# Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites

Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, John Palfrey[†]

The Berkman Center for Internet & Society at Harvard University

December 2010

† Ethan Zuckerman is a senior researcher at the Berkman Center for Internet & Society. Hal Roberts is a fellow at the Berkman Center. Ryan McGrady is a PhD student at North Carolina State University. Jillian York is a staff member at the Berkman Center. John Palfrey is a faculty co-director of the Berkman Center.

Table of Contents

## 1. Executive Summary

Our research begins with the idea that Distributed Denial of Service (DDoS) is an increasingly common Internet phenomenon and is capable of silencing Internet speech, usually for a brief interval but occasionally for longer. We explore the specific phenomenon of DDoS attacks on independent media and human rights organizations, seeking to understand the nature and frequency of these attacks, their efficacy, and the responses available to sites under attack. Our report offers advice to independent media and human rights sites likely to be targeted by DDoS but comes to the uncomfortable conclusion that there is no easy solution to these attacks for many of these sites, particularly for attacks that exhaust network bandwidth.

We began our inquiry by attempting to answer four major research questions:

- How common are DDoS attacks against independent media and human rights sites, especially outside of well-known elections, protests, and military operations?
- Which methods do DDoS attacks against independent media and human rights sites use?
- What are the impacts of DDoS attacks on independent media and human rights sites?
- How can independent media and human rights sites best protect themselves against DDoS attacks?

To answer these questions, we undertook a slate of related research projects in 2009 and 2010:

- We created a database of media reports of DDoS with a focus on attacks on independent media and human rights sites.
- We surveyed the administrators of independent media and human rights sites in nine countries, distributed across multiple regions.
- We conducted interviews with twelve site administrators, discussing their experiences suffering from and fending off DDoS attacks.
- We held a meeting of independent media site administrators and core network experts to discuss the needs of the human rights and independent media community, the services available to fend off DDoS, and possibilities for collaboration between core network experts and independent media and human rights publishers.

Our research suggests that:

- DDoS attacks against independent media and human rights sites have been common in the past year, even outside of elections, protests, and military operations. With recent highly publicized DDoS attacks on Wikileaks, and "Operation Payback" attacks by "Anonymous" on sites perceived to oppose Wikileaks, we expect these attacks to become more common.
- Independent media and human rights sites suffer from a variety of different types of cyber attacks, including filtering, intrusions, and defacements in addition to DDoS attacks, and those attacks interact with each other in complex ways.
- Independent media and human rights sites suffer from both application DDoS attacks, which exhaust local server resources and can usually be mitigated by a skilled system administrator; and network DDoS attacks, which exhaust network bandwidth and can usually only be mitigated with the help of a hosting provider at considerable expense.
- Mitigating DDoS attacks against independent media and human rights sites will likely require moving those sites closer to the core of the Internet: inside the small number of major ISPs, websites, and content distribution networks* (CDNs) that have the experience and resources to defend against these attacks, particularly network DDoS attacks.

We recommend the following responses to DDoS attacks against independent media and human rights sites:

- Application attacks can be strongly mitigated by replacing complex content management systems* (CMSes) with static HTML* or by adding aggressive caching* systems to deliver content at the expense of interactivity.
- All organizations should carefully consider whether to host their sites on a free, highly DDoS-resistant hosting service* like Blogger, even at the cost of prestige, functionality and possible intermediary censorship. Organizations that choose to host their own sites should plan for attacks in advance, even if those plans include acceptable levels of downtime.
- Organizations that choose to host their own sites should use systems to detect attacks and, when necessary, degrade site performance and retreat to backup hosting on a free, highly

DDoS-resistant hosting service like Blogger. Simple modules for popular content management systems could automate this process and minimize the disruption of an attack.

- Human rights funders should identify and support local experts in communities of the attack sites, since defending against DDoS and other attacks requires not only technical skill but also knowledge about and trust of each of the local communities.
- Human rights funders should consider funding a coordinator to identify both local experts for human rights communities and core network organizations willing to help human rights sites and to help local experts and core networks organizations work with one another.
- The human rights community should work with Internet service providers (ISPs) and online service providers (OSPs) to identify providers who will work to protect sites from DDoS and who will agree not to remove controversial content unless required by law.
- We propose a broad public discussion of a range of policy responses to the rise of DDOS attacks against independent media organizations and human rights groups, with a view toward a sustainable long-term approach that balances the range of legitimate interests involved.

## 2. Introduction

On the morning of September 18, 2010, the website of the Motion Picture Association of America (MPAA) was unreachable to most Internet users. A massive number of requests overwhelmed the mpaa.org web server*—essentially, the web server collapsed under the weight of trying to serve web pages to thousands of demanding users, who requested page after page, hundreds of times a second. This DDoS attack prevented legitimate users from accessing the site for over twenty hours.[1] Attacks also targeted the Recording Industry Association of America and the British Photographic Industry.

Participants on the Internet bulletin board 4chan organized the attack, urging readers to participate as "payback" for a DDoS attack the MPAA was alleged to have encouraged Indian firm Aiplex Software to carry out against popular file sharing site PirateBay.org.[2]

While attackers were only effective in silencing the MPAA for a day, their actions generated widespread media attention with stories in the BBC, Reuters, the London Telegraph, and the San Francisco Examiner within hours of the attack's end. Commenting on the attacks on the MPAA and their media fallout, security researcher Sean-Paul Correll described DDoS as "the future of cyber protests."[3] His prediction was timely. Three months later, some of the same activists organized "Operation Payback," a set of highly publicized attacks on PayPal, Visa, MasterCard, Swiss bank PostFinance designed to punish the firms for denying services to whistleblowing website Wikileaks. Wikileaks, in turn, reported coming under sustained DDoS attack after publishing classified US diplomatic cables and briefly moved its servers to Amazon's cloud architecture, seeking protection from attacks.

Correll's predictions about DDoS and activism would not have surprised Sergey Sokolov, deputy executive editor of *Novaya Gazeta*, widely considered to be Russia's most liberal independent newspaper. His website has come under sustained DDoS attack multiple times in the past year, once disabling it for more than a week. Sokolov isn't sure who is attacking his site but suspects government-

1 Sean-Paul Correll, "4chan Users Organize Surgical Strike Against MPAA," September 17, 2010, accessed September 20, 2010, http://pandalabs.pandasecurity.com/4chan-users-organize-ddos-against-mpaa/.

