Citizen Lab, Munk School of Global Affairs, University of Toronto

MUNK SCHOOL OF GLOBAL AFFAIRS

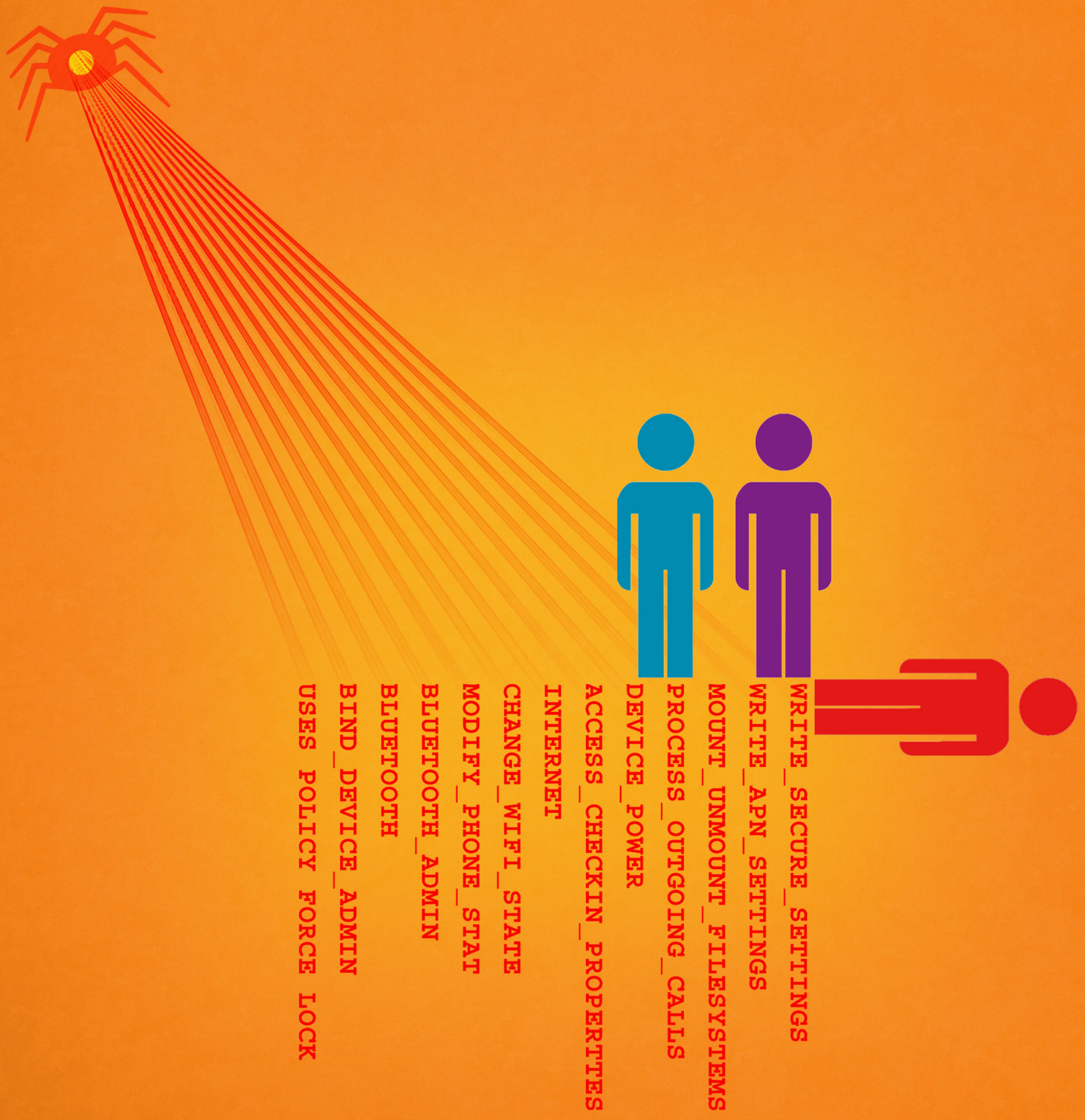
UNIVERSITY OF TORONTO

COMMUNITIES @ RISK

Targeted Digital Threats Against Civil Society

November 11, 2014

https://targetedthreats.net/



FURTHER READING

CITIZEN LAB REPORTS

Ron Deibert, "Towards a cyber security strategy for global civil society?" Global Information Society Watch, 2011, http://www.giswatch.org/en/freedom-expression/towards-cyber-security-strategy-global-civil-society

Seth Hardy, "What is an APT without a sensationalist name?" SecTor Conference, October 18, 2011, http://sector.ca/Media/Past-Events/what-is-an-apt-without-a-sensationalist-name-13636

Targeted malware attacks are particularly dangerous to NGOs and other organizations that take real-world risks while often having little if any IT security budget. This presentation describes a variety of targeted malware attacks observed in the wild against human rights organizations, and the techniques (both social and technical) that they use to be successful. It then looks at the technical details of a data exfiltration network: what information is being stolen, how it is leaving your network, and where it is going. The presentation concludes with observations on how this kind of targeted malware differs from those used for financial gain, and steps that organizations can take to defend themselves, even with very limited resources.

Citizen Lab, "Information Operations and Tibetan Rights in the Wake of Self-Immolations: Part I," March 9, 2012, https://citizenlab.org/2012/03/information-operations-and-tibetan-rights-in-the-wake-of-self-immolations-part-i/

This post is the first in a series of analyses that the Citizen Lab prepared regarding the urgent and ongoing threat presented by information operations deployed against Tibetans and others who advocate for Tibetan rights and freedoms, including in Tibetan areas of China. The Citizen Lab is concerned with the apparent increase in the use of social engineering linked to the issue of self-immolation to target Tibetan activists with malware, as well as the reported increase in magnitude of information controls (in close coordination with more physical measures) utilized by the Chinese government in Tibetan areas.

