DOI:10.1145/3199477

The U.S. State Department's Internet Freedom agenda is being adapted to help them communicate without DNS and IP address filtering.

BY RICHARD R. BROOKS, LU YU, YU FU, OLUWAKEMI HAMBOLU, JOHN GAYNARD, JULIE OWONO, ARCHIPPE YEPMOU, AND FELIX BLANC

Internet Freedom in West Africa: Technical Support for Journalists and Democracy Advocates

key insights

- West African governments try to restrict access through Internet blackouts and invasive surveillance, and pro-democracy movements use the Internet to promote free and fair elections.
- Innovative technologies for avoiding detection produced by criminal botnets are being adapted by legitimate network services to increase network privacy and security.
- What we viewed as a purely technical project helped launch a grassroots movement promoting freedom of expression, transparency, and democracy in West Africa that subsequently also influenced the social, economic, and political frameworks there.

IN DEVELOPED COUNTRIES, Internet penetration is near saturation and population growth is stagnant. In contrast, the African population is young and growing quickly. UNICEF estimates that by the end of the century, 40% of the world's population will be African.[a] Where Africa in May 2016 had 16% Internet penetration, the McKinsey Global Institute predicted

a https://www.unicef.org/publications/files/UNICEF_Africa_Generation_2030_en_11Aug.pdf

Opposition supporters protest at the Place de la Nation in Burkina Faso's capital Ouagadougou, November 2, 2014.

IMAGE BY ISSOUF SANOGO/AFP/GETTY IMAGES

in 2013 that by 2025 the penetration rate will be approximately 50%[b] and that 600 million Africans will be using the Internet,[c] producing approximately $75 billion in annual e-commerce activity and contributing $300 billion to African GDP.

West Africa is a diverse region in sub-Saharan Africa, including both the Sahel desert and lush rain forests. Many local languages from distinct language groups are spoken, along with the former colonial languages, including French, Spanish, Portuguese, and English. The region includes thriving democracies like Ghana (with press freedom ranked by Reporters Without Borders better than France and the U.K.) and repressive regimes like Equatorial Guinea (with press freedom ranked by Reporters Without Borders at the level of Cuba, Eritrea, Iran, and North Korea). The majority of the West African population lives in countries that do not allow effective freedom of expression.[d,e]

This article discusses Internet freedom in West Africa. In April 2016, we completed a project sponsored by the U. S. State Department's Bureau of Democracy, Human Rights, and Labor, whose goal was to promote online freedom of expression by West African activists. To this end, we implemented a distributed proxy network and held

b https://www.mckinsey.com/industries/high-tech/our-insights/lions-go-digital-the-internets-transformative-potential-in-africa

c According to http://www.internetworldstats.com/stats.htm, there are approximately 320 million Internet users in North America and approximately 630 million Internet users in Europe.

d https://freedomhouse.org/sites/default/files/FH_FTOP_2016Report_Final_04232016.pdf

e https://rsf.org/en/ranking

annual training sessions. Our proxy counters Internet censorship and surveillance, following a design loosely modeled on criminal botnets.

Our training sessions provided participants the skills they needed to protect their freedom of expression, bringing together a regional community of bloggers, technologists, journalists, and democracy advocates. Trainees from multiple countries found they were facing similar problems.

Internet Freedom

Though freedom of expression is guaranteed by Article 19 of the United Nations Universal Declaration of Human Rights (http://www.un.org/en/universal-declaration-human-rights/index.html), the world's ability to access information and openly express opinions is tenuous and unevenly distributed. The non-governmental organization (NGO) Freedom House's 2016 report on press freedom said that global press freedom was at its lowest point in 12 years.[f]

Non-democratic countries with poor human rights records maintain power by tightly controlling information, limiting their populations' ability to share opinions, organize, and create democratic alternatives. For these governments, the traditional press is easier to control than the Internet. They can physically intervene in print and broadcast media operations. Newspaper distribution networks are expensive to maintain and easily disrupted. In almost every country, radio and television broadcasters are controlled, or licensed, by the government.

In contrast to traditional media, it is inexpensive and less risky to put a web server online in another country. In countries where the population does not trust traditional media, social media has emerged as an alternative. As more voices become available to the population, fearing a loss of control, repressive governments invest in technologies for shriveling and censoring Internet traffic. Firewalls can block the domain name system (DNS) and/or Internet Protocol (IP) addresses of offending news sites (such as *The New York Times*). Internet surveillance tools using deep packet inspection (DPI) can block network sessions containing sensitive keywords. DPI tools are often considered "dual-use," along with legitimate network management, making it difficult to regulate the export of these technologies.

Repressive governments subject dissenting voices to denial-of-service (DoS) attacks that are inexpensive,[g] difficult to attribute, and make objectionable viewpoints unavailable. Governments hire cheap, unskilled laborers to flood websites with either pro-government "50-cent army" or abusive troll comments. If all else fails, a government can simply shut off the Internet and other telecommunications technologies during politically sensitive times. In 2017, the governments of Cameroon, the Democratic Republic of Congo, and Gabon all used Internet blackouts as a political tool.

To protect the freedom of expression guaranteed in Article 19, NGOs and Western governments try to foster Internet freedom. Technical tools, like The Onion Router, or Tor,[h] Psiphon,[i] uProxy,[j] and Lantern,[k] provide proxy services for evading national firewalls. Trainers teach at-risk populations to use the Internet securely, avoid surveillance, and circumvent censorship. NGOs lobby governments and international groups to put in place laws and policies to safeguard the public's freedom of expression. Our project promoted Internet freedom within West Africa, producing a censorship-circumvention tool and building a West African user community. This article documents our experiences.

