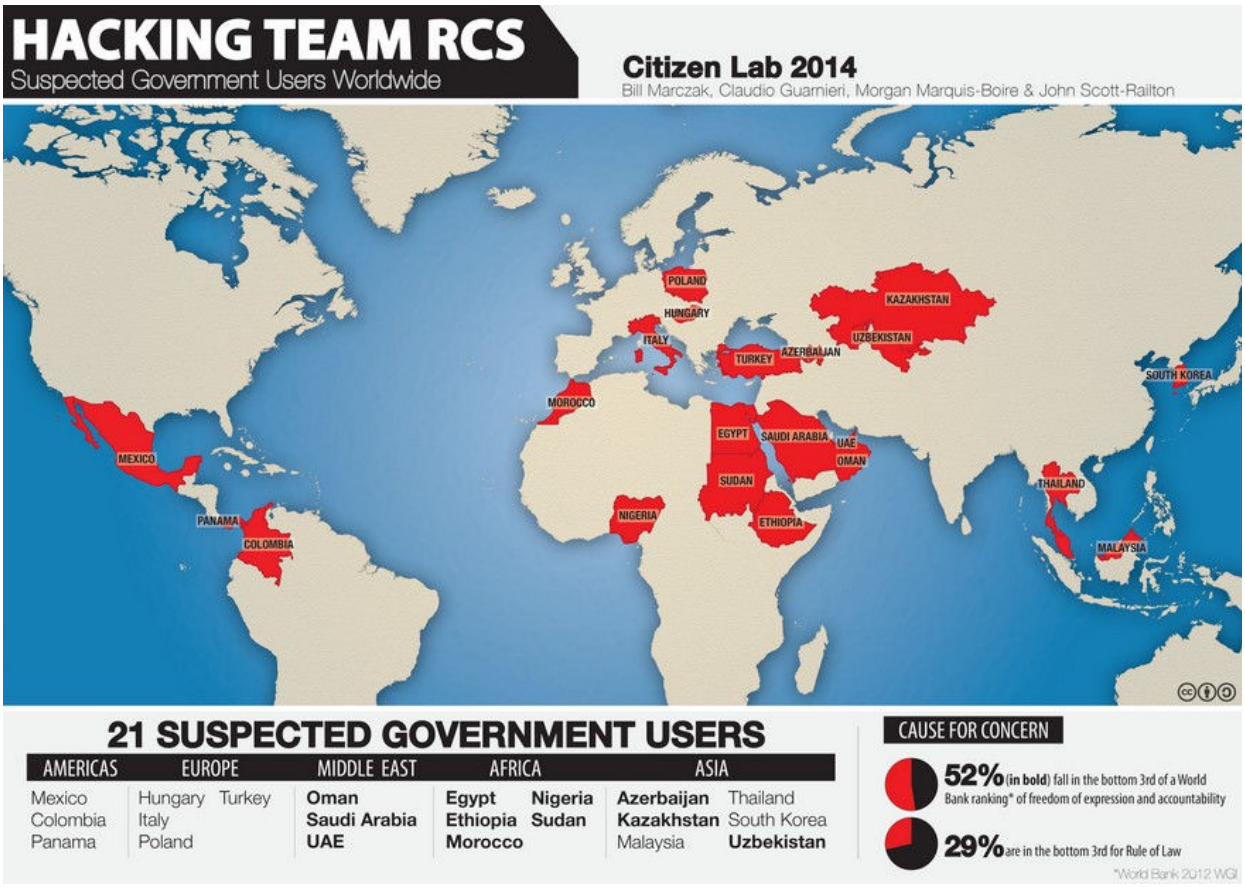
Previous to this regulation, the company had already instituted internal controls and procedures to assure its software is not abused. The Wassenaar protocols add additional insurance that Hacking Team technologies are only provided to and used by appropriate agencies and governments.

Since its founding, Hacking Team has recognized the power of its tools that allow law enforcement agencies to monitor computer traffic, mobile phone and other similar communications. The company voluntarily instituted a customer policy published on the hackingteam.com website to assure that its tools were not abused.
Hacking Team has also committed to abiding by international black lists and other guidelines so that its surveillance system is not sold to states or state agencies that might abuse it.