Morgan Marquis-Boire and Seth Hardy, "Syrian Activists Targeted with BlackShades Spy Software," Citizen Lab, June 19, 2012, https://citizenlab.org/2012/06/syrian-activists-targeted-with-blackshades-spy-software/

The use of remote surveillance software against activists has been a feature of the ongoing conflict in Syria. The EFF and Citizen Lab report on the use of a new toolkit by a previously observed attacker, which has been circulating malware which surreptitiously installs BlackShades Remote Access Trojan (RAT) on victim's machines.

Citizen Lab, "Spoofing the European Parliament," June 20, 2012, https://citizenlab.

org/2012/06/spoofing-the-european-parliament/

The Citizen Lab analyzes a recent targeted malware attack against the Tibetan community which spoofs a June 14, 2012 resolution of the European Parliament on the human rights situation in Tibet. While such repurposing of authentic content for use as a malware delivery mechanism is not unusual, this incident raises serious questions surrounding the use of legitimate political resources for illegitimate ends.

Morgan Marquis-Boire, "From Bahrain with Love: FinFisher's Spy Kit Exposed?," Citizen Lab, July 25, 2012, https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/

This Citizen Lab posts analyzes several pieces of malware targeting Bahraini dissidents, which were shared with us by Bloomberg News. The analysis suggests that the malware used is FinSpy, part of the commercial intrusion kit, Finfisher, distributed by the United Kingdom-based company, Gamma International.

Citizen Lab, "Recent Observations in Tibet-Related Information Operations: Advanced Social Engineering for the Distribution of LURK Malware," July 26, 2012, https://citizenlab.org/2012/07/recent-observations/

The Citizen Lab has analyzed recent targeted malware attacks against Tibetan organizations that share a common payload —LURK malware—and command-and-control server, as well as several other features.

Seth Hardy, "IEXPL0RE RAT," Citizen Lab, August 2012, https://citizenlab.org/wp-content/uploads/2012/09/IEXPL0RE_RAT.pdf

This report describes a Remote Access Trojan (RAT) that three human rights-related organizations taking part in our study received via email in 2011 and at the end of 2010. We refer to this RAT as the IEXPL0RE RAT, after the name of the launcher program. This RAT has the ability to record user keystrokes (including passwords), copy and delete files, download and run new programs, and even use the computer's microphone and camera to listen and watch the user in real-time.

Morgan Marquis-Boire, Bill Marczak, and Claudio Guarnieri, *The SmartPhone who Loved Me: FinFisher Goes Mobile?*, Citizen Lab, August 29, 2012, https://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/

This post describes our work analyzing several samples which appear to be mobile variants of the FinFisher Toolkit, and scanning we performed which identified more apparent FinFisher command and control servers.

Citizen Lab, "Human Rights Groups Targeted by PlugX RAT," September 28, 2012, https://citizenlab.org/2012/09/human-rights-groups-targeted-by-plugx-rat/

In this Citizen Lab blog post, we report on malware campaigns targeting human rights groups using the PlugX Remote Access Trojan.

Morgan Marquis-Boire, *Backdoors are Forever: Hacking Team and the Targeting of Dissent*, Citizen Lab, October 10, 2012, https://citizenlab.org/wp-content/uploads/2012/10/12-2012-backdoorsareforever.pdf

In this report, Citizen Lab Security Researcher Morgan Marquis-Boire describes analysis performed on malicious software used to compromise a high profile dissident residing in the United Arab Emirates. The findings indicate that the software is a commercial surveillance backdoor distributed by an Italian company known as Hacking Team. The report also describes the potential involvement of vulnerabilities sold by the French company, VUPEN.

Seth Hardy, "APT1's GLASSES—Watching a Human Rights Organization," Citizen Lab, February 25, 2013, https://citizenlab.org/2013/02/apt1s-glasses-watching-a-human-rights-organization/

In this report we found malware used in a targeted attack against a Tibetan human rights organization which was closely related to malware described by Mandiant. In their report, Mandiant described how APT1 (referred to as "Comment Crew" or "Byzantine Candor" in other reports) has targeted a large number of organizations in a wide range of industries, stealing terabytes of data. Our report demonstrates that APT1 is not only involved in industrial and corporate espionage, but also in attacks against civil society actors documented as early as 2010. This observation reflects other findings showing that in some cases the same threat actors and infrastructure are used to target government and industry are also used against civil society groups.

Ron Deibert and Sarah McKune, "Civil Society Hung Out To Dry in Global Cyber Espionage," *CircleID*, March 4, 2014, http://www.circleid.com/posts/20130304_civil_society_hung_out_to_dry_in_global_cyber_espionage/

Canada Centre for Global Security Studies and Citizen Lab Director Ron Deibert and Senior Researcher Sarah McKune authored an article in CircleID on an often overlooked dimension of cyber threats and cyber espionage: the targeting of civil society actors.

Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, *You Only Click Twice: FinFisher's Global Proliferation*, Citizen Lab, March 13, 2013, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

This report describes the results of a comprehensive global Internet scan for the command-

and-control servers of FinFisher's surveillance software. We have found command-and-control servers for FinSpy backdoors, part of Gamma International's FinFisher "remote monitoring solution," in a total of 25 countries: 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, Vietnam. The report also details the discovery of FinFisher in Ethiopia, which targets individuals using pictures of Ginbot 7, an Ethiopian opposition group, as bait to infect users. Additionally, it provides examination of a FinSpy Mobile sample found in the wild, which appears to have been used in Vietnam.

Citizen Lab, "Permission to Spy: An Analysis of Android Malware Targeting Tibetans," April 18, 2013, https://citizenlab.org/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/

In January 2013, we were provided with a sample of a highly targeted attack delivered through email that contained compromised versions of two Android applications that are popular in the Tibetan community: KakaoTalk (a mobile messaging client) and TuneIn (an Internet radio application). The email message repurposed a legitimate private email message sent by an information security expert in the Tibetan community to a member of the Tibetan parliament-in-exile. The compromised versions of the Android applications contained malware that is is designed to send a user's contacts, SMS message history, and cellular network location to attackers.The cellular network information gathered by this malware would only be useful to actors with detailed knowledge of the cellular communication provider's technical infrastructure. These findings demonstrate the risks communities face from targeted mobile malware. While the majority of targeted attacks we observe are designed to exploit the Windows operating system, we are also observing attacks targeting OS X, Linux and Android. Attackers will continue to adopt new methods and widen targeting of platforms. We had this report translated into Tibetan and circulated amongst the community to raise user awareness of targeted mobile malware threats.

Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, *For Their Eyes Only: The Commercialization of Digital Spying*, Citizen Lab, April 30, 2013, https://citizenlab.org/2013/04/for-their-eyes-only-2/

The report features new findings, as well as consolidates a year of our research on the commercial market for offensive computer network intrusion capabilities developed by Western companies. Taken together with our previous research into FinFisher, we can now assert that FinFisher's command-and-control servers are currently active, or have been present, in 36 countries (Australia, Austria, Bahrain, Bangladesh, Brunei, Bulgaria, Canada, Czech Republic, Estonia, Ethiopia, Germany, Hungary, India, Indonesia, Japan, Latvia, Lithuania, Macedonia, Malaysia, Mexico, Mongolia, Netherlands, Nigeria, Pakistan, Panama, Qatar, Romania, Serbia, Singapore, South Africa, Turkey, Turkmenistan, United Arab Emirates, United Kingdom, United States, Vietnam.) We have also identified a FinSpy sample that appears to be specifically targeting Malay language speakers, masquerading as a document discussing Malaysia's upcoming 2013 General Elections.We identify instances where FinSpy makes use of Mozilla's Trademark and Code. The latest Malay-language sample masquerades as Mozilla Firefox in both file properties and in manifest.

John Scott-Railton and Morgan Marquis-Boire, "A Call to Harm: New Malware Attacks Target the Syrian Opposition," Citizen Lab, June 21, 2013, https://citizenlab.org/2013/06/a-call-to-harm/

Syria's opposition has faced persistent targeting by Pro-Government Electronic Actors throughout the Syrian civil war. A pro-government group calling itself the Syrian Electronic Army has gained visibility throughout the conflict with high profile attacks against news organizations. Meanwhile, Syrian activists continue to be targeted with online attacks apparently for the purposes of accessing their private communications and stealing their secrets. Researchers have identified a common theme among the attacks against the Syrian opposition: sophisticated social engineering that is grounded in an awareness of the needs, interests, and weaknesses of the opposition. This report describes two types of attacks that follow this theme: One is a malicious installer of the circumvention tool Freegate, while the other is an e-mail attachment calling for jihad against Hezbollah and the Assad regime or promising interesting regional news. The report was translated into Arabic by Cyber Arabs.

Katie Kleemola and Seth Hardy, "Surtr: Malware Family Targeting the Tibetan Community," Citizen Lab, August 2, 2013, https://citizenlab.org/2013/08/surtr-malware-family-targeting-the-tibetan-community/

In this report, we document the discovery of a malware family we call "Surtr," which we have observed used in attacks against Tibetan groups since November 2012. This malware family continues to be used in campaigns and we are actively tracking its development and the threat actors and infrastructure behind its operation. Before we published our report, we prepared a special advisory for the Tibetan community that we circulated privately to increase user awareness. We also submitted technical details on the malware family to the DeepEnd Research Library of Malware Traffic patterns, which is a community resource that collects traffic analysis of malware families from open sources to help researchers identify and track these malware families and develop defenses against them.

Seth Hardy, "Targeted Threat Index," Citizen Lab, October 18, 2013, https://citizenlab.org/2013/10/targeted-threat-index/

We published a short report on our first iteration of the Targeted Threat Index (TTI) following strong interest shown in the metric when we presented it at Canada's premier information security Conference SecTor in October 2013. We later refined and iterated on the

TTI and produced an expanded version of the analysis for our Usenix Security 2014 paper submission.

Eva Galperin, Morgan Marquis-Boire, and John Scott-Railton, *Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns*, Electronic Frontier Foundation, December 23, 2013, https://www.eff.org/deeplinks/2013/12/social-engineering-and-malware-syria-eff-and-citizen-labs-latest-report-digital

Citizen Lab security researchers Morgan Marquis-Boire and John Scott-Railton along with Electronic Frontier Foundation (EFF) Global Policy Analyst Eva Galperin published a technical paper outlining how Syrian pro-government attackers targeted the opposition, as well as NGO workers and journalists, with social engineering and Remote Access Tools. The report builds on extensive previous research and writings by EFF and Citizen Lab to update what we know about malware campaigns targeting the Syrian opposition. The report's accompanying piece was published in Wired magazine.

Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, "Hacking Team and the Targeting of Ethiopian Journalists," Citizen Lab, February 12, 2014, https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/

In February 2014, we reported on targeted attacks against the Ethiopian Satellite Television Service (ESAT), an independent satellite television, radio, and online news media outlet run by members of the Ethiopian diaspora, that we revealed to be using Remote Control System, sold exclusively to governments by Milan-based Hacking Team. The malware communicated with an IP address belonging to Ariave Satcom, a satellite provider that services Africa, Europe, and Asia.

Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, "Mapping Hacking Team's Untraceable Spyware," Citizen Lab, February 17, 2014, https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

This report maps out covert networks of "proxy servers" used to launder data that Hacking Team's Remote Control System (RCS) exfiltrates from infected computers, through third countries, to an "endpoint," which we believe represents the spyware's government operator. This process is designed to obscure the identity of the government conducting the spying. For example, data destined for an endpoint in Mexico appears to be routed through four different proxies, each in a different country. This so-called "collection infrastructure" appears to be provided by one or more commercial vendors—perhaps including Hacking Team itself. Hacking Team advertises that their RCS spyware is "untraceable" to a specific government operator. However, we claim to identify a number of current or former government users of the spyware by pinpointing endpoints, and studying instances of RCS that we have observed. We suspect that agencies of these twenty-one governments are current or former users of RCS: Azerbaijan, Colombia, Egypt, Ethiopia, Hungary, Italy, Kazakhstan, Korea, Malaysia, Mexico, Morocco, Nigeria, Oman, Panama, Poland, Saudi Arabia, Sudan, Thailand, Turkey, UAE, and Uzbekistan.

Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, John Scott-Railton, and Sarah McKune, "Hacking Team's US Nexus," Citizen Lab, February 28, 2014, https://citizenlab.org/2014/02/hacking-teams-us-nexus/

This report is a follow up to our previous report, titled "Mapping Hacking Team's "Untraceable" Spyware," which identifies 21 governments that we suspect are current or former users of Remote Control System (RCS). The report showed that computers infected with RCS send surveillance data back to the government operator through a series of servers in multiple third countries, called a proxy chain or circuit. We delve deeper into these proxy chains, and find that in at least 12 cases, US-based data centers are part of this dedicated foreign espionage infrastructure. Our analysis traces these proxy chains, and finds that US-based servers appear to assist the governments of Azerbaijan, Colombia, Ethiopia, Korea, Mexico, Morocco, Poland, Thailand, Uzbekistan, and the United Arab Emirates in their espionage and/or law enforcement operations.

John Scott-Railton, "Maliciously Repackaged Psiphon Found," Citizen Lab, March 13, 2014, https://citizenlab.org/2014/03/maliciously-repackaged-psiphon/

In March 2014, we documented a malicious repackaging of Psiphon 3, which is a circumvention tool originally developed by the Citizen Lab, which was spun out into a private Canadian corporation in 2008. The malware contains both a functioning copy of Psiphon, and the njRAT trojan. When executed, the implant communicates with a Syrian command-and-control server. This is likely part of a targeted attack against the Syrian opposition by a known actor, not all users of Psiphon. This report was translated into Arabic and disseminated to at risk users. (https://citizenlab.org/2014/03/arabic-warning-maliciously-repackaged-psiphon/)

Morgan Marquis-Boire, John Scott-Railton, Claudio Guarnieri, and Katie Kleemola, "Police Story: Hacking Team's Government Surveillance Malware," Citizen Lab, June 24, 2014, https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/

This report analyzes Hacking Team's Android implant, and uses new documents to illustrate how their Remote Control System (RCS) interception product works. RCS is a surveillance malware toolkit marketed for "lawful interception" use. We identified and analyzed RCS Android implants that had lures with a political subtext suggesting targets in the Qatif Governorate of Saudi Arabia. Analysis of these implants revealed a range of surveillance functions.

Bill Marczak, John Scott-Railton, Morgan Marquis-Boire and Vern Paxson, "When Governments Hack Opponents: A Look at Actors and Technology," 23rd USENIX Security Symposium (USENIX Security 14), August 2014, https://www.usenix.org/conference/usenix-security14/technical-sessions/presentation/marczak

Repressive nation-states have long monitored telecommunications to keep tabs on political dissent. The Internet and online social networks, however, pose novel technical challenges to this practice, even as they open up new domains for surveillance. We analyze an extensive collection of suspicious files and links targeting activists, opposition members, and nongovernmental organizations in the Middle East over the past several years. We find that these artifacts reflect efforts to attack targets' devices for the purposes of eavesdropping, stealing information, and/or unmasking anonymous users. We describe attack campaigns we have observed in Bahrain, Syria, and the United Arab Emirates (UAE), investigating attackers, tools, and techniques. In addition to off-the-shelf remote access trojans and the use of third-party IP-tracking services, we identify commercial spyware marketed exclusively to governments, including Gamma's FinSpy and Hacking Team's Remote Control System (RCS). We describe their use in Bahrain and the UAE, and map out the potential broader scope of this activity by conducting global scans of the corresponding command-and-control servers. Finally, we frame the real-world consequences of these campaigns via strong circumstantial evidence linking hacking to arrests, interrogations, and imprisonment.

Seth Hardy, Masashi Crete-Nishihata, Katharine Kleemola, Adam Senft, Byron Sonne, Greg Wiseman, Phillipa Gill and Ronald J. Deibert, "Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware," 23rd USENIX Security Symposium (USENIX Security 14), August 2014, https://www.usenix.org/system/files/conference/usenix-security14/sec14-paper-hardy.pdf

Targeted attacks on civil society and non-governmental organizations have gone underreported despite the fact that these organizations have been shown to be frequent targets of these attacks. In this paper, we shed light on targeted malware attacks faced by these organizations by studying malicious e-mails received by 10 civil society organizations (the majority of which are from groups related to China and Tibet issues) over a period of four years. Our study highlights important properties of malware threats faced by these organizations with implications on how these organizations defend themselves and how we quantify these threats. We find that the technical sophistication of malware we observe is fairly low, with more effort placed on socially engineering the e-mail content. Based on this observation, we develop the Targeted Threat Index (TTI), a metric which incorporates both social engineering and technical sophistication when assessing the risk of malware threats. We demonstrate that this metric is more effective than simple technical sophistication for identifying malware threats with the highest potential to successfully compromise victims. We also discuss how education efforts focused on changing user behaviour can help prevent compromise. For two of the three Tibetan groups in our study simple steps such as avoiding the use of email attachments could cut document-based malware threats delivered through e-mail that we observed by up to 95%.

Morgan Marquis-Boire, “Schrodinger’s Cat Video and the Death of Clear-Text,” Citizen Lab, August 15, 2014, https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/

This report provides a detailed analysis of two products sold for facilitating targeted surveillance, known as network injection appliances. These products allow for the easy deployment of targeted surveillance implants and are being sold by commercial vendors to countries around the world. Compromising a target becomes as simple as waiting for the user to view unencrypted content on the Internet. While the technology required to perform such attacks has been understood for some time, there is limited documentation of the operation of these attacks by state actors. This report provides details on the use of such surveillance solutions including how they are built, deployed, and operated.