West African press freedom. As shown in the table here,[l] freedom of expression in Africa is being confronted by special challenges. Approximately 40% of the countries in sub-Saharan Africa (over 38% of the population) live in countries whose press freedom

West African freedom surveys populations from the *CIA World Factbook*, 2016 (https://www.cia.gov/library/publications/the-world-factbook/); RSF columns from Reporters Sans Frontières, 2010 and 2017 (https://rsf.org/en/ranking); and FH FIW columns from Freedom House Freedom in the World, 2010 and 2017 (https://freedomhouse.org/report-types/freedom-world).

Country	Population	2010 RSF	2017 RSF	2010 FH FIW	2017 FH FIW	Users
Benin	10,741,458	70	78	Free	Partly Free	8
Burkina Faso	19,512,533	49	42	Partly Free	Partly Free	5
Camer.	24,360,803	129	130	Not free	Not Free	8
Chad	11,852,462	112	121	Not Free	Not Free	6
Cote d'Ivoire	23,740,424	118	81	Not Free	Partly Free	39
Congo (Kinshasa)	81,331,050	148	154	Not Free	Not Free	2
Djibouti	846,687	110	172	Partly Free	Not Free	3
Equat. Guinea	759,451	167	171	Not Free	Not Free	1
Gabon	1,738,541	107	108	Not Free	Not Free	1
Gambia	2,009,648	125	143	Partly Free	Not Free	15
Guinea	12,093,349	113	101	Not Free	Not Free	4
Liberia	4,299,994	84	94	Partly Free	Partly Free	2
Mali	17,467,108	26	116	Free	Partly Free	1
Niger	18,638,600	104	61	Partly Free	Partly Free	1
Nigeria	186,053,386	146	122	Partly Free	Partly Free	4
Sierra Leone	6,018,888	91	85	Partly Free	Partly Free	3
Senegal	14,320,055	93	58	Partly free	Partly Free	7
Togo	7,756,937	60	86	Partly Free	Partly Free	12

RSF = Reporters Without Borders
FH FIW = Freedom House Freedom In the World

f https://freedomhouse.org/sites/default/files/FH_FTOP_2016Report_Final_04232016.pdf

g Reports (2016) suggest distributed DoS (DDoS) attacks can be ordered online for as little $5 per hour; https://www.incapsula.com/blog/unmasking-ddos-for-hire-fiverr.html

h https://www.torproject.org/

i https://psiphon3.com/en/index.html

j https://www.uproxy.org/

k https://getlantern.org/

l Population statistics from *The CIA World Factbook* (https://www.cia.gov/library/publications/the-world-factbook/); RSF rankings from Reporters Without Borders, 2010 and 2017, with 1 as best (such as Norway) and 180 as worst (such as North Korea); and qualitative rankings from Freedom House Freedom in the World, 2010 and 2017 (https://freedomhouse.org/report-types/freedom-world).

is ranked by Freedom House as "not free," and more than 61% of the population lives in countries ranked as "partly free." The West African countries with the lowest press-freedom rankings are The Gambia and Equatorial Guinea.[m] The Gambia is a small, English-speaking country surrounded by larger, French-speaking Senegal. Many Gambian journalists have lived in exile to avoid persecution. Its 2016 election, which removed the former strongman, may yet change its ranking. Equatorial Guinea is a small, Spanish-speaking country between Cameroon and Gabon, with large oil reserves producing revenues that go mainly to the ruling family. Trainees told us that Equatorial Guinea blocks access to social media.

Freedom House gave both countries the lowest possible ranking for political rights in 2016. Independent of our work, a pan-African group augmented Article 19 by drafting a comprehensive African Declaration on Internet Rights and Freedoms[n] to put in place African norms in support of online freedom of expression.

Other countries in the region have relatively positive rankings for their press freedom. We had participants from Benin, which is ranked as "partly free," with one of the better rankings in West Africa (Reporters Sans Frontières ranks Benin next to Italy). Training participants from Benin still feared legal proceedings meant to intimidate political speech. During our training sessions, 2012 to 2016, the status in some countries improved. Côte D'Ivoire (Ivory Coast) moved from "not free" to "partly free," and Senegal's rankings improved. The only available statistics for Internet Freedom in Africa can be found in Freedom House's series of Internet Freedom Reports,[o] which increased the number of African countries it covers from six in 2011 to 16 in 2016. Unfortunately, only two West African countries—The Gambia and Nigeria—were included, thus limiting our ability to provide objective demographics here.

Activist community. We worked with bloggers, journalists, and activists. Bloggers use multiple platforms to express opinions and inform local populations about political, economic, and ecological developments. Journalists were dedicated to their profession in situations with limited monetary reward and real physical danger. Some of those we trained were international correspondents working in West Africa for international broadcasters, including representatives of the Committee for the Protection of Journalists, International Federation of Journalists, and local journalist unions. The "users" column in the table lists the number of participants from each country,[p] not including international correspondents.

Our activist community included human rights and technical activists. The region has a growing open source and maker community that is politically engaged, promoting economic, social, intellectual, and political democratic development in the region. Approximately 15% of our participants were female, and approximately 20% were primarily technical activists; the remaining 80% were about evenly split between bloggers and professional journalists. These numbers are inexact in part because participants were not easily categorized, and some had their own businesses providing both content and technical services.

Internet influence. All participants used the Internet, including social-media platforms, giving them a strong voice. The government of The Gambia recognized the power of the Internet in 2013 by passing a law that punishes its use to "spread dissatisfaction with the government" with fines over $100,000 and 15 years in jail.[q] The influential Balai Citoyen[r] (Burkina Faso) and Y'en a Marre[s] (Senegal) movements had used the combined influence of musicians and web activists to bring about free and fair democratic elections since 2011. Repressive governments and free-expression activists alike were aware of the power of the Internet and new media, using them to advance their agendas.