2 Ben Grubb, "Film industry hires cyber hitmen to take down Internet pirates," Sydney Morning Herald, September 8, 2010, accessed September 20, 2010, http://www.smh.com.au/technology/technology-news/film-industry-hires-cyber-hitmen-to-take-down-Internet-pirates-20100907-14ypv.html.

3 Correll, "4chan Users Organize Surgical Strike Against MPAA."

sponsored “Kremlin Youth” organizations.[4] He has received very little help from local authorities in preventing the attacks or tracing their origins. He believes the lack of help is because the actors have active or tacit government approval.

We know—thanks to extensive research conducted by major network operators and the companies that work with them—that DDoS is a major security issue. Security firm Arbor Networks surveys network operators annually to identify major security concerns. Their 2008-2009 survey identified DDoS as the issue about which administrators were most concerned. Virtually every network operator surveyed by Arbor had fended off a DDoS attack in the past year, and many reported having extensive procedures and methods in place to combat attacks.[5]

Historically, DDoS has been associated with extortion. By harnessing a large number of computers—often computers compromised by malware,* allowing remote users to control the computers' behavior without the users' knowledge—criminals are able to render a website unusable, then seek “protection money” from the site's owners. But DDoS is also used for a variety of non-financial reasons, including political ones.

For major network operators, DDoS is expensive but manageable, in a way analogous to unsolicited commercial email (spam) today. The world's largest Internet service providers* and destination websites manage DDoS attacks by over-provisioning (maintaining more servers and connectivity than they generally need to cope with peak loads due to legitimate traffic or DDoS) and by monitoring and rapidly responding to attacks using a set of best practices and tools. Operators of major networks and major websites often interact with one another through closed mailing lists, helping each other fend off attacks.

While network operators identify DDoS as their most expensive security issue, end users have generally been unaware of DDoS attacks. Even though major sites and network are constantly under DDoS attacks, it is rare for them to go down for any extended period of time. Google, AT&T, and CNN do not

4 Gregory Asmolov, “Russia: Novaya Gazeta, An Opposition Newspaper Under Internet Attack,” Global Voices Online, June 18, 2010, accessed September 20, 2010, http://globalvoicesonline.org/2010/06/18/russia-interview-with-deputy-executive-editor-of-novaya-gazeta/.

5 Worldwide Infrastructure Security Report, Volume V (Arbor Networks, 2009).

go down every day in the face of these constant attacks because they defend themselves well, and so end users generally are not aware of the attacks. High profile attacks, such as the "Operation Payback" attacks, have called attention to activists' political goals, but have been largely ineffective in disturbing the business operations of targeted firms. It is worth noting that the Operation Payback attacks disabled promotional websites associated with the financial firms targeted, not their mission-critical payment processing systems, because those promotional sites are much less well-protected than the firms' core operational systems.

The substantial costs of mitigating DDoS attacks are incorporated into the prices end users pay for services. This modest cost might be thought of as a social insurance system. The costs of DDoS mitigation efforts are spread across net users and hosts, even though the vast majority of them do not know the attacks are taking place, precisely because the small incremental costs are sufficient to fend off the attacks in the core of the network.

We also know that there is a long history of DDoS being used as a political tool, often in conjunction with real-world events like elections or military operations. Dr. Jose Nazario has written an indispensable paper that examines sixteen major instances of DDoS attacks where the primary motivation was political, not financial.[6] While Nazario's research is extremely helpful in understanding the dynamics, scale and methods behind these attacks, it leaves open questions about the future of these attacks, their overall prevalence outside of particular political crises, and the effectiveness of attacks on independent media and human rights organizations.

This paper includes many highly technical words that are not defined in the body of the paper. For the lay reader not versed in technical Internet jargon, we have included a glossary at the end of the paper that defines most of these technical terms. All words included in the glossary are marked with italics in the body of the paper.

6 Jose Nazario, "Politically Motivated Denial of Service Attacks," Arbor Networks, 2009, accessed March 3, 2010, http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf.

# 3. Background

## 3.1. Core vs. Edge

Throughout this paper, we differentiate organizations and entities as being closer to "the core" or "the edge" of the Internet. These concepts are difficult to define precisely and are in flux, but they are critical to our understanding of the challenges facing independent media and human rights sites.

The communications industry refers to a small set of Internet service providers as "Tier 1 ISPs". These organizations are distinguished by the fact that they connect directly to all other major networks through peering. These ISPs are not customers of one another—they exchange traffic with each other without paying transit, the industry's term for charging a customer for carrying Internet traffic. The advantages of being a Tier 1 ISP are great, and the status is only extended to networks that reach a very large number of customers, so that it is financially worthwhile to carry that network's traffic as a peer. By contrast, Tier 2 ISPs peer with some networks and pay for transit to reach other networks, while Tier 3 networks pay transit for all of their traffic. The vast majority of ISPs are Tier 2 or 3; most estimates suggest that there a dozen or fewer Tier 1 providers.

Traditionally, companies that maintain websites are customers of Tier 1, 2, or 3 ISPs, or resellers of services from those ISPs. Companies that maintain their own server farms might contract with two or more Tier 1 providers to ensure redundant paths to their servers. However, the landscape is shifting, due to the rise of massively popular sites like Google/YouTube, which is responsible about 6–12% of the Internet's total traffic.[7] Google owns a great deal of fiber optic cable and connects directly with Tier 1 ISPs as a peer. This arrangement makes sense for Tier 1 ISPs because their customers demand speedy access to Google's services, and it is advantageous for Google because they don't pay transit costs. In addition to Google, other huge content providers like Facebook may have similar arrangements to peer directly.[8] In addition, large and medium sized websites contract with content distribution networks to cache their content in widely distributed servers around the world, so a user requesting a cnn.com web

7 Craig Labovitz, "Google Sets New Internet Traffic," Security to the Core, October 15, 2010, accessed October 25, 2010, http://asert.arbornetworks.com/2010/10/google-breaks-traffic-record/.