59 http://www.hackingteam.it/index.php/about-us

For further information:
Eric Rabe
Chief Marketing and Communications Officer
Hacking Team
215-839-6639
e.rabe@hackingteam.comThis e-mail address is being protected from spambots. You need JavaScript enabled to view it

Annex III: Map of Hacking Team Software Proliferation[60]



60 https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

Annex IV

Approve | Correct | Modify | Save Tmplt | Delete | Print | Help

Award Type: Purchase Order **Prepared Date:** 03/31/2011 07:16:28 **Prepared User:** SHAWN.M.SMITH4.W911W4@MI.ARMY.MIL

Award Status: Final **Last Modified Date:** 03/31/2011 15:20:09 **Last Modified User:** RANDY.DREYER.W911W4@MI.ARMY.MIL

Document Information

	Agency	*Procurement Identifier*	*Modification No*	*Trans No*
Award ID:	9700	W911W411P0055	0	0
Referenced IDV ID:				
Reason For Modification:				
Solicitation ID:	W911W411T0107			

	Agency Identifier	*Main Account*	*Sub Account*	*Initiative*
Treasury Account Symbol:				Select One

Dates

Date Signed *(mm/dd/yyyy)* **:**	03/31/2011
Effective Date *(mm/dd/yyyy)* **:**	03/31/2011
Completion Date *(mm/dd/yyyy)* **:**	04/30/2011
Est. Ultimate Completion Date *(mm/dd/yyyy)* **:**	04/30/2011

Amounts

Action Obligation:	$350,000.00
Base And Exercised Options Value:	$350,000.00
Base And All Options Value:	$350,000.00
Fee Paid for Use of IDV:	$0.00

Purchaser Information

Contracting Office Agency ID:	2100	**Contracting Office Agency Name:**	DEPT OF THE ARMY
Contracting Office ID:	W911W4	**Contracting Office Name:**	W00Y CONTR OFC DODAAC
Funding Agency ID:	2100	**Funding Agency Name:**	DEPT OF THE ARMY
Funding Office ID:	W23BFK	**Funding Office Name:**	W4VY INSCOM MISSION SPT CMD
Foreign Funding:	Not Applicable		

Contractor Information

SAM Exception: Remove Exception

DUNS No:	963322842	**Street:**	1997 ANNAPOLIS EXCHANGE PKWY STE 30
Vendor Name:	CICOM USA, LLC	**Street2:**	
DBAN:		**City:**	ANNAPOLIS
		State:	MD **Zip:** 214013271
		Country:	UNITED STATES
		Phone:	(443) 949-7470
		Fax No:	(443) 949-7471
		Congressional District:	MARYLAND 03

Business Category Show Details

Organization Type:	PARTNERSHIP
Number of Employees:	3
State of Incorporation:	
Country of Incorporation:	
Annual Revenue:	$3,000,000

Business Types
✓Partnership or Limited Liability Partnership
Socio Economic Data
✓Minority Owned Business
✓Hispanic American Owned
Line Of Business
✓Educational Institution
✓Hispanic Servicing Institution
Relationship With Federal Government
✓Both (Contracts and Grants)
Organization Factors
✓For Profit Organization
✓Limited Liability Corporation
Certifications
✓DoT Certified Disadvantaged Business Enterprise

Contract Data

Type of Contract:	Firm Fixed Price
Multiyear Contract:	Select One
Major Program:	
National Interest Action:	None
Cost Or Pricing Data:	Select One
Purchase Card Used As Payment Method:	No
Undefinitized Action:	No
Performance Based Service Acquisition:	Not Applicable

**** FY 2004 and prior; 80% or more specified as performance requirement***

FY 2005 and later; 50% or more specified as performance requirement

Contingency Humanitarian Peacekeeping Operation: Not Applicable
Contract Financing: Not Applicable
Cost Accounting Standards Clause: Select One
Consolidated Contract: No
Number Of Actions: 1

Legislative Mandates

Clinger-Cohen Act: No
Service Contract Act: No
Walsh-Healey Act: No
Davis Bacon Act: No
Interagency Contracting Authority: Not Applicable
Other Interagency Contracting Statutory Authority: *(1000 characters)*

Principal Place of Performance

	State	*Location*	*Country*
Principal Place Of Performance Code:	MD		USA
Principal Place Of Performance County Name:	ANNE ARUNDEL		
Principal Place Of Performance City Name:	ANNAPOLIS		
Congressional District Place Of Performance:	03		
Place Of Performance Zip Code(+4):	21401 - 3271		USPS ZIP Codes