Internet censorship and attacks on free speech in West African countries have not attracted as much attention as censorship in countries like China and Iran. Only limited information has been available regarding network surveillance and censorship in West Africa, let alone use of censorship-circumvention tools there. Although our project was not intended to collect statistics, we learned the reality of the situation from the trainees. We generated reports that circulated among the human rights community. The fact that Freedom House increased the number of sub-Saharan countries in its *Freedom on the Net* reports[t] since 2010 indicates increased awareness by the international community of the situation in the region.

Our Project

Clemson University and Syre Inc. designed our project to adapt the U.S. State Department's Internet Freedom agenda to the needs of West Africa. We recruited the NGO Internet Without Borders (Internet Sans Frontières) as a liaison with the human rights community in sub-Saharan Africa. The project had two main objectives: develop secure messaging tools based on author Brooks's research at Clemson University tailored to local needs; and provide bilingual (English and French) training for the West African user community.

Proxy networks. Tools are available for circumventing censorship, many providing proxy connections to Internet users. A local client initiates a connection to a remote server through an encrypted "tunnel," and the remote computer executes actions requested by the local host, returning results to the local host through the tunnel. We now discuss the Tor, Psiphon, Lantern, and uProxy proxy systems. Proxy networks and virtual private networks (VPNs) help users circumvent surveillance and censorship but are not perfect solutions:

National firewall. A national firewall can track remote connections, detect DNS/IP addresses used by proxies, and block suspect addresses. Censors use DPI to identify addresses with suspect content;

m https://freedomhouse.org/sites/default/files/FH_FTOP_2016Report_Final_04232016.pdf
n http://africaninternetrights.org
o https://freedomhouse.org/report-types/freedom-net
p See the table for demographic and human rights data on the countries discussed here.
q https://freedomhouse.org/report/freedom-net/freedom-net-2015
r English translation: "A citizen's broom sweeps clean."
s English translation: "We are fed up."
t https://freedomhouse.org/report/freedom-net/freedom-net-2015

Proxy connections. Proxy connections can be security risks at both ends. Clients can have sessions spied on by the proxy server. Servers can be made responsible for client actions that seem to be from the local machine; and

Latency and jitter. Increased latency and jitter hinder user acceptance.[4] Even users aware of local censorship and surveillance risks tend to use faster direct Internet connections.

Each proxy has its own strategy for overcoming these drawbacks. Psiphon[u] is a one-hop proxy with multiple modes, including one that hides its use of encryption. It avoids nation-state firewall blocking by running a large, international park of proxy nodes that are difficult to enumerate and providing access options that obfuscate the connection. The proxy nodes are provided by Psiphon, making Psiphon potentially liable for criminal abuse. (An online system allows Chinese users to rank the speed and stability of existing proxy solutions, https://cc.greatfire.org/en; from here on, we include, in parentheses, its ranking of each proxy as of June 2017, if the proxy was present in the survey.) For example, Psiphon (11) users have to trust Psiphon not to spy on proxy connections and exploit session information.

The Tor[v] (9) proxy network tunnels connections through three, separately encrypted hops. To protect user privacy, entry into the Tor network is normally through a small number of trusted guard nodes. Tor provides advice to help exit-node providers minimize their legal risk, primarily by telling ISPs in advance that the node is a Tor exit node. Exit nodes have been used to spy on users in the past. It is unwise to send personally identifiable information through Tor. Tor's use of two additional network connections to increase anonymity adds more latency and jitter than one-hop proxies. Many countries block Tor. Iran has blocked SSL/TLS connections, which block Tor. China blocks connections to IP addresses that run Tor. China looks for the TLS cipher lists that indicate Tor use. Some countries actively probe and blacklist nodes they suspect of providing access to Tor. Tor counters such blocks by maintaining a set of reserve (bridge) addresses that become available as needed, though this set of nodes sometimes is scarce. Tor is also implementing pluggable transport[w] (PT) layers that modify the network transport layer and disguise Tor traffic. Unfortunately, each PT is usually supported by only a small number of bridges; a PT can also produce a fingerprint that can be detected.

Non-democratic countries with poor human rights records maintain power by tightly controlling information, limiting their populations' ability to share opinions, organize, and create democratic alternatives.

uProxy[x] is a browser extension for Chrome and Firefox that allows users to share their Internet connection with others. It was developed by Google Ideas, now the Jigsaw subsidiary of Alphabet, in conjunction with Lantern and the University of Washington. uProxy functionality is roughly similar to CGI-Proxy we used in our system. Ideally, a friend of a user in a repressive country would volunteer to provide a friend with a proxy connection. In this scenario, the friend risks being potentially responsible for illegal activities done by the proxy client, and the client could be spied on by the friend. Alternatively, the proxy connection can be through a commercial provider. This second scenario is basically equivalent to using a commercial VPN. As with Psiphon, the user has to trust the commercial VPN. Many users do not have friends available in countries outside the firewall, and countries with national firewalls often block the service providers (such as Github and Gmail) uProxy relies on.

Lantern[y] (6) is a product of Brave New Software, a nonprofit providing a distributed proxy, bootstrapping initial connections through Google Talk servers, but does not provide anonymity, aiming instead to provide efficient access to websites. If a site is not blocked locally, Lantern will load the material directly and not use the proxy. If a webpage is blocked locally, Lantern will retrieve the webpage through a proxy connection. Lantern maintains a distributed set of proxies for the user. Users can allow their connection to be shared. All traffic passing through the Lantern peer-to-peer system is encrypted. The distributed na-

u https://psiphon3.com/en/index.html
v https://www.torproject.org/
w https://www.torproject.org/ docs/pluggable-transports
x https://www.uproxy.org/
y https://getlantern.org/

ture of Lantern reduces, but does not eliminate, the risks of proxy use. Since only part of the session would be sent through an individual proxy exit node, the likelihood that an exit node would be blamed for the acts of a malicious user are reduced. Similarly, the amount of information an exit node can harvest from a naive user is reduced.