8 Labovitz et al., "ATLAS Internet Observatory, 2009 Annual Report," accessed October 14, 2010, http://www.nanog.org/meetings/nanog47/presentations/Monday/Labovitz_ObserveReport_N47_Mon.pdf.

page or a video from Brazil gets the content from a server in Brazil rather than in the U.S. The largest CDN, Akamai, claims to transit over 20% of all web traffic alone.[9]

When we refer to the core Internet, we are referring to Tier 1 and large Tier 2 ISPs, to these hypergiant web hosts, and to a few of the very largest CDNs. Further towards the edge of the Internet are Tier 3 ISPs, who resell connectivity from Tier 1 and 2 providers. Even further towards the edge are customers of those Tier 3 providers. A customer of a webhosting company that purchases connectivity from a Tier 3 provider—the description of many of the independent media and human rights sites we considered—is at the farthest edge of the Internet.

Organizations near the core of the Internet tend to have large, well-trained staff focused on network security. In Arbor Networks' 2009 survey of network operators, more than 50% of Tier 1 ISPs reported having security staff of 15 or more professionals, while Tier 2 ISPs most commonly reported 2-4 security staff. Three out of ten web hosting providers reported having no dedicated security staff.[10]

The network operators at the core often know one another through industry meetings and, importantly, from private mailing lists and forums where network security issues are discussed. Near the edge, network administrators frequently don't know about these lists and sometimes would not be welcomed into these conversations even if they knew of them.

In the past decade, there has been a decisive concentration of Internet traffic towards the core. Arbor refers to this move as “the rise of the hypergiants” and observes that 30% of Internet traffic terminates with 30 companies. There are many implications to this move, but the key one for this discussion is the increasing vulnerability of operators closer to the edge. As the size of the Internet grows—in bandwidth and in end users—while bandwidth and expertise is concentrated in the core, those at the edge are increasingly resource-constrained and cut off from the networks where key security issues are discussed. And, because they are often connected to the rest of the Internet by a single link, they are especially vulnerable to DDoS network attacks.

9 “Visualizing Global Web Performance with Akamai,” http://www.akamai.com/html/technology/visualizing_akamai.html, retrieved 10/26/2010.

10 Danny McPherson et al., “Worldwide Infrastructure Security Report: Volume V, 2009 Report,” Arbor Networks, January 19, 2010, accessed January 20, 2010, http://staging.arbornetworks.com/dmdocuments/ISR2009_EN.pdf.

This isolation of independent media and human rights sites away from the growing core of the Internet raises a key set of conceptual questions. There's a strong temptation for sites that handle sensitive data to maintain their operations in house as much as possible, leading them to maintain their own servers on Tier 2 or 3 networks, which provide cheaper service for self-hosting. Large ISPs in many nations have close contacts with the national government, so dissident sites might choose to use smaller ISPs or hosting providers to avoid the big, government-controlled ISPs.

But as we detail below, moving towards the edge of the network on balance makes sites more vulnerable to DDoS attacks. And a site that runs its own server on a small ISP removes itself from the system of social insurance that protects sites within the core from DDoS attacks, putting itself at risk of catastrophic DDoS attack. This situation is analogous to (and costly in the same way as) paying cash for a consumer purchase and therefore forsaking the protection most credit cards offer against fraud. Hosting on Blogger or another large hosting provider is the cheapest way to buy into this system of insurance—the costs are in non-financial considerations like prestige and functionality. A much more expensive option is to pay for a DDoS protection service in the core from a Tier 1 ISP or from one of the major CDNs.

### 3.2. A Brief History of DDOS

While DDoS attacks have received increasing attention from both network operators and journalists in the past half-dozen years, the basic network vulnerabilities that make attacks possible have been recognized since the early days of the commercial web. Practical Unix and Internet Security, the "bible" for many system administrators of the early commercial web, offers a chapter on denial of service attacks.[11] Carnegie Mellon's Computer Emergency Response Team* (CERT) published its first bulletin on SYN flooding* (a popular technique for overwhelming a target system) in September 1996,[12] and a more thorough bulletin on denial of service in October 1997,[13] suggesting that denial of service was beginning to emerge as a priority for network administrators.

11 Simson Garfinkel and Gene Spafford, Practical Internet and Unix Security (New York: O'Reilly, 1996).

12 CERT Advisory: SYN Flooding and IP Spoofing Attacks, September 19, 1996, accessed September 20, 2010, http://www.cert.org/advisories/CA-1996-21.html.

13 CERT, "Tech Tips: Denial of Service Attacks," June 4, 2001, accessed September 20, 2010, http://www.cert.org/tech_tips/denial_of_service.html.

While CERT and others offered helpful advice for mitigating DDoS attacks, the particular attack documented in 1996—SYN flooding—is still common today, pointing to the wide gap between understanding these attacks and successfully defending against them. Similarly, the U.S. National Information Infrastructure Protection Act of 1996 took steps to criminalize DDoS, redefining computer fraud "damage" as preventing access to a computer system. Previous definitions had focused on unauthorized access and damage to systems. But Arbor's annual survey reports that the vast majority of system administrators do not bother reporting DDoS attacks to the authorities.

Shortly after denial of service emerged as a concern for system administrators, activists began using it as a political technique. Artist and professor Ricardo Dominguez, co-founder of Electronic Disturbance Theatre, pioneered the use of denial of service as a tool for activists in 1998. He built FloodNet, a tool designed to allow activists to crash the websites of the Frankfurt Stock Exchange, the Pentagon, and Mexican President Ernesto Zedillo.[14] Perhaps because these protests generally failed to shut down the sites, they were little discussed outside the art community.

Denial of service took on new visibility and importance in February 2000, when denial of service attacks took down the websites of Yahoo, Buy.com, eBay, CNN, Amazon.com, ZDNet.com, E*Trade, and Excite. These attacks were so large that they suggested multiple origin points harnessed into a DDoS attack. The attacks were ultimately traced to Michael Calce, aka "Mafiaboy," a fifteen-year-old from Montreal who was identified only because he bragged about the attacks in an Internet Relay Chat* (IRC) channel. He served eight months of "open custody" for his crimes.