Product Or Service Information

Product/Service Code: 7030 **Description:** ADP SOFTWARE
Principal NAICS Code: 541512 **Description:** COMPUTER SYSTEMS DESIGN SERVICES
Bundled Contract: Not a bundled requirement
System Equipment Code: 000 **Description:** NONE
Country of Product or Service Origin: ITA ITALY
Place of Manufacture: Mfg outside U.S. - Qualifying country (DoD only)
Domestic or Foreign Entity: Foreign-Owned Business Not Incorporated in the U.S.
Recovered Materials/Sustainability: No Clauses Included and No Sustainability Included — OMB Policy on Sustainable Acquisition
InfoTech Commercial Item Category: Commercially Available
Claimant Program Code: C9E **Description:** ALL OTHERS NOT IDENTIFIABLE TO ANY OTHER PROCUREI
Sea Transportation: No
GFE/GFP Provided Under This Action: Transaction does not use GFE/GFP
Use Of EPA Designated Products: Meets Requirements
Description Of Requirement: *(4000 characters)* REMOTE CONTROL SYSTEM

Competition Information

Extent Competed For Referenced IDV:
Extent Competed: Not Competed
Solicitation Procedures: Only One Source
Type Of Set Aside: No set aside used.
Evaluated Preference: No Preference used
SBIR/STTR: Select One
Fair Opportunity/Limited Sources: Select One
Other Than Full And Open Competition: National Security (FAR 6.302-6)
Local Area Set Aside: No
FedBizOpps: Yes
A76 Action: No
Commercial Item Acquisition Procedures: Commercial Item
Number Of Offers Received: 1
Small Business Competitiveness Demonstration Program: ☐
Commercial Item Test Program: No

Preference Programs / Other Data

Contracting Officer's Business Size Selection: Small Business
Subcontract Plan: Plan Not Required
Price Evaluation Percent Difference: %

Annex V

Approve | Correct | Modify | Save Tmplt | Delete | Print | Help

Award Type: Definitive Contract **Prepared Date:** 09/09/2014 14:08:40 **Prepared User:** JCGIRARD

Award Status: Final **Last Modified Date:** 10/02/2014 08:10:25 **Last Modified User:** JCGIRARD

Document Information

	Agency	*Procurement Identifier*	*Modification No*	*Trans No*
Award ID:	1524	DJD12C0033	6	0
Referenced IDV ID:				

Reason For Modification: EXERCISE AN OPTION

Solicitation ID:

	Agency Identifier	*Main Account*	*Sub Account*	*Initiative*
Treasury Account Symbol:	15	1100	000	Select One

Dates

Date Signed *(mm/dd/yyyy)* **:**	09/09/2014
Effective Date *(mm/dd/yyyy)* **:**	08/29/2014
Completion Date *(mm/dd/yyyy)* **:**	08/26/2015
Est. Ultimate Completion Date *(mm/dd/yyyy)* **:**	08/26/2015

Amounts

	Current	Total
Action Obligation:	$140,000.00	$927,000.00
Base And Exercised Options Value:	-$20,000.00	$1,952,000.00
Base And All Options Value:	$25,000.00	$2,457,000.00
Fee Paid for Use of IDV:	$0.00	

Purchaser Information

Contracting Office Agency ID:	1524	**Contracting Office Agency Name:**	DRUG ENFORCEMENT ADMINISTRATION
Contracting Office ID:	DEAHQ	**Contracting Office Name:**	HEADQUARTERS-DRUG ENFORCEMENT ADMIN
Funding Agency ID:	1524	**Funding Agency Name:**	DRUG ENFORCEMENT ADMINISTRATION
Funding Office ID:	DEAST	**Funding Office Name:**	LABORATORY-SPECIAL TESTING
Foreign Funding:	Not Applicable		

Contractor Information

SAM Exception: Remove Exception

DUNS No:	963322842	**Street:**	1997 ANNAPOLIS EXCHANGE PKWY STE 30
Vendor Name:	CICOM USA, LLC	**Street2:**	
DBAN:		**City:**	ANNAPOLIS
		State:	MD **Zip:** 214013271
		Country:	UNITED STATES
		Phone:	(443) 949-7470
		Fax No:	(443) 949-7471
		Congressional District:	MARYLAND 03

Show Details

Business Category

Organization Type:	OTHER
Number of Employees:	3
State of Incorporation:	
Country of Incorporation:	
Annual Revenue:	$3,000,000

Socio Economic Data
- ✓ Minority Owned Business
- ✓ Hispanic American Owned

Line Of Business
- ✓ Educational Institution
- ✓ Hispanic Servicing Institution

Relationship With Federal Government
- ✓ Both (Contracts and Grants)

Organization Factors
- ✓ For Profit Organization
- ✓ Limited Liability Corporation

Certifications
- ✓ DoT Certified Disadvantaged Business Enterprise
- ✓ Self-Certified Small Disadvantaged Business