CIVIL SOCIETY REPORTS /CAMPAIGNS

Access, “Defending against Denial of Service,” October 2011, https://www.accessnow.org/page/-/docs/Defending_Against_Denial_of_Service_1.pdf

Access, “Global Civil Society At Risk: An Overview of Some of the Major Cyber Threats Facing Civil Society,” January 2012 , https://www.accessnow.org/civil-society-at-risk

Access, “Global Civil Society At Risk: One of these things is not like the other—A report on fake domain attacks,” August 2, 2013, https://www.accessnow.org/page/-/docs/Access%20Tech/FakeDomainsReport.pdf

Access Now, Collin Anderson, Internews, Reporters Without Borders and Open Technology Institute, “Recommendations for the Implementation of the 2013 Wassenaar Arrangement Changes Regarding “Intrusion Software” and “IP Network Communications Surveillance Systems,” May 5, 2014, http://oti.newamerica.net/sites/newamerica.net/files/articles/Joint_Recommendations_Wassenaar_Implementation.pdf

Bahrain Watch, “Bahrain Government Hacked Lawyers and Activists with UK Spyware,” August 7, 2014, https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/

Bloomberg News, “Wired for Repression,” http://topics.bloomberg.com/wired-for-repression/

Bytes for All Pakistan, “Digital Security for Human Rights Defenders,” http://content.bytesforall.pk/node/9

Bytes for All Pakistan, “Loss of privacy is always permanent—Snags in hearing of FinFisher case at Lahore High Court,” August 22, 2014, https://content.bytesforall.pk/node/143

Bytes for All Pakistan, “Notorious spy technology found in Pakistan,” May 1, 2013, https://content.bytesforall.pk/node/99

Bytes for All Pakistan, “Online surveillance becomes a priority for the Human Rights Council, as Pakistan joins the wrong side of the debate,” September 25, 2013, https://content.bytesforall.pk/node/111

Bytes for All Pakistan, “Oral Statement delivered by Bytes for All, Pakistan at 23rd Regular Session of the UN Human Rights Council,” June 14, 2013, https://content.bytesforall.pk/node/103

Bytes for All Pakistan, “Privacy rights violations challenged in Lahore High Court,” May 8, 2013, https://content.bytesforall.pk/node/100

Bytes for All Pakistan, “Update: Lahore High Court Orders Inquiry into FinFisher Usage in Pakistan,” May 15, 2013, https://content.bytesforall.pk/node/101

Cindy Cohn, Trevor Timm and Jillian C. York, “Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes,” Electronic Frontier Foundation, April 17, 2012, https://www.eff.org/document/human-rights-and-technology-sales

Coalition Against Unlawful Surveillance Exports (CAUSE), http://www.globalcause.net/

Committee to Protect Journalists, “Attacks on Knight Center sites reflect digital dangers,” April 5, 2013, https://cpj.org/blog/2013/04/attacks-on-knight-center-sites-reflect-digital-dan.php

Committee to Protect Journalists, “Journalist Security Guide: Information Security,” http://www.cpj.org/reports/2012/04/information-security.php

Digital Defenders Partnership, https://digitaldefenders.org/

Digital Rights Foundation, “Pakistan is a FinFisher customer, leak confirms,” August 22, 2014, http://digitalrightsfoundation.pk/2014/08/pakistan-is-a-finfisher-customer-leak-confirms/

Electronic Frontier Foundation, “Blogger Under Fire,” https://www.eff.org/issues/defending-digital-voices

Electronic Frontier Foundation, “State-Sponsored Malware,” https://www.eff.org/issues/state-sponsored-malware

Robert Faris, Hal Roberts, Rebekah Heacock, Ethan Zuckerman and Urs Gasser, “Online Security in the Middle East and North Africa: A Survey of Perceptions, Knowledge and Practice,” Berkman Center for Internet & Society, August 1, 2011, http://cyber.law.harvard.edu/node/6973

Eva Galperin and Morgan Marquis-Boire, “Vietnamese Malware Gets Very Personal,” Electronic Frontier Foundation, January 19, 2014, https://www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal

Eva Galperin and Morgan Marquis-Boire, “The Internet is Back in Syria and so is Malware Targeting Syrian Activists,” Electronic Frontier Foundation, December 3, 2012, https://www.eff.org/deeplinks/2012/12/iinternet-back-in-syria-so-is-malware

Eva Galperin and Morgan Marquis-Boire, “Pro-Syrian Government Hackers Target Activists with Fake Anti-Hacking Tool,” Electronic Frontier Foundation, August 15, 2012, https://www.eff.org/deeplinks/2012/08/syrian-malware-post

Eva Galperin and Morgan Marquis-Boire, “New Malware Targeting Syrian Activists Uses Blackshades Commercial Trojan,” Electronic Frontier Foundation, July 12, 2012, https://www.eff.org/deeplinks/2012/07/new-blackshades-malware

Eva Galperin and Morgan Marquis-Boire, “New Trojan Spread Over Skype as Cat and Mouse game Between Syrian Activists and Pro-Syrian-Government Hackers Continues,” Electronic Frontier Foundation, June 19, 2012, https://www.eff.org/deeplinks/2012/06/darkshades-rat-and-syrian-malware

Eva Galperin and Morgan Marquis-Boire, “Trojan Hidden in Fake Revolutionary Documents Targets Syrian Activists,” Electronic Frontier Foundation, May 31, 2012, https://www.eff.org/deeplinks/2012/05/trojan-hidden-fake-revolutionary-documents-targets-syrian-activists

Eva Galperin and Morgan Marquis-Boire, “Fake Skype Encryption Tool Targeted at Syrian

Activists Promises Security, Delivers Spyware," Electronic Frontier Foundation, May 2, 2012, https://www.eff.org/deeplinks/2012/05/fake-skype-encryption-tool-targeted-syrian-activists-promises-security-delivers

Eva Galperin and Morgan Marquis-Boire, "New Wave of Facebook Phishing Attacks Targets Syrian Activists", Electronic Frontier Foundation, April 24, 2012, https://www.eff.org/deeplinks/2012/04/new-wave-facebook-phishing-attacks-targets-syrian-activists

Eva Galperin and Morgan Marquis-Boire, "Campaign Targeting Syrian Activists Escalates with New Surveillance Malware," Electronic Frontier Foundation, April 4, 2012, https://www.eff.org/deeplinks/2012/04/campaign-targeting-syrian-activists-escalates-with-new-surveillance-malware

Eva Galperin and Morgan Marquis-Boire, "Syrian Activists Targeted With Facebook Phishing Attack," Electronic Frontier Foundation, March 29, 2012, https://www.eff.org/deeplinks/2012/03/pro-syrian-government-hackers-target-syrian-activists-facebook-phishing-attack