DDoS attacks became more common in 2000 and 2001 as techniques became available to compromise large numbers of Windows systems. Worms* (Code Red) and Trojan horse programs* sent via email (LoveLetter, Anna Kournikova) demonstrated the ability to exploit known vulnerabilities to compromise large numbers of systems.[15] At the same time, attackers began to organize compromised computers into networks centrally controlled by IRC “bots.” Using one of these “botnets,”* a single controller is able to

14 “Notable Hacks,” PBS Frontline, accessed September 20, 2010, http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html/.

15 Kevin Houle and George Weaver, “Trends in Denial of Service Attack Technology,” (CERT Coordination Center, 2001).

manipulate thousands of compromised computers and order them to send spam email, steal credit card information, or mount DDoS attacks. Most existing techniques for defending against denial of service attacks were based on identifying the attacking computers by IP address.* Botnets invalidated many of these techniques because a single botnet could include thousands of computers with randomly distributed IP addresses, making them very hard to distinguish by IP address alone.

Despite the rise of botnets, other forms of DDoS have continued to demand attention and media coverage. Denial of service attacks that recruit participants—"volunteer DDoS"—remain common. Recently, the organization "Help Israel Win" invited individuals to install a software package ("Patriot DDoS") on their PCs that would give a remote administrator the capability to harness the machine in an attack on a (presumably Palestinian) target.[16] During the Iranian Green Movement protests of 2010, protesters used a page refreshing service to manually execute a DDoS attack against President Mahmoud Ahmadinejad's website.[17] The "Operation Payback" attacks require participants to download software fancifully named "Low Orbit Ion Cannon" (LOIC). The software allows a computer to become part of a botnet controlled by administrators of the Anonymous group via IRC.

### 3.3. Current State of the Art

For the past few years, large-scale DDoS has been the most expensive security problem for major network operators. In its 2009 security report, Arbor Networks reported that the size of the largest reported DDoS attacks had increased steadily, from 400 megabits (Mbps*) per second in 2002 to 49 gigabits per second (Gbps*) in 2009.[18][19] For comparison, Harvard College connects its tens of thousands of users on its network to the Internet through a 2 Gbps link, so a 400 Mbps attack would consume one fifth of Harvard's bandwidth, while a 49Gbps attack would consume the bandwidth of fully 25 Harvards.[20] An attack of 400 Mbps remains a challenge for most site administrators; it is generally big enough to overwhelm a site hosted by a single server but can potentially be mitigated by the

16 Noah Schactman, "Wage Cyberwar Against Hamas, Surrender your PC," Wired: Danger Room Blog, January 8, 2009, accessed March 3, 2010, http://www.wired.com/dangerroom/2009/01/israel-dns-hack/.

17 Peter Wilkinson, "Briton's Software a Surprise Weapon in Iran Cyberwar," CNN, June 17, 2009, accessed October 14, 2010, http://edition.cnn.com/2009/WORLD/meast/06/17/iran.elections.hackers/index.html.

18 1 megabit equals 1 million bits, where a bit represents either a '1' or a '0'. 1 gigabit equals 1 billion bits, so 1 gigabit is a thousand times larger than 1 megabit. There are 8 bits in a byte, so 1 gigabit equals 125 megabytes.

19 Danny McPherson et al., "Worldwide Infrastructure Security Report: Volume V, 2009 Report."

20 The Harvard bandwidth figure is from a private report from a Harvard network administrator. Harvard actually has two separate Gbps links to each of two separate ISPs, but the second link to each ISP is reserved as a backup.

administrator of the local site through some of the techniques we describe below. An attack of 49 Gbps would consume the entire Internet bandwidth of (and so effectively remove from the Internet) all but a dozen or so of the world's largest Internet service organizations.

In 2009, Arbor's study described a shift away from concern about pure bandwidth attacks, as the growth in scale of those attacks appeared to slow. Instead, there was increasing concern about smaller attacks that rely less on bandwidth and more on clever tricks to fool a site into thinking that it is overloaded from even a relatively small attack. These attacks can be effective at very low bandwidths even against well-administered networks.[21]

Despite concerns about DDoS, major network operators are usually able to fend off attacks rapidly. Among the respondents to Arbor's survey, 75% reported that they fended off attacks within an hour, and 18% said that they fought off most attacks within 10 minutes.[22] Administrators are able to react swiftly by being prepared for DDoS attacks: they have filtering systems ready for deployment and have alternative network paths through which they can route legitimate traffic. Critically, they are also able to rely on assistance from upstream and peer system administrators, who can often assist in fighting DDoS by disconnecting computers that are mounting the attack.

It is a good thing that major network operators have the hardware, bandwidth and human resources to treat DDoS as part of their daily administrative chores because DDoS is disturbingly pervasive. Arbor monitors a large percentage of backbone Internet networks and is often able to detect DDoS attacks by searching for unexplained surges of traffic. On a "normal" day, Arbor detects roughly 1300 DDoS attacks.[23] This number, however, is an undercount of attacks underway; Arbor's tools detect large attacks and a subset of small attacks. We sent Arbor a list of our survey sample, consisting of 300 independent media sites we thought were likely to be attacked. Of the 34 respondents to the survey, 21 reported being attacked, and we assume more who did not respond had also been attacked. Arbor detected attacks against only 7 of the sites. It's possible that some of the attacks were misreported by

21 Danny McPherson et al., "Worldwide Infrastructure Security Report: Volume V, 2009 Report."
22 Ibid.
23 Arbor Networks, "Atlas Summary Report: Global Denial of Service," accessed October 26, 2010, http://atlas.arbor.net/summary/dos.

the survey respondents or that Arbor was simply unable to match detected attacks with our sample set, but we think it is more likely that some were simply too small for Arbor to detect.

The pervasiveness of DDoS for core network operators leads to economies of scale. The operators of a major hosting site we interviewed mentioned that they have seen dozens of variations of DDoS and know what techniques to deploy for each. In many cases, they have been able to systematize responses, so responding to the vast majority of attacks is routine. Administrators of smaller sites at the edge of the network have a much harder time fending off attacks. They are less prepared, less connected to other administrators, and less likely to have access to key resources (alternative routes to servers, servers, and bandwidth on demand), and they have much less experience diagnosing and countering the broad range of different DDoS attacks. For many of these administrators at the edge of the Internet, DDoS is far from routine and can cause sustained downtime.