Contract Data

Type of Contract:	Firm Fixed Price
Multiyear Contract:	Yes
Major Program:	
National Interest Action:	None
Cost Or Pricing Data:	No
Purchase Card Used As Payment Method:	No
Undefinitized Action:	No
Performance Based Service Acquisition:	Not Applicable

**** FY 2004 and prior; 80% or more specified as performance requirement***

FY 2005 and later; 50% or more specified as performance requirement

Contingency Humanitarian Peacekeeping Operation: Not Applicable
Contract Financing: Select One
Cost Accounting Standards Clause: Not Applicable exempt from CAS
Consolidated Contract: No
Number Of Actions: 1

Legislative Mandates

Clinger-Cohen Act: No
Service Contract Act: Not Applicable
Walsh-Healey Act: Not Applicable
Davis Bacon Act: Not Applicable
Interagency Contracting Authority: Not Applicable
Other Interagency Contracting Statutory Authority: *(1000 characters)*

Principal Place of Performance

	State	*Location*	*Country*
Principal Place Of Performance Code:	VA		USA
Principal Place Of Performance County Name:	FAIRFAX		
Principal Place Of Performance City Name:	LORTON		
Congressional District Place Of Performance:	08		
Place Of Performance Zip Code(+4):	22079 - 1447		USPS ZIP Codes

Product Or Service Information

Product/Service Code: 7010 **Description:** ADPE SYSTEM CONFIGURATION
Principal NAICS Code: 334290 **Description:** OTHER COMMUNICATIONS EQUIPMENT MANUFACTURING
Bundled Contract: Not a bundled requirement
System Equipment Code: **Description:**
Country of Product or Service Origin: USA UNITED STATES
Place of Manufacture: Mfg in U.S.
Domestic or Foreign Entity: U.S. Owned Business
Recovered Materials/Sustainability: No Clauses Included and No Sustainability Included OMB Policy on Sustainable Acquisition
InfoTech Commercial Item Category: Select One
Claimant Program Code: **Description:**
Sea Transportation: Select One
GFE/GFP Provided Under This Action: Transaction does not use GFE/GFP
Use Of EPA Designated Products: Not Required
Description Of Requirement: *(4000 characters)*

IGF::CL::IGF
Remote Control Host Based Interception Systems and support services

Competition Information

Extent Competed For Referenced IDV:

Extent Competed: Not Competed
Solicitation Procedures: Only One Source
Type Of Set Aside: No set aside used.
Evaluated Preference: No Preference used
SBIR/STTR: Select One
Fair Opportunity/Limited Sources: Select One
Other Than Full And Open Competition: Only One Source-Other (FAR 6.302-1 other)
Local Area Set Aside: No
FedBizOpps: Yes
A76 Action: No
Commercial Item Acquisition Procedures: Commercial Item
Number Of Offers Received: 1
Small Business Competitiveness Demonstration Program: ☐
Commercial Item Test Program: No

Preference Programs / Other Data

Contracting Officer's Business Size Selection: Small Business
Subcontract Plan: Plan Not Required
Price Evaluation Percent Difference: 0 %

New | Save Draft | Validate | Approve | Correct | Modify | Save Tmplt | Delete | Print | Help

Transaction Information

Award Type:	Definitive Contract	**Prepared Date:**	08/30/2012 12:29:56	**Prepared User:**	GXSHABNAM
Award Status:	Final	**Last Modified Date:**	09/06/2012 09:25:13	**Last Modified User:**	GXSHABNAM

Document Information

	Agency	*Procurement Identifier*	*Modification No*	*Trans No*
Award ID:	1524	DJD12C0033	0	0
Referenced IDV ID:				
Reason For Modification:				
Solicitation ID:				

	Agency Identifier	*Main Account*	*Sub Account*	*Initiative*
Treasury Account Symbol:	15	1100		Select One

Dates

Date Signed *(mm/dd/yyyy)* **:**	08/20/2012
Effective Date *(mm/dd/yyyy)* **:**	08/17/2012
Completion Date *(mm/dd/yyyy)* **:**	08/26/2013
Est. Ultimate Completion Date *(mm/dd/yyyy)* **:**	08/26/2017

Amounts

Action Obligation:	$575,000.00
Base And Exercised Options Value:	$1,950,000.00
Base And All Options Value:	$2,410,000.00
Fee Paid for Use of IDV:	$0.00

Purchaser Information

Contracting Office Agency ID:	1524	**Contracting Office Agency Name:**	DRUG ENFORCEMENT ADMINISTRATION
Contracting Office ID:	DEAIT	**Contracting Office Name:**	OFFICE-INVESTIGATIVE TECHNOLOGY
Funding Agency ID:	1524	**Funding Agency Name:**	DRUG ENFORCEMENT ADMINISTRATION
Funding Office ID:	DEAIT	**Funding Office Name:**	OFFICE-INVESTIGATIVE TECHNOLOGY
Foreign Funding:	Not Applicable		

Contractor Information

SAM Exception: Remove Exception

DUNS No:	963322842	**Street:**	1997 ANNAPOLIS EXCHANGE PKWY STE 30
Vendor Name:	CICOM USA, LLC	**Street2:**	
DBAN:		**City:**	ANNAPOLIS
		State:	MD **Zip:** 214013271
		Country:	UNITED STATES
		Phone:	(443) 949-7470
		Fax No:	(443) 949-7471
		Congressional District:	MARYLAND 03

Show Details

Business Category

Organization Type:	OTHER
Number of Employees:	3
State of Incorporation:	
Country of Incorporation:	
Annual Revenue:	$3,000,000

Socio Economic Data
- ✓ Minority Owned Business
- ✓ Hispanic American Owned

Line Of Business
- ✓ Educational Institution
- ✓ Hispanic Servicing Institution

Relationship With Federal Government
- ✓ Both (Contracts and Grants)

Organization Factors
- ✓ For Profit Organization
- ✓ Limited Liability Corporation

Certifications
- ✓ DoT Certified Disadvantaged Business Enterprise
- ✓ Self-Certified Small Disadvantaged Business

Contract Data

Type of Contract:	Firm Fixed Price
Multiyear Contract:	Yes
Major Program:	
National Interest Action:	None
Cost Or Pricing Data:	No
Purchase Card Used As Payment Method:	No
Undefinitized Action:	No
Performance Based Service Acquisition:	Not Applicable
**** FY 2004 and prior; 80% or more specified as performance requirement***	
**** FY 2005 and later; 50% or more specified as performance requirement***	
Contingency Humanitarian Peacekeeping Operation:	Not Applicable

Contract Financing: Select One
Cost Accounting Standards Clause: Not Applicable exempt from CAS
Consolidated Contract: No
Number Of Actions: 1

Legislative Mandates

Clinger-Cohen Act: No
Service Contract Act: Not Applicable
Walsh-Healey Act: Not Applicable
Davis Bacon Act: Not Applicable
Interagency Contracting Authority: Not Applicable
Other Interagency Contracting Statutory Authority: *(1000 characters)*

Principal Place of Performance

	State	*Location*	*Country*
Principal Place Of Performance Code:	VA		USA
Principal Place Of Performance County Name:	FAIRFAX		
Principal Place Of Performance City Name:	LORTON		
Congressional District Place Of Performance:	08		
Place Of Performance Zip Code(+4):	22079 - 1447		USPS ZIP Codes

Product Or Service Information

Product/Service Code: 7010 **Description:** ADPE SYSTEM CONFIGURATION
Principal NAICS Code: 334290 **Description:** OTHER COMMUNICATIONS EQUIPMENT MANUFACTURING
Bundled Contract: Not a bundled requirement
System Equipment Code: **Description:**
Country of Product or Service Origin: USA UNITED STATES
Place of Manufacture: Mfg in U.S.
Domestic or Foreign Entity: U.S. Owned Business
Recovered Materials/Sustainability: No Clauses Included and No Sustainability Included OMB Policy on Sustainable Acquisition
InfoTech Commercial Item Category: Select One
Claimant Program Code: **Description:**
Sea Transportation: Select One
GFE/GFP Provided Under This Action: Transaction does not use GFE/GFP
Use Of EPA Designated Products: Not Required
Description Of Requirement: *(4000 characters)*
Critical Functions: Software

Competition Information

Extent Competed For Referenced IDV:
Extent Competed: Not Competed
Solicitation Procedures: Only One Source
Type Of Set Aside: No set aside used.
Evaluated Preference: No Preference used
SBIR/STTR: Select One
Fair Opportunity/Limited Sources: Select One
Other Than Full And Open Competition: Only One Source-Other (FAR 6.302-1 other)
Local Area Set Aside: No
FedBizOpps: Yes
A76 Action: No
Commercial Item Acquisition Procedures: Commercial Item
Number Of Offers Received: 1
Small Business Competitiveness Demonstration Program:
Commercial Item Test Program: No

Preference Programs / Other Data

Contracting Officer's Business Size Selection: Small Business
Subcontract Plan: Plan Not Required
Price Evaluation Percent Difference: 0 %