Eva Galperin and Morgan Marquis-Boire, "Fake YouTube Site Targets Syrian Activists With Malware," Electronic Frontier Foundation, March 15, 2012, https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware

Freedom House, "2013 Freedom on the Net," October 3, 2013, http://freedomhouse.org/report-types/freedom-net

Freedom House, "What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World," Freedom House, 2014, http://www.freedomhouse.org/report/special-reports/what-next-quest-protect-human-rights-defenders-and-journalists-digital-world

Hankey, S. and Clunaigh, D., "Rethinking risk and security of human rights defenders in the digital age," Journal of Human Rights Practice (2013) 5 (3): 535-547 doi:10.1093/jhuman/hut023, http://jhrp.oxfordjournals.org/content/5/3/535.full

Human Rights Watch, "'They Know Everything We Do' - Telecom and Internet Surveillance in Ethiopia," March 25, 2014, https://www.hrw.org/reports/2014/03/25/they-know-everything-we-do

Index on Censorship, "Global coalition of NGOs call to investigate and disable FinFisher's espionage equipment in Pakistan," May 13, 2013, http://www.indexoncensorship.org/2013/05/global-coalition-of-ngos-call-to-investigate-and-disable-finfishers-espionage-equipment-in-pakistan/

International Principles on the Application of Human Rights to Communications Surveillance, July 10, 2013, https://en.necessaryandproportionate.org/text

Internews, “SaferJourno: Digital Security Resources for Media Trainers,” 2014, https://saferjourno.internews.org/

Frankie Li, Anthony Lai and Ddl Ddl, “Evidence of Advanced Persistent Threat: A Case Study of Malware for Political Espionage,” Proceedings of the 2011 Sixth International Conference on Malicious and Unwanted Software, 2011, http://dl.acm.org/citation.cfm?id=2359579

Tim Maurer, Edin Omanovic and Ben Wagner, “Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age,” New America Foundation, March 2014, http://newamerica.net/sites/newamerica.net/files/policydocs/Uncontrolled_Surveillance_March_2014.pdf

Robert Morgus, “Summer of Surveillance Revelations Highlights Spread of Spy Tech to Repressive Regimes,” August 28, 2014, http://oti.newamerica.net/blogposts/2014/summer_of_surveillance_revelations_highlights_spread_of_spy_tech_to_repressive_regi_1

PEN International, “Digital Freedom,” http://www.pen-international.org/digital-freedom/

Privacy International, “Big Brother Inc.,” https://www.privacyinternational.org/campaigns/big-brother-inc

Privacy International, “Surveillance Industry Index,” https://www.privacyinternational.org/sii

Privacy International, “Privacy International commences legal action against British government for failure to control exports of surveillance technologies,” July 19, 2012, https://www.privacyinternational.org/press-releases/privacy-international-commences-legal-action-against-british-government-for-failure

Privacy International, “Has Hacking Team’s government trojan been used against journalists?,” August 7, 2012, https://www.privacyinternational.org/blog/has-hacking-teams-government-trojan-been-used-against-journalists

Privacy International, “Privacy International calls on HMRC to investigate Gamma International’s potential breach of UK export laws,” December 26, 2012, https://www.privacyinternational.org/press-releases/privacy-international-calls-on-hmrc-to-investigate-gamma-internationals-potential

Privacy International, “Our OECD complaint against Gamma International and Trovicor,” February 5, 2013, https://www.privacyinternational.org/blog/our-oecd-complaint-against-gamma-international-and-trovicor

Privacy International, “A guide to the Wassenaar Arrangement,” December 10, 2013, https://www.privacyinternational.org/blog/a-guide-to-the-wassenaar-arrangement

Privacy International, “Privacy International seeking investigation into computer spying on refugee in UK,” Feburary 17, 2014, https://www.privacyinternational.org/press-releases/privacy-international-seeking-investigation-into-computer-spying-on-refugee-in-uk

Privacy International, “Privacy International files criminal complaint on behalf of Bahraini activists targeted by spyware FinFisher,” October 13, 2014, https://www.privacyinternational.org/news/press-releases/privacy-international-files-criminal-complaint-on-behalf-of-bahraini-activists

Ranking Digital Rights, http://rankingdigitalrights.org/

Reporters Without Borders, “Enemies of the Internet 2013,” 2013, http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf

Reporters Without Borders, “Enemies of the Internet 2014,”, 2014, http://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf

Steven Adair and Ned Moran, “Cyber Espionage & Strategic Web Compromises – Trusted Websites Serving Dangerous Result,” Shadowserver, May 15, 2012, http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/

Tibet Action, “Safe Travels Online,” https://tibetaction.net/safetravels/

Tibet Action, “Mobile Phone Security,” https://tibetaction.net/mobile-security/

Tibet Action, “Detach from Attachments,” https://tibetaction.net/detach-from-attachments-english/

Tibet Action, “Think Before You Click,” https://tibetaction.net/think-before-you-click/

Tor, “Activists in Iran and Syria Targeted with Malicious Computer Software,” March 15, 2012, https://blog.torproject.org/blog/activists-iran-and-syria-targeted-malicious-computer-software

Trevor Timm, “Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA,” Electronic Frontier Foundation, February 21, 2012, https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa

Trevor Timm, “SpyTech Companies & Their Authoritarian Customers, Part I: FinFisher and Amesys,” Electronic Frontier Foundation, February 16, 2012, https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys

Trevor Timm, “Next Step: Identifying Customers of Surveillance Technology Companies and Turning up the Heart,” Electronic Frontier Foundation, December 21, 2011, https://www.eff.org/deeplinks/2011/12/next-step-identifying-customers-surveillance-technology-companies-and-turning-heat

Ben Wagner and Claudio Guarnieri, “German Companies Are Selling Unlicensed Surveillance Technologies to Human Rights Violators – and Making Millions,” Global Voices Advocacy, September 5, 2014, http://globalvoicesonline.org/2014/09/05/exclusive-german-companies-are-selling-unlicensed-surveillance-technologies-to-human-rights-violators-and-making-millions/

Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York and John Palfrey, “Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites,” Berkman Center for Internet & Society, December 2010, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf

SECURITY INDUSTRY REPORTS AND RESOURCES

9b+, “Watching Attackers Through Virustotal,” September 1, 2014, http://blog.9bplus.com/watching-attackers-through-virustotal/

Steven Adair, “The Comment Group - Long Term Cyber Espionage,” Shadowserver, February 22, 2013, http://blog.shadowserver.org/2013/02/22/comment-group-cyber-espionage-additional-information-clarification/

Kurt Baumgartner, Costin Raiu and Denis Maslennikov, “Android Trojan Found in Targeted Attack,” Kaspersky Lab Securelist, March 26, 2013, http://securelist.com/blog/incidents/35552/android-trojan-found-in-targeted-attack-58/

Kurt Baumgartner, “Cyber Attacks Against Uyghur Mac OSX Users Intensify,” Kaspersky Lab Securelist, February 13, 2013, http://securelist.com/blog/incidents/64259/cyber-attacks-against-uyghur-mac-os-x-users-intensify/

Kurt Baumgartner, “Central Tibetan Administration Website Compromised,” Kaspersky Lab Securelist, August 12, 2013, http://securelist.com/blog/incidents/57476/central-tibetan-administration-website-strategically-compromised/

Jaime Blasco, “New MaControl Variant Targeting Uyghur Users, the Windows Version using Gh0st RAT,” Alien Vault, June 29, 2012, http://www.alienvault.com/open-threat-exchange/blog/new-macontrol-variant-targeting-uyghur-users-the-windows-version-using-gh0s

Jamie Blasco, “Targeted Attacks Against Tibetan Organizations,” Alien Vault, March 13, 2012, http://www.alienvault.com/open-threat-exchange/blog/targeted-attacks-against-tibet-organizations

Jaime Blasco, “Latest Adobe PDF Exploit Used to Target Uyghur and Tibetan Activists,” Alient Vault, March 14, 2013, http://www.alienvault.com/open-threat-exchange/blog/latest-adobe-pdf-exploit-used-to-target-uyghur-and-tibetan-activists

Jamie Blasco, “Cyber Espionage Campaign Against the Uyghur Community, Targeting MacOSX Systems,” Alien Vault, February 13, 2013, http://www.alienvault.com/open-threat-exchange/blog/cyber-espionage-campaign-against-the-uyghur-community-targeting-macosx-syst

Jamie Blasco, “Thailand NGO Site Hacked and Serving Malware,” Alien Vault, June 28, 2012, http://www.alienvault.com/open-threat-exchange/blog/thailand-ngo-site-hacked-and-serving-malware

Jamie Blasco, “CVE-2012-0158, Tibet, Targeted Attacks and so on, “ Alien Vault, April 18, 2012, http://www.alienvault.com/open-threat-exchange/blog/cve-2012-0158-tibet-targeted-attacks-and-so-on

Jamie Blasco, “Targeted attacks against Tibet organizations,” Alien Vault, March 13, 2012, http://www.alienvault.com/open-threat-exchange/blog/targeted-attacks-against-tibet-organizations

Jaime Blasco, “AlienVault Tibet Related Research Now Used to Target Tibetan Non-Governmental Organizations,” Alient Vault, March 19, 2012, http://www.alienvault.com/open-threat-exchange/blog/alienvault-tibet-related-research-now-used-to-target-tibetan-non-government

Contagio Malware Dump, http://contagiodump.blogspot.ca/

CrowdStrike, “Deep in Thought: Chinese Targeting of National Security Think Tanks,” July 7, 2014, http://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/index.html

F-Secure, “Targeted attacks in Syria,” May 3, 2012, http://www.f-secure.com/weblog/archives/00002356.html

F-Secure, “New Mac Malware Found on Dalai Lama Related Website,” December 3, 2012, http://www.f-secure.com/weblog/archives/00002466.html

F-Secure, “FinFisher Range of Attack Tools,” August 30, 2013, http://www.f-secure.com/weblog/archives/00002601.html

F-Secure, “Another Document Targeting Uyghur Mac Users,” April 25, 2013, http://www.f-secure.com/weblog/archives/00002546.html

F-Secure, “Flash Exploit Targets Uyghur Website,” March 13, 2013, http://www.f-secure.com/weblog/archives/00002524.html

Sergey Golovanov, “Spyware. HackingTeam,” Kaspersky Lab Securelist, April 23, 2013, http://securelist.com/analysis/publications/37064/spyware-hackingteam/

Thoufique Haq, “New Targeted Attack on Taiwanese Government & Tibetan Activists Open up a Can of Warms - GrayPigeon, Hangame & Shiqiang Gang,” FireEye, April 18, 2013, http://www.fireeye.com/blog/technical/targeted-attack/2013/04/new-targeted-attack-on-taiwanese-government-tibetan-activists-open-up-a-can-of-worms-graypigeon-hangame-shiqiang-gang.html

Kaspersky Lab, “The Syrian Malware House of Cards,” August 18, 2014, https://securelist.com/blog/research/66051/the-syrian-malware-house-of-cards/

Kaspersky Lab, “The NetTraveler,” June 4, 2013, http://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/

Frankie Li, “A Detailed Analysis of an Advanced Persistent Threat Malware,” SANS Institute, October 13, 2011, http://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware-33814

Mandiant, “The Advanced Persistent Threat,” 2010, https://www.mandiant.com/resources/mandiant-reports/

Mandiant, “APT1: Exposing one of China’s cyber espionage units,” February 18, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Erika Mendoza, “NGOs Targeted with Backdoors,” Trend Micro, January 1, 2012, http://blog.trendmicro.com/trendlabs-security-intelligence/human-rights-organizations-possible-new-targets/

Costin Raiu, “NetTraveler is Back: The ‘Red Star’ APT Returns with New Tricks,” Kaspersky Lab Securelist, September 3, 2013, http://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/

Costin Raiu, “A Gift for Dalai Lama’s Birthday,” Kaspersky Lab Securelist, July 4, 2012, http://securelist.com/blog/incidents/33351/a-gift-for-dalai-lamas-birthday-23/