Our proxy design. We developed and deployed a network of peer-to-peer proxies for our user community that included journalists, human rights activists, political dissidents, and technology activists from the region. Our technical goal was to adapt tools used in the botnet community to avoid DNS and IP-address filtering. Many botnets remain active for years despite our best efforts to stop them.

Unlike Tor, Psiphon, and Lantern, which are open to the public, our tool resembles uProxy in that it is deployed by a small, trusted, authorized user community. It is similar to Lantern in that our clearinghouse maintains a dynamic list of proxies available for immediate use. Unlike other proxies, we vetted the people invited to our training sessions, and they helped define the rules we enforce in maintaining the network. To reduce the risk of using a proxy, we did the following:

Informed users of risks. We explained the risks involved in being a proxy server, with users allowed to opt out of being proxies for others;

Established a trustworthy user community. We provided the system to a small set of users, all individually vetted by our partners. Most were professional journalists, well-known bloggers, and/or human rights activists. All had strong professional credentials;

Protected privacy. We limited access to the network to only authenticated users and kept no records of user sessions;

Adopted community-defined standards. We enlisted users in defining the code of conduct to be respected by the user community;

Recognized political boundaries. We maintained a matrix segregating countries by security agreements and shared infrastructure, with proxy nodes chosen only from countries not friendly with the local users' governments; and

Created a sense of community. We had the user community meet at training sessions, with individual users deciding whether or not to be a proxy server after talking face-to-face with potential proxy clients.

Our users made fully informed decisions as to whether or not to share their network connection. The risk of acting as a proxy in this setting is less than with Tor and similar to sharing a network connection with a colleague through uProxy. It is difficult to compare this risk with the risk of being an exit node for Lantern, where users provide small slices of their bandwidth to strangers. With our system, users provide a vetted colleague with an entire session. We are the only proxy we are aware of that automatically blocks the use of proxy servers when the political stance of the exit server's country could pose a risk.

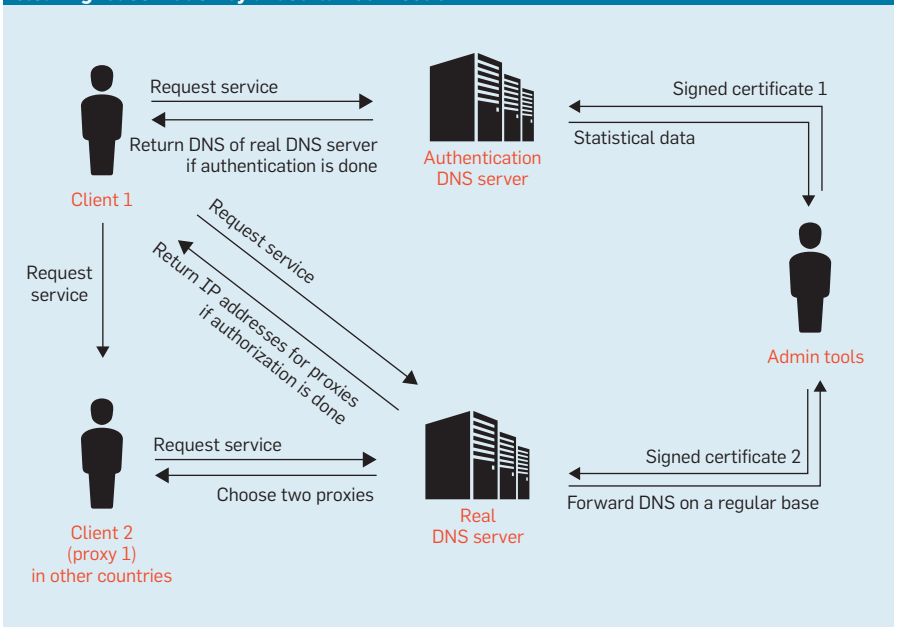
We did not conduct extensive performance comparisons between our tool and the other proxy networks. It is probably fair to assume that the connection speed and jitter of the one-hop proxies, including ours, are roughly equivalent. The observed network throughput of the connection is one factor we considered in choosing the proxy location. Worth noting is that the performance of our tool in Africa was quite different from when we tested it in North America and Europe. The Internet in Africa uses less wired infrastructure, and a number of 4G wireless providers compete for business in the urban centers.

To access our network, clients use the network protocol in Figure 1 to find the address of a remote proxy. They have a dynamically updated list of DNS names used to connect to our proxy network. It attempts to open a Secure Shell (ssh) session through a DNS tunnel to our authentication node. Password-less ssh credentials verify that the connection is from one of our authenticated users. When authentication succeeds, the local node receives the DNS name of a proxy clearinghouse node.

The local node opens a second DNS tunnel to the clearinghouse and uses Secure Copy through the DNS tunnel to retrieve the IP address of the node/proxy it can use to access the Internet for the current session. Our protocol design and implementation included a number of innovations adapted from criminal botnets to counter Internet censorship, especially DNS/IP filtering. The following sections describe the techniques we used to avoid tracking and detection.

To establish secure communication to our system's authentication servers, we had to bypass firewalls and network filters and found that many malicious botnets use DNS to communicate covertly.[1] DNS is of interest for several reasons: it is globally deployed and used; its filtering typically blocks attempts to connect to a blacklisted set of sites; and its

Figure 1. Nodes find their remote proxy partner using DNS tunneling to access a proxy clearinghouse hidden by a fast flux connection.



packets and records are rarely validated by the ISP, allowing DNS servers to be impersonated. These factors make DNS suited for use as a covert communication channel.

Besides DNS tunneling, we also adapted "fast flux" ideas created by botnets to protect our users. The term fast flux refers to frequent redefinition of the IP addresses affiliated with a DNS name. In current botnets, one symbolic DNS name is affiliated with a large number of IP addresses. The IP addresses are given "short time to live" values and swapped out frequently, generally less than three minutes. The result is a DNS name that cannot be reliably tied to any computer through its IP address (see Figure 2).

Nodes in the fast flux tend to work as proxies for a "mothership" that wants to be hidden, effectively avoiding detection and tracking by providing a moving target. This is largely why botnets have been so difficult to stop, even when law enforcement and tech vendors might conspire to track down and neutralize them.[5] Our approach applied this concept to our authentication and proxy-distribution servers to add an additional layer of redundancy and survivability. The proxy-distribution server determined what proxy would be used by the client. As with botnet fast flux, the servers moved frequently to different physical and logical locations on the Global Environment for Network Innovations (GENI) network.[z]

We also regularly changed the server's domain names. In practice, we chose them from Latin-alphabet-language words taken from Wikipedia. One alternative to this approach would be to algorithmically generate domain names[3] using an algorithm like the one in Fu et al.[2] To further obscure the network, we used dynamic DNS services to register our domain names, allowing individuals to register, at no cost, subdomains to any of a large set of volunteer root domains. This is useful, since the root domains are quite varied and have no direct connection to our project.

Criminal botnets are known to have been "sinkholed," or a law-enforcement agency anticipates the domain name that will be used and then registers that name. This allows law enforcement to identify and isolate the infected nodes, effectively dismantling the botnet. We used the following strategies to avoid sinkholing:

Refreshed DNS names. Each node regularly received, during its session, a list of DNS names the authentication server would use in the future when the current DNS name would no longer be available.

Hidden Tor service. We maintained a Tor hidden service with a user forum. Should users be disconnected from the service, we would provide a script on the forum that would provide the system with the current list of DNS names.

In practice, we had no difficulty with sinkholing and never had to use the second approach.

Hardened environment. We gave users a hardened networking environment consisting of a bootable, encrypted Linux USB drive (Linux Mint[aa]), a set of scripts that create and remove a temporary environment on Windows (encrypted using 7-Zip[ab]), or an Android app. When using the first two, no software would be installed on the user's machine, and care would be taken to avoid leaving data traces for later forensic analysis. Users had to safeguard only the encrypted USB drive. Unlike the proxy tools discussed earlier, we did not assume the user computer could be kept secure from local authorities.

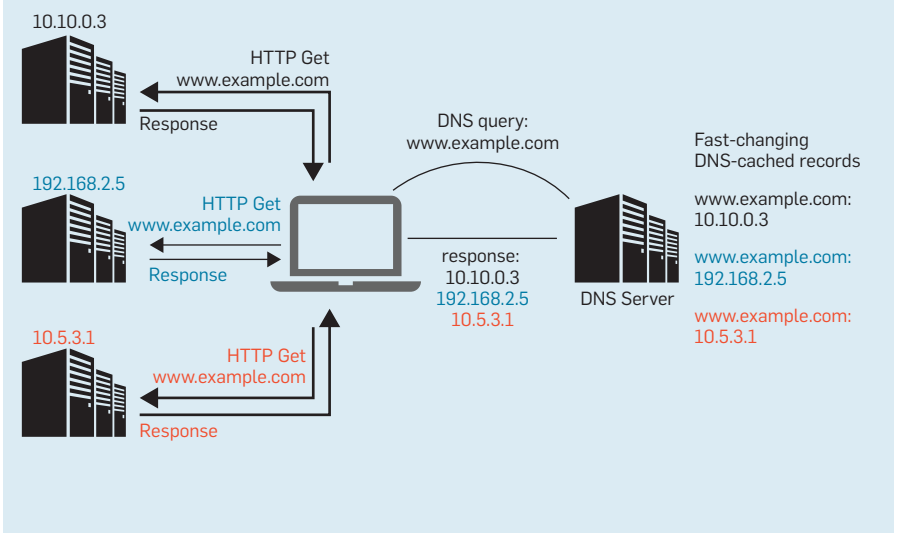
The hardened environment would automatically launch a browser using CGIProxy[ac] to access a remote proxy node launched in the hardened environment. CGI-proxy connections all use TLS, thus limiting DPI's ability to identify suspect communications.

Client hardening encrypted the work environment so even if the software would be lost or fall into the wrong hands, the risk of a user data breach and disclosure of the proxies would be greatly reduced. A strong password was required for users to extract data and use our tool.

Should hostile users acquire a copy of our tool, the amount of damage they could inflict on the system would be limited. Our user community became rather close, and it is quite likely we would have been informed of arrest, detention, or physical threats, in which case we would have disabled the user's access to the system. Even if we were unaware of a user's compromise, our matrix of political alliances and shared infrastructure would have guaranteed a

z https://www.geni.net/#

Figure 2. Fast flux.



aa Linux Mint provides full disk encryption to counter viruses and keyloggers on users' laptop computers; https://www.linuxmint.com/

ab 7-Zip is portable software for compressing or zipping files secured with encryption; http://www.7-zip.org/

ac CGI-proxy is a tool comparable to uProxy that lets nodes without web servers function as a proxy for others; https://www.jmarshall.com/tools/cgiproxy/

compromised node could connect only to nodes of no possible interest to local authorities. Any attempt to enumerate network addresses providing proxy access would have never provided information of interest to a local regime. To the best of our knowledge, this is a unique feature of our approach.

Peer-to-peer proxies. The list of proxy nodes we maintain includes only those that are currently active. In addition to proxy servers in Africa, we maintained at least four active proxy servers on the GENI network for approximately 50 users. The clearinghouse kept up-to-date information on the quality of the network connections to proxy nodes that let us do load balancing. Members of our user community also acted as proxies for each other, as shown in Figure 1.

We gave each user the choice of whether or not to act as a proxy server. This option had not been anticipated at the beginning of the project but was requested by users during training. We originally assumed solidarity with the community would lead it to provide secure connections for each other. Many expressed concern over how authorities could misuse information harvested through eavesdropping on proxy sessions on their nodes.

Internet Without Borders (http://internetsansfrontieres.org/) developed a matrix identifying countries with either mutual defense agreements or the same telecommunications providers. Proxy connections are made only through countries that are not friendly with local government and various providers. We did this to protect our user community. Proxy connections were encrypted while passing from the client through the network to the proxy but in clear text when leaving the proxy. By forcing connections through a country not aligned with the home country, it becomes functionally impossible for the home country's political authorities to survey the session. Should a node become compromised and used to harvest the addresses of our users, the home country authorities would be able to harvest only the IP addresses of users in countries with which they *do not* have friendly relations. The user community grew close and was often aware when a member was detained, thus allowing us to remove that user's credentials from the authorization node.

Repressive governments and free-expression activists alike were aware of the power of the Internet and new media, using them to advance their agendas.

Lessons learned. During deployment, we learned a number of important lessons:

Qualitatively different. The Internet in Africa is qualitatively different from the Internet in Europe and the U.S. Wired connections are rare and power disruptions are common. Most connections use 4G wireless in urban areas;

Test as soon as possible. Start testing the tool in the local environment as soon as possible. Our first version, which we tested in Europe and the U.S., delivered extremely poor quality of service on African networks;

Enlist local technologists. Enlist local technologists into the project for testing early in the process if possible. Once we began using colleagues in Abidjan and Abuja to test our system, we were able to find timing errors more quickly;

Use local technologists. Use local technologists to support other users. Many web activists who were part of coworking spaces made themselves available on short notice to help journalists;

Listen to the local participants. Listen to the local participants to learn their security problems, many of which we could not have anticipated. We had assumed users would be eager to serve as proxies for their colleagues, but many were, in fact, hesitant. This is reasonable for people living under authoritarian regimes, and we were naive not to have foreseen it;

Apply local lessons. We adapted war games from African training and used it as a class exercise for our college students who found ways to evade our surveillance we had not anticipated. We added those tools to the next set of training sessions; and

Make no assumptions. Do not make assumptions about the local security situation based on rules of Western law enforcement. Warrantless searches occur. Some users had problems with informers within their own local networks. The political situation can be changed for the better by the local population when it has access to information. Participants in our training were in groups (rap singers and web activists working together) that even managed to bring about regime change, removing entrenched governments from power.

Fadel Barro (2-L), a leader of Le Y'en a Marre (We're Fed Up) movement, and Oscibi Johann (2-R), a leader of Burkina Fasos Le Balai Citoyen (Citizens Broom), at a press conference in Kinshasa.

Proxy system comparison. Such systems vary according to how proxy nodes are chosen. Tor and Lantern users rely on public proxy nodes, though public proxy nodes have been used to spy on users. Psiphon runs its own proxies and has access to incoming and outgoing traffic. uProxy forces users to find their own proxy nodes. We were able to provide users with a community of professionally vetted colleagues they could meet face to face.

Proxies also route traffic differently. Psiphon connects users directly with nodes located mainly in Western countries. When not using the connection of a friend, uProxy uses cloud connections through Digital Ocean (sites in North America, Europe, Bangalore, and Singapore), Facebook, Github, or Google. Such a connection can be difficult to access from countries with active censorship; for example, many are blocked in China. Tor routes are chosen from nodes distributed throughout the world. Users can specify preferred nodes (and therefore countries) for entry and exit. Lantern's routing assumes individuals are *not* being targeted. Proxy routes include nodes in the local country. We assumed our users *were* being targeted. We routed traffic to proxy nodes located at either U.S. research universities or in a West African country not allied with a local government.

To the best of our knowledge, ours is the only proxy that explicitly considers political tensions in choosing how to route proxy traffic. The way Tor, Psiphon, Lantern, and uProxy maintain direct connections to proxy nodes has made them vulnerable to traffic fingerprinting, blacklisting, and active probing. Our use of fast flux was different from these existing tools. By frequently changing the DNS and IP addresses associated with our proxy, it should have been more difficult to use such techniques to disable our system. However, traffic fingerprinting would still be possible for identifying our use of DNS tunneling, and our use of DNS tunneling required very few, small messages. To date, this has not been a problem.

Training sessions. We sought out local activists who were most capable of contributing to our training sessions. We posted advertisements, used social networks, and took advantage of our connections within the African diaspora to recruit a diverse set of participants. Our plan was to have two sessions each year from 2014 to 2016, one in Abidjan, Côte D'Ivoire, and one in Paris, France. We chose Abidjan, since it is a major commercial center for West Africa with excellent travel connections. As Abidjan is a member of the Economic Community of West Africa, citizens of almost all countries in our target area did not need a visa to travel there. It also has a stable political climate. Training in Abidjan was held at a computer training facility at Université Felix Houphouet Boigny.

As the former colonial power, France still has strong cultural and economic ties to most West African countries. There is also a large African diaspora in greater Paris, and it is not unusual for African dissidents to come to France as political refugees. For the third year, we held two training sessions in Abidjan but dropped the one in Paris. During the first two years, we had already educated the members of the diaspora in France who were most influential and were having difficulty getting visas approved to travel to France to participate.

Participants. We received a large number of applicants who recognized the importance of secure Internet use for their own projects. Although most were natives of West Africa, a few were also from Europe. The Europeans worked for NGOs involved in the region or for international organizations or were journalists working for international broadcasters. The training groups included members of the International Federation of Journalists, the Committee for the Protection of Journalists, and several NGOs that preferred to not be identified. Most of the African participants were either journalists or bloggers, many also influential activists.

One participant had set up an online election-monitoring system that was largely responsible for his country's first peaceful democratic transition of power. Another worked with a group of rap musicians and tech activists who had mobilized their local populations to protest a planned change in the local constitution that would have let the local strongman remain in power for more than 27 years. Enough protesters took part to convince the country's army to ask the strongman to leave the country, leading to a free and fair election.

Participants not able to take part in the training included a blogger from Mali who continued reporting from his city even while it was occupied by Al Qaeda and a journalist working in the Central African Republic during a violent civil conflict between Christians and Muslims.

Participants reported a number of threats to Internet freedom in the region:

In Gambia. Journalists would be held by the National Intelligence Agency until they allowed access to their email messages;

In Togo. Journalists worried that communications networks would be shut down during elections and journalists detained following sensitive mobile phone conversations;

PHOTO BY FEDERICO SCOPPA/AFP/GETTY IMAGES

In the public interest. Some activists were jailed for putting online apolitical information that was clearly in the public interest; and

Forced to flee. Following training, at least three activists were forced to flee their country of origin due to threats of imprisonment or physical harm due to their online presence. Other participants helped them find safe haven in other countries.

There is a very active maker community in West Africa, including a number of free-software activists. The local tech community is socially engaged, creating maker spaces that promote technical literacy within the region. By bringing these local technicians into our training sessions, we were able to provide the democracy advocates local contacts who could provide them technical support as needed.

Curriculum. The training curriculum concentrated on Internet freedom. We surveyed the global situation, discussed surveillance and censorship technologies, and taught the user community the necessary skills. In addition to teaching them to use our proxy, we tutored them in the use of Tor, Psiphon, and encrypted email.

In the second and third years, we added new topics and deployed a Friendica open source social-network site at a .onion address on the dark web. We found that providing the community a private, secure forum it could reach only through Tor helped its members understand the tool would give them access to items unavailable through normal means. Previously, the students had noticed Tor's latency more than its strong points. Once they were used to using Tor for communicating within the community, such communication became a habit. We found that people teaching the use of privacy tools should introduce them in ways that emphasize their unique abilities. Otherwise, students would be more likely to notice some deficiency of the user interface, like, say, latency.

War (role-playing) game. We developed role-playing game scenarios where trainees would have to cooperate and share information to win. A detailed introduction of the game is available online,[ad] and we used the game as a final exam for the training. The training personnel acted as the "national intelligence agency" that would block access to Internet sites and sniff the network for "evidence." Concrete evidence of users accessing "politically sensitive" information would cause them to be "imprisoned," or expelled from the game.

The trainees were divided into groups, with players in the same group working together. Each player would choose a role in the game by picking a piece of paper from a hat. Each team included an "agent provocateur" who would inform the "national intelligence agency" of suspicious activity. The first scenario involved reporters trying to collect information about corrupt officials and the second an armed insurgency resembling Boko Haram.

The game scenarios required trainees to apply the tools they had been given without help from the instructors. They indeed had to prove their ability to outwit them. We found this to be very useful, as it was popular with the trainees, allowing them to gain confidence in their ability to use the tools. And embedding "informers" in the scenarios was an essential aspect of the game, forcing users to think about the security of their internal communications and seriously contemplate possible threat models.

After using these scenarios for instructing journalists, the author Brooks integrated them into his computer-engineering security course at Clemson University. In addition to it being a useful exercise for the course, his students managed to find some tools (notably anonymous chat services) for use in the war game he had not previously considered. The insights he gained from his students became part of the following year's security seminar in Abidjan.

Training surveys. An anonymous survey (bilingual in English and French) was performed at the end of each training session. Participant satisfaction with the training scored an average of 4.4 out of 5 on our five-point scale.[ae] Participants rated both the appropriateness and effectiveness of the project at 4.6. They disagreed strongly (1.4) with the idea that Internet freedom is not a problem in West Africa. The main complaint was the fact that the training facilities were not adequate (3.69 out of 5), which is understandable given the limited funds, time, personnel, or a combination of reasons. The most frequent complaint about the training facilities was the quality of the local Internet connection. We received the following user suggestions for improvement: provide information on mobile phone security; provide information on telephone wiretaps; provide guidance on how to collect information on state surveillance infrastructure; and provide guidance on how to work around Internet blackouts.

Africtivistes Movement

During the final year of the course, many trainees, who had initially met at our training sessions, worked together to create the Africtivistes movement[af] and League of African Bloggers and Cyber-Activists for Democracy, which held its first annual meeting in Dakar, Senegal, November 25, 2015. The initial team was lead by Cheikh Fall (@cypher007), who helped *Y'en a Marre* put in place an election-monitoring tool in Senegal, Justin Yarga (@y_jus), who worked as a web liaison for Balai Citoyen as it led pro-democracy protests in Burkina Faso, and Aisha Dabo (@mashanubian), a Gambian journalist. They assembled 150 activists from 35 countries representing the major online movements in sub-Saharan Africa. Attendees included Youssou N'Dour, a major world-music star who was a former Minister of Culture in Senegal and current minister-adviser to the President of Senegal. We provided onsite security training for the Africtiviste delegates and helped them set up their own dark web forum.

The Africtivistes movement is coordinating national pro-democracy activities into a pan-African force. We were able to help many of them simply by giving access to other people facing similar problems. The Africtivistes group is currently working to help a number of national actions, including:

#Sassoufit. Trying to convince the President of Congo Brazzaville to respect his country's constitution and enforce the term limit of 30 years on the current president;

#Article59 Togo. Trying to convince the government of Togo to respect

ad https://clemson.box.com/s/4knwbrq4j27zn0w4iig2at0wanymza4t

ae All questions used a five-point scale ranging from strong disagreement (1) to strong agreement (5);

af http://www.africtivistes.org/!/

term limits, as written, in its national constitution;

Benin Vote 2016. Trying to establish an online election-monitoring system to make the country's presidential election more transparent;

#StopBokoHaram. Protesting expansion of the Boko Haram insurrection into Cameroon and persuade the international community to intervene; and

#Mauritanie. Protesting actions taken to imprison human rights activists arrested for working against the modern slave trade in Mauritania.

The Africtivistes movement is ongoing and has brought together the sub-Saharan human rights, blogging, journalism, and tech communities into a common front. Plans are underway to create a new generation of security training sessions where local trainees will train yet others to use the tools we would provide. Remote technical support will be provided by author Brooks's team at Clemson.

Conclusion

Our project ended in the spring of 2016, with its technical products having been taken over by the Internet Without Borders NGO that had expressed interest in deploying our tool for other user communities. Our training sessions were successful in many ways, some we could not have foreseen:

Influential activists. A large number of influential activists in the region are now aware of the larger international struggle for Internet freedom;

Trainees. A number of trainees used our materials and tools to hold their own local training sessions to spread their new knowledge;

Local participants. We trained local participants on a range of tools, including ours, for using the Internet securely while avoiding censorship and surveillance; and

Like-minded colleagues. Many participants connected with like-minded colleagues throughout the region with whom they could collaborate.

Plans are under way to expand this work by having Internet Without Borders deploy our technology to support other user groups and Africtivistes creating a new set of training sessions derived from our original curriculum.

Before working with local activists, we were unable to find reliable documentation as to Internet censorship and surveillance in the region. Since then, numerous reports have indicated many of the more authoritarian countries in the region have purchased and deployed sophisticated network-surveillance tools from companies in Western democracies. We have found no documentation on Chinese involvement in Internet surveillance in the region. On the contrary, China is investing in local networking infrastructure, and we have anecdotal evidence of individual Chinese citizens helping the African population learn to evade censorship of social media.

The Internet in Africa is qualitatively different from the Internet in North America and Europe. There is much less wired infrastructure, and most users rely on 4G wireless links. The reliability of network and electrical infrastructure is not assured. We found it difficult to assure the performance of our tools without them being tested in the region. On the other hand, the McKinsey Group has estimated that in 2025 the Internet in Africa will involve approximately 600 million users buying $75 billion in e-commerce goods and services, and the Internet will add approximately $300 billion to the region's economy.[ag]

Demographically and financially, the sub-Saharan Internet is growing, and we are witnessing an ongoing struggle between authoritarian governments and local democracy activists taking place largely over the Internet. While in many ways the Internet is helping the pro-democracy forces, it is also helping keep non-democratic governments in place.

Acknowledgments

We would like to acknowledge the support of the U.S. State Department's Bureau of Democracy, Human Rights, and Labor in part for this work through Internet Freedom for West Africa grant number SLM-AQM-12GR1033. The statements in this article are the opinions of the authors and do not reflect the positions of the U.S. government or the U.S. Department of State. We also wish to acknowledge the support we received from our seminar participants and the Fondation Robert Fiadjoe pour le Qualité and to thank the editor and reviewers for their thoughtful reviews and suggestion of improvements to this article, greatly improving its quality.

ag https://www.mckinsey.com/industries/high-tech/our-insights/lions-go-digital-the-internets-transformative-potential-in-africa

References

1. Dietrich, C.J., Rossow, C., Felix, Freiling, C., Bos, H., Van Steen, M., and Pohlmann, N. On botnets that use DNS for command and control. In *Proceedings of the Seventh European Conference on Computer Network Defense* (Gothenburg, Sweden, Sept. 6–7). IEEE Computer Society Press, 2011, 9–16.
2. Fu, Y., Yu, L., Hambolu, O., Ozcelik, I., Husain, B., Sun, J., Sapra, K., Du, D., Beasley, C., and Brooks, R. Stealthy domain-generation algorithms. *IEEE Transactions on Information Forensics and Security 12*, 6 (June 2017), 1430–1443.
3. Hagen, J. and Luo, S. *Why Domain-Generating Algorithms?* Trend Micro, Aug. 18, 2016; http://blog.trendmicro.com/domain-generating-algorithms-dgas
4. Roberts, H., Zuckerman, E., and Palfrey, J. *Circumvention Landscape Report: Methods, Uses, and Tools.* The Berkman Center for Internet & Society at Harvard University, Cambridge, MA, 2007; http://cyber.harvard.edu/sites/cyber.harvard.edu/files/2007_Circumvention_Landscape.pdf
5. Silva, S.S.C., Silva, R.M.P., Pinto R.C.G., and Salles, R.M. Botnets: A survey. *Computer Networks 57*, 2 (Feb. 2013), 378–403.

Richard Brooks (rrb@g.clemson.edu) is a professor of computer engineering in the Holcombe Department of Electrical and Computer Engineering at Clemson University, Clemson, SC, USA.

Lu Yu (lyu@g.clemson.edu) is a postdoctoral fellow of computer engineering in the Holcombe Department of Electrical and Computer Engineering at Clemson University, Clemson, SC, USA.

Yu Fu (fu2@g.clemson.edu) is a staff engineer at Palo Alto Networks, Palo Alto, CA, USA.

Oluwakemi Hambolu (ohambol@g.clemson.edu) is a Ph.D. student in the Holcombe Department of Electrical and Computer Engineering at Clemson University, Clemson, SC, USA.

John Gaynard (jgaynard@gmail.com) has taught innovation at ESIEE Engineering School in Paris, France, and the OU Business School, U.K., and spent much of his professional career consulting on strategic and telecoms issues in French West Africa.

Julie Owono (julie@internetsansfrontieres.org) is a lawyer and Executive Director of Internet Without Borders (https://internetwithoutborders.org/).

Archippe Yepmou (archippe@internetsansfrontieres.org) is a musical composer and President of Internet Without Borders (https://internetwithoutborders.org/).

Félix Blanc (fb.blanc@gmail.com) is head of public policy in Internet Sans Frontières (https://internetwithoutborders.org/) and a research fellow in the Center for Technology and Society in the Law Department of the Getulio Vargas Foundation, Rio de Janeiro, Brazil.

Watch the authors discuss their work in this exclusive *Communications* video. https://cacm.acm.org/videos/internet-freedom-in-west-africa