### 3.4. How DDoS Works

Denial of service (DoS) attacks focus on consuming scarce resources so that legitimate work cannot be done. In outlining the space of denial of service attacks, Mark Handley gives examples that range from cutting off power to a data center to "legal DoS" involving cease and desist letters that force a customer off a server. Most types of DoS attacks focus on vulnerabilities in software, which can be exploited to exhaust computer resources like processing time and memory.[24]

For example, a SYN flood attack takes advantage of a peculiarity of the process used to open TCP/IP* connections. A client opens communications by sending a "SYN" message to a server. The server responds with a message, "SYN-ACK", at which point the client should respond with "ACK." The two sides of a connection use this "three-way handshake" to establish and confirm a connection. But when the client side of the connection fails to send an ACK, the server uses memory resources holding its side of the connection open. If a client sends thousands of SYN messages and never responds with an ACK, it is possible to consume all the memory a server has allocated towards opening connections and thereby stop the server from accepting legitimate connections.

24 Handley et. al., RFC 4732, http://tools.ietf.org/html/rfc473.

An attack like the SYN flood just described is easy to execute with just a single attacking machine, but it is also easy for an experienced system administrator to defend because it is easy to distinguish the attack from legitimate traffic. Legitimate TCP requests send ACKs in response to SYN-ACK; illegitimate ones do not and should be quickly ignored. Attacks that look like legitimate traffic are harder to fend off. If the attacker requests random web pages from the site, the attack looks more like traffic generated by a set of legitimate users. Blocking this type of attack requires using other information to distinguish between legitimate and illegitimate requests.

Many methods for mitigating DoS attacks rely on blocking IP addresses that issue too many requests, or slowing requests from these addresses, a process called "rate limiting."* An IP address requesting 10 web pages in 10 seconds might well be legitimate, while one requesting 1000 probably is not (unless it's a proxy* server, as we'll discuss further on in this paper). What makes DDoS attacks so powerful is not just that many machines can issue many more requests. It's that the requests can be spread across a set of machines, and no one machine has to make many requests. A competent system administrator might easily fend off an attack in which 10 users (each on a different IP address) each issue 100 requests per second. But an attack in which a thousand users on different IP addresses each issue a single request per second is much harder to distinguish, and an attack in which a million users on different IP addresses issue one request a minute is much, much harder.

We distinguish DDoS attacks into two basic categories based on the resources they seek to exhaust: application attacks and network attacks. Application attacks use software vulnerabilities to exhaust resources on the local machine, like processing time and memory. Network attacks attempt to saturate the communications lines that connect servers to the Internet. Arbor's 2009 report states that 45% of DDoS attacks were network attacks and 49% were application attacks. Because Arbor's network monitoring techniques are more likely to register network attacks, the 45% figure may overstate the proportion of network attacks.[25]

In most cases, network attacks use botnets, amplifiers (see below), or a combination of the two to generate sufficient traffic. By controlling many computers through a botnet, the attacker is able to send many streams of packets instead of a single one. Still, even using a botnet of compromised computers, it

25 Danny McPherson et al., "Worldwide Infrastructure Security Report: Volume V, 2009 Report."

is hard to generate 40 Gbps of traffic by sending packets from thousands of computers attached to home DSL connections; an attack that size requires a botnet of hundreds of thousands or even millions of computers, and botnets of that size are rare and very valuable. In large network DDoS attacks, the scarce commodity for the attacker isn't processing time or memory; rather, it's the number of believable identities (in simplest terms, unique IP addresses) available to mount the attack. As opposed to application attacks, which can use software vulnerabilities to take down a site with relatively few users, botnet attacks are powerful because they involve large numbers of compromised computers, each of which might be a legitimate user trying to reach a website. Large volunteer efforts, like the one that attacked the MPAA, are similarly powerful because they involve many individual users making the atomic decision to attack a target.

Attackers can also use a strategy called “amplification,” in which a skilled attacker can exploit a network or application vulnerability to trick other computers into turning the attacker's single stream of traffic into a flood of thousands or millions of streams. For example, in DNS* amplification, the attacker makes a request to a DNS server that appears to have come from the target web server. The DNS server does what it's supposed to do and delivers a chunk of domain name information to the computer that (putatively) requested it: the target computer. The information delivered is much larger than the size of the request—some attacks are able to leverage DNS servers to amplify their traffic by a factor of 76:1. A single attacker might deliver 1000 DSL connections worth of data to DNS servers, which in turn could deliver 76,000 DSL connections worth of data to a target computer to overwhelm it with bogus data. Another example of an amplification attack is a Smurf attack, in which an attacker can fool entire networks of computers into responding to a single broadcast ping* with a flood of return pings to the victim computer.[26][27]

Application attacks rely less on brute force. Instead, they focus on vulnerabilities in web server, operating system, and networking software. Some techniques attack known flaws in popular programs. Slowloris (freely downloadable at http://ha.ckers.org/slowloris/) takes advantage of a flaw in how many

26 Gholam Reza Zagar and Peyman Kabiri, “Identification of effective network features to detect Smurf attacks,” Lecture Notes in Computer Science, 6171 (2010): 49-52.

27 McPherson, Baker, Halpern, “SAVI Threat Scope” draft 3, September 8, 2010, accessed October 14, 2010, http://tools.ietf.org/html/draft-ietf-savi-threat-scope-03; Randal Vaughn and Gadi Evron, “DNS Amplification Attacks,” March 2006, accessed October 14, 2010, http://www.isotf.org/news/DNS-Amplification-Attacks.pdf.

popular web servers treat partial HTTP* requests to exhaust the number of simultaneous threads a web server can start. Servers that are subject to slowloris attacks and do not defend themselves appear merely to be idle, since the attack tricks the server into opening its maximum number of responding threads and then idling all of those threads, leaving none available to respond to legitimate requests.

Other attacks simply take advantage of legitimate pages that are very expensive for server software to generate. Search pages are frequently targeted—on many systems, executing a search requires an expensive database query. A moderately large site might be capable of serving static HTML pages to a thousand users at a time but be crippled by only a handful of requests at a time to one of these expensive pages. One of our interviewees reported that as few as five machines executing simultaneous searches crippled his website, which otherwise served almost a million page views a day. Our interviews and media research found that this kind of attack against a slow loading page (often but not always a search or discussion forum page) was a common form of attack.

Content management systems like WordPress and Drupal are inherently vulnerable to DDoS attacks in their default configurations. Often, simple page requests put a heavy load on their databases, and these systems are not, in the default configurations, optimized for the very high traffic peaks generated by DDoS attacks. The considerable strength of CMSes is that they provide very sophisticated functionality with little need for technical expertise. Unfortunately, this strength is also a weakness. Many people who install these complex CMSes are not experienced system administrators and so are capable of setting up the systems but are not capable of properly configuring the systems to handle very high loads or patching the systems to protect against ongoing vulnerabilities. Many of these systems have features that allow them to handle high traffic loads and resist DDoS attacks when configured correctly. But configuring and maintaining the combination of machine, operating system, web server, and CMS application to resist DDoS attacks is much more difficult than simply running a base install of one of these systems. So many independent media publications find themselves running (and largely dependent on) a CMS but not capable of the considerably harder task of defending the CMS against a DDoS attack.

In understanding how to combat DoS attacks, it's important to distinguish between attacks carried out by a solitary individual, those carried out by an individuals or groups leveraging a botnet, and

"volunteer" attacks, where multiple attackers cooperate and combine forces. While single-source denial of service attacks are generally far easier to defend and trace than distributed attacks, easily downloaded tools permit technically unsophisticated users to target websites and launch attacks that might be effective in some circumstances. Among the attacks we saw in our survey, interviews, and media research, it is likely that a significant percentage originated from a single source. It is possible that a small, focused effort to prosecute users of these tools could deter their usage.

Attacks involving botnets, on the other hand, can be extremely difficult to defend against or to trace back to their perpetrators. A botnet is at its most effective not when all machines in the network are delivering as much traffic as possible to the target site but when each machine from a random, continually switching subset of the botnet delivers a small stream of traffic. This makes those streams harder to detect, and when administrators block attacking machines, others rise up to take their place. Tracing a botnet by identifying the machines involved with the attack is usually unhelpful, as the machines involved are owned by users who have no idea they are participating in an attack. Instead, security experts track botnets by watching for attack patterns in network traffic or by monitoring IRC servers, attempting to intercept control traffic. Determining where a bot is controlled, however, does not help in attributing the attack to a particular adversary, as it is likely that an adversary hired the botnet controller.

While they have received a great deal of publicity and are capable of being quite effective, attacks that rely on voluntary participation—like the recent attack on the MPAA—may be less frightening from a security perspective. The attacks can generally be attributed by simply studying the messages used to recruit and organize the volunteers. And since many of the tools used in these attacks make no attempt to disguise the users' IP addresses, identifying participants in an attack for prosecution or civil remedy is more likely. The arrest and prosecution of a Dutch teenager for participation in the "Operation Payback" protests suggests that some prosecutors may be willing to use the legal system to deter participation in such attacks.[28] However, the success of the protests in temporarily disabling some sites suggests that large voluntary efforts can create potent attacks, at least for short periods of time.

28 Jeremy Kirk, "Dutch Arrest 16-year-old Related to WikiLeaks Attacks," PCWorld, December 9, 2010, accessed December 19, 2010, http://www.pcworld.com/businesscenter/article/213120/dutch_arrest_16yearold_related_to_wikileaks_attacks.html.

Much of the discussion of DDoS attacks, especially in the press, focuses on the magnitude of attacks, primarily because magnitude allows comparisons between attacks. A 1 Gbps attack will take down many small ISPs and hosting providers at the edge of the Internet. A 10 Gbps attack will take down almost any ISP or website other than a couple dozen of the biggest ISPs, websites, and content distribution networks at the core of the Internet. At these magnitudes, filtering requests at the attacked site does not work—the site is overwhelmed because the attack saturates the link to the Internet. Attacks of this size need to be fought off upstream, either by cooperating with the administrators of networks involved in the attack or by routing* bad traffic away from the server's main connection using sophisticated routing tricks: for instance, by propagating null routes* to attacking networks (sending a null route to an attacking computer tells that computer that there is no valid network route to the target computer, thus preventing the attacking computer from sending attack traffic to the target). Compounding the difficulty of dealing with large network attacks is the fact that when an attack overwhelms an ISP, the ISP has to consider the impact on the rest of its customers. In many cases the ISP takes the attacked site off the network to protect itself and its other customers as well as to avoid bandwidth costs.

While magnitude is useful for understanding some attacks, we believe an over focus on magnitude may mask some of the important dynamics that govern DDoS attacks in the human rights and independent media space. In one illustration of over focus on magnitude, a white paper from VeriSign reports on "one site offering botnets capable of launching DDoS attacks of 10–100 Gbps for as little as $200 per 24 hours" before acknowledging a paragraph later that the largest attack reported in the wild peaked at 49 Gbps.[29] This report focuses on the reported magnitude without considering even the obvious context of the largest known attack. Our research suggests that much lower magnitude attacks often overwhelm independent media sites, especially if an attack focuses on application vulnerabilities rather than network saturation. In other words, the size of an attack is important, but it is far from the only variable needed to understand what attacks are effective and how to mitigate against them.

29 "DDoS Mitigation: Best Practices for a Rapidly Changing Threat Landscape," VeriSign white paper, 2010, http://www.verisign.com/Internet-defense-network/resources/whitepaper-ddos.pdf.

3.5. Mitigating DDoS

Deterring denial of service attacks is not a matter of a simple technical fix—any such technical fix would require addressing underlying problems of Internet architecture. Many Internet connected computers are not controlled solely by their owners. They have been compromised by viruses, Trojan horses, or other malware and are controlled as parts of botnets. Proposed solutions to this problem have focused on security at the PC level, but fixing the security of PCs is an enormously difficult problem to mitigate, let alone solve. It might be possible to address the problem of botnets by asking ISPs to take responsibility for cutting off service to compromised computers. ISPs generally resist this solution, concerned that users who are put in “quarantine” or “walled gardens” will switch their infected machines to a competing ISP rather than patch vulnerabilities in their systems.

Many strategies for DDoS take advantage of the fact that it is very easy to spoof an identity on the Internet. Identity in this sense means identifying a specific machine on the network. Identifying specific machines on the Internet is the purpose of IP addresses, which are the unique identifiers that serve an analogous role within the Internet to that of phone numbers within the phone system. Attacks like DNS amplification rely on the fact that it is very easy to misrepresent oneself as the target of a request by spoofing an IP address (analgous to flooding a victim with phone calls by leaving the phone number of the victim as the call back number on the voicemail of many different phone numbers). Tracing DDoS attacks is complicated by the fact that there is usually no easy way to connect IP addresses to real life individuals. And the multinational nature of the Internet means that, even once a hostile IP address has been traced to the ISP who controls it, local laws may make it difficult to prosecute an attacker.

As a result of these complexities, for all but the biggest ISPs and websites DDoS attacks are not deterred so much as they are mitigated. Strategies for mitigating attacks often center on packet filtering and rate limiting. In packet filtering, requests from apparent attackers are ignored, allowing the server to focus on serving legitimate users. Rate limiting puts a cap on how many requests a single IP can issue in a time period, making it more difficult for a computer within a botnet or a determined individual assailant to flood a site with packets. These techniques can be effective, especially when system administrators share blacklists* of likely compromised machines. However, they can adversely affect legitimate users, especially users accessing a site through a proxy server, and they provide only a basic first line of defense that can be bypassed by a determined attacker.

Scrubbing involves setting up a large server farm capable of accepting many incoming connections and using a combination of automated and manual techniques to drop illegitimate traffic and pass through legitimate traffic. Scrubbing can be very effective given enough resources, but it can also be very expensive. It first requires enough bandwidth to accept the entire attack. It next requires enough CPU time to be able to process the full bandwidth of the attack in real time to distinguish legitimate from attack traffic. And finally it requires very skiiled and experienced engineers to be able to instruct the scrubbing system how to distinguish attack traffic (often different instructions for each different attack).

Dynamic rerouting is an alternative to accepting and processing the full stream of attack traffic. Instead of accepting the traffic, an ISP or protection service can use dynamic rerouting to prevent the attack traffic from ever leaving the networks that host the attacking machines. Dynamic rerouting accomplishes this by sending "null routes" to attacking networks. Those null routes tell the attacking machines that there is no longer a valid route through the Internet to the target machine, thereby causing the attacking network (including both attacking machines and legitimate machines on the network) to stop sending any traffic to the target machine. Dynamic rerouting is only effective for attacks that come from a relatively small number of networks, and it requires a very skilled network operator. Too much use of dynamic rerouting by a given organization can also have bad side effects on how other networks treat traffic from the organization, so simple source or destination-based is preferred over dynamic rerouting where possible.

Load balancing uses caching proxies (often the popular nginx) to spread the stress of an attack across multiple servers. Caching proxies store the contents of otherwise slow loading pages as static files and serve those static files in place of the slow pages. For example, when the first user connects to a blog and requests the home page, the caching proxy would request the home page from the blog software, which might take a half second for the blog software to generate. But for all subsequent requests for the home page, the caching proxy would serve its cached version of the home page, which might take a thousandth of a second. In this example, the caching system would enable the server to handle one thousand (legitimate or attack) requests per second instead of two requests per second. As with scrubbing, this defense can require having extra server capacity on demand to handle a large attack even with the increased efficiency added by the caching. And because caching systems rely on being

able to serve the same version of a given page for at least minutes at a time, they do not work well for interactive sites (a discussion served through a caching proxy, for instance, would not show new posts for minutes at a time, or however long the caching proxy was set to store pages).

Many hosting providers advertise some level of DDoS protection as part of their services. In many cases, hosting providers advertise themselves as “DDoS-resistant” as merely one feature of their primary business of hosting ordinary websites. In other cases, hosting providers advertise themselves primarily as DDoS protection services. All of these hosting providers use some combination of the above methods to mitigate attacks. Unfortunately, most are not communicative about which of the techniques they use, and in many cases, “DDoS-resistant” simply means “we will not automatically null-route you at the first sign of attack, but if we do we will give refund one month's hosting fee.” There is some value even in this very low level of guarantee because the response of many hosting providers is simply to null route attacked sites at the first sign of attack. But for many independent media sites that are likely to experience aggressive, sustained attacks, this level of protection is clearly not sufficient. For example, one dissident media site is hosted by a hosting provider advertising itself as “First and Leading in DDoS Protection Solutions,” but the hosting provider null routed the site in the face of the first large (4 Gbps), sustained attack. The provider was likely able to provide protection in face of the attack, but the site’s administrators had only paid for 2 Gbps of protection and were unwilling to pay the increased fees the provider demanded for protection from this larger attack.

Many of the most effective mitigation strategies—packet filtering, rate limiting, scrubbing, dynamic rerouting—are unavailable to inexperienced administrators or administrators using shared hosting solutions. And inexperienced administrators often lack access to the social networks that allow system administrators to request help effectively from providers upstream. Unfortunately, many of the human rights and independent media organizations we studied have inexperienced system administrators and shared hosting setups.

### 3.6. Additional attacks

Throughout this paper, we discuss other attacks that prevent a site from delivering content to its audience. As we discuss in our findings, we see a strong correlation between sites targeted for DDoS and sites that experience other forms of attack. Those attacks include:

- Filtering: using a network filter to block, often with government authorization or mandate, the ability for users from a particular country to access a particular website.[30]
- Defacement: replacing key content on the website with offensive content or pages announcing that hacking has occurred. In more serious cases, defacement may include adding code to a page to trigger "drive-by downloads" of malware.
- Intrusion: gaining privileged access to a server. Privileged access can be used to release data, to harass and threaten members of an online community, or to delete valuable data, among other attacks.
- Hijacking: seizing control of a web server by redirecting the domain name to point to a different—often hostile—website.
- Attacks on administrators and end users: Administrators of websites are often targeted with malware that seeks to log their keystrokes and seize passwords, or otherwise access the content of their hard drives.
- DDoS by bureaucracy: Attackers can render a site unreachable by challenging the ownership of the domain name or other resources and forcing resolution through complex and time-consuming processes.

Each of these types of attack has a different impact on the target site. For example, filtering a site is relatively easy to setup and maintain but only controls users within the filtering country—users within China cannot see http://falundafa.org because China filters the sites, but users from the rest of the world can still the site. A DDoS attack, by contrast, is generally more expensive to launch and maintain but, when successful, prevent any user from any country from accessing the target site. As detailed below, independement media and human rights sites often report being subject to more than one type of attack at the same time, complicating the efforts of the sites to defend themselves.

30 OpenNet Initative, "About Filtering," http://opennet.net/about-filtering.

## 4. Research

To explore the nature and prevalence of DDoS attacks against independent media, we used four different research methods: a review of media reports of relevant DDoS attacks; an online survey of independent media and human rights organizations; technical interviews with independent media publications suffering from DDoS attacks; and a meeting of independent media publishers, network and security experts, human rights NGOs and funders, and academics to discuss the topic. For all of these methods, we focused on a sample of nine target countries chosen for geographical diversity and likelihood to exhibit DDoS attacks against local human rights sites or politically-oriented independent media. Those countries were China, Russia, Iran, Kazakhstan, Uzbekistan, Egypt, Tunisia, Vietnam, and Burma.

### 4.1. Media Review

For three months, beginning in May 2010, we monitored mostly English-language news sources for reports of politically-motivated DDoS attacks. We used a set of Google News alerts crafted to return a superset of stories about DDoS attacks, looking specifically for stories about one of the nine sample countries. For example, our most prolific alert filter was '(+ddos | +"denial of service" | +hacktivism | +defacement | +defaced | +hacked | +hacker | +hackers) AND (China | russia | iran | vietnam | burma | egypt | tunisia | kazakhstan | uzbekistan | censorship)', which returned about 30-60 stories a day, of which 2-3 a week were relevant. We also set up alerts with common translations for terms related to 'DDoS,' 'hack' and 'intrusion' in the primary languages of each of the nine sample countries.

In addition to monitoring these Google News alerts, we mined thousands of Google searches, using terms in English and in the primary languages of each of the above countries, including idiomatic terms from local experts. We also followed any links to other attacks that came up in the reported stories, included attacks that were reported to us by the many contacts we made in the course of our research. We published all reported attacks to a Twitter feed to encourage followers to report attacks back to us, and we specifically searched for attacks against sites included in our independent media sample (described in the survey section below). Although we were searching for DDoS attacks against independent media in the nine sample countries, we included in the list of attacks a superset of those attacks. We included defacement and intrusion attacks as well as DDoS attacks because in many cases

the reports themselves did not make clear the difference between these sorts of attacks. We included politically motivated attacks of all sorts, regardless of whether they were against independent media or human rights oriented sites. And we included reports of attacks against any country, not just attacks in the nine sample countries.

The full list of media reports of DDoS attacks against independent media and human rights sites is available at the following URL:

http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/DDoS Public Media Reports_0.xls

Through this media research, we found reports of 329 different attacks against more than 815 different sites going back to 1998. In the 12-month span from September 2009 to August 2010, we found reports of 140 attacks against more than 280 different sites. We are confident that, despite designing the media research to collect a superset of the desired attacks, we collected reports of only a small portion of all attacks against independent media primarily because most attacks are never reported in the media and because our research methods covered primarily English-language reports. At best, these results should be considered a partial sample of DDoS attack reports, focusing on high profile attacks in the English-language press. (Our survey ended well before the set of recent, high-profile DDoS attacks. We will be interested to see whether giving visibility to DDoS increases the prevalence of this form of attack.)

These numbers confirm that, despite the under-reporting inherent in this method, DDoS and other cyber attacks are common against independent media and human rights sites, even outside of elections, protests, and military actions. We saw a particularly high prevalence of attacks in the USA, Tunisia, Russia, China, Vietnam, Burma, Mexico, Israel, Egypt, and Iran. This list of geographic prevalence again under represents the geographic spread of attacks globally because of our focus on the nine sample countries. But it does show that these attacks are at a minimum spread widely across the world.

We found examples not only of DDoS and other cyber attacks against local sites that offend local governments, but also of attacks across country borders and of attacks by dissidents against the governments of their own countries. In fact, we did not find a single clear case of a government taking responsibility for a DDoS attack, whether against its own dissidents, against activists in another country,

or against another government. This does not indicate that governments are never behind these attacks, but simply that it is very difficult to attribute responsibility for the attacks and/or that governments do not think it in their best interest to take the same kind of responsibility for DDoS attacks that they take for Internet filtering.

In contrast, we found many examples of activists claiming responsibility for attacks, sometimes against their own governments but mostly against either governments or activists in other countries—for example the multiple attacks by the Electronic Disturbance Theater against the Mexican government. Again, this does not show that activist individuals use DDoS attacks more often than do governments, but rather that activists evidently have a greater motivation to claim responsibility for DDoS attacks.

We found repeated attacks between countries beyond the most commonly cited examples of Israel/Palestine, Russia/Georgia, and Russia/Estonia. Other cross-border attacks in our set include China/Japan, China/USA, Armenia/Azerbaijan, Malaysia/Indonesia, Iran/China, Argentine/United Kingdom, Japan/South Korea, and Algeria/Egypt. There were also many reports of attacks between Muslim and European or American actors.

Some of these cross-country attacks coincided with times of crisis in the relationships between these countries. For example, Chinese actors attacked a number of U.S. sites following the shooting down of a spy plane over Chinese soil in 2001, and U.S. actors in return attacked a number of Chinese sites.[31] But many of the reported attacks were triggered by much smaller or less obviously critical incidents and seemed more directly a product of long-simmering cultural or historical conflicts—for instance the major DDoS attacks between Japan and South Korea in 2010,[32] or the attacks between Indonesia and Malaysia over cultural primacy. We found no clear relationship between ideology and use of DDoS attacks; for example, Muslim actors used the attacks to take down conservative political sites in the U.S., conservative American actors used the attacks to take down Muslim jihadist sites, and actors from both sides of the Israel/Palestine conflict took down opposing sites in