Costin Raiu, “New MacOSX Backdoor Variant Used in APT Attacks,” Kaspersky Lab Securelist, June 29, 2012, http://securelist.com/blog/events/33214/new-macos-x-backdoor-variant-used-in-apt-attacks-7/

Costin Raiu and Kurt Baumgartner, “NetTraveler APT Gets a Makeover for 10th Birthday,” Kaspersky Lab Securelist, August 27, 2014, http://securelist.com/blog/research/66272/nettraveler-apt-gets-a-makeover-for-10th-birthday/

Trend Micro, “Luckycat Redux: Inside an APT Campaign with Multiple Targets in India and Japan,” March 29, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf

Nart Villeneuve, “Trends in Targeted Attacks”, Trend Micro, October 2011, http://www.trendmicro.ca/media/wp/trends-in-targeted-attacks-whitepaper-en.pdf

Nart Villeneuve, Ned Moran, Thoufique Haq, and Mike Sott, “Operation Saffron Rose,” FireEye, May 13, 2014, http://www.fireeye.com/resources/pdfs/fireeye-operation-saffron-rose.pdf

Websense Security Labs, “The Amnesty International UK website was compromised to serve Gh0st RAT,” May 11, 2012, http://community.websense.com/blogs/securitylabs/archive/2012/05/11/amnesty-international-uk-compromised.aspx

Weedon, Jen, “NGOs: Fighting Human Rights Violations and, Now, Cyber Threat Groups,” FireEye, April 24, 2014, http://www.fireeye.com/blog/technical/2014/04/ngos-fighting-human-rights-violations-and-now-cyber-threat-groups.html

Vyacheslav Zakorzhevksy, "New Flash Player 0-Day (CVE-2014-0515) Used in Watering-hole Attacks," Kaspersky Lab Securelist, April 28, 2014, http://securelist.com/blog/incidents/59399/new-flash-player-0-day-cve-2014-0515-used-in-watering-hole-attacks/

The Dark Visitor, http://www.thedarkvisitor.com/

DIGITAL SECURITY TOOLS

This section contains a series of guides and online resources on digital security. Digital security is highly specific to an individual or group's context and environment, and no one guide or tool can address all possible risks. We do not endorse any particular products or services.

Access, "Protecting Your Security Online," https://www.accessnow.org/pages/protecting-your-security-online

Association for Progressive Communications, "Digital Security First-Aid Kit for Human Rights Defenders," https://www.apc.org/en/irhr/digital-security-first-aid-kit

CloudFlare, "Protect Galileo: DDoS attack protection for at-risk public interest websites," http://www.cloudflare.com/galileo

Digital Defenders Project, "The Digital First Aid Kit," 2014, https://digitaldefenders.org/digitalfirstaid/

Electronic Frontier Foundation, "Surveillance Self-Defense," 2014, https://ssd.eff.org/

Free Software Campaign, "Email Self-Defense Guide," 2014, https://emailselfdefense.fsf.org/en/

Google, "Project Shield," https://projectshield.withgoogle.com/en/

Reporters Without Borders, "Handbook for Bloggers and Cyber-Dissidents," 2008, http://www.rsf.org/IMG/pdf/guide_gb_md-2.pdf

Tactical Technology Collective and Front Line Defenders, "Security In-A-Box," https://securityinabox.org/

GOVERNMENT RESOURCES

Organization for Security and Co-operation in Europe (OSCE), "Joint declaration on freedom of expression and the Internet," June 1, 2011, http://www.osce.org/fom/78309

European Union, "No Disconnect strategy," http://europa.eu/rapid/press-release_IP-11-1525_en.htm?locale=en

Marietje Schaake, "European Parliament endorses stricter European export control of digital arms," October 23, 2012, http://www.marietjeschaake.eu/2012/10/ep-steunt-d66-initiatief-controle-europese-export-digitale-wapens/

Stop Digital Arms Trade, http://www.stopdigitalarms.eu/

The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," December 12, 2013, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

INDUSTRY AND MULTI-STAKEHOLDER INITIATIVES

Global Network Initiative
http://www.globalnetworkinitiative.org/

The Global Network Initiative is a collection of ICT companies, civil society organizations, investors, and academics which aims to provide guidance, expertise and policy engagement to ICT companies on issues of protecting and advancing rights to privacy and freedom of expression.

Telecommunications Industry Dialogue
http://www.telecomindustrydialogue.org/home

The Telecommunications Industry Dialogue is a group of telecommunications operators and vendors who jointly address freedom of expression and privacy rights in the telecommunications sector in the context of the UN Guiding Principles on Business and Human Rights. The initiative was launched in March of 2013.

INTERNATIONAL ORGANIZATION AND INTERNATIONAL LEGAL RESOURCES

The following United Nations declaration and covenants form the basis for the definition of “human rights” used in this study:

United Nations General Assembly, “Universal Declaration of Human Rights,” December 10, 1948, http://www.un.org/en/documents/udhr/

United Nations General Assembly, “International Covenant on Civil and Political Rights,” December 16, 1966, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

United Nations General Assembly, International Covenant on Economic, Social and Cultural Rights, 16 December 1966, http://www.ohchr.org/EN/ProfessionalInterest/Pages/cescr.aspx

A number of reports, guides and resolutions by United Nations bodies and the European Commission have specifically dealt with the issue of human rights and ICTs:

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, “Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,” May 17, 2010, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement

John Ruggie, “Guiding principles on business and human rights: Implementing the United Nations “Protect, Respect and Remedy,” Framework, 2011, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

UN Human Rights Council, “The promotion, protection and enjoyment of human rights on the Internet,” June 29, 2012, http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement

European Commission, “ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights,” 2013, http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business_en.pdf

Frank La Rue, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,” April 17, 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

United Nations Group of Governmental Experts, “Developments in the Field of Information and Telecommunications in the Context of International Security,” June 24, 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98

United Nations General Assembly, “The right to privacy in the digital age,” November 20, 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1

Office of the United Nations High Commissioner for Human Rights, “The right to privacy in the digital age,” June 30, 2014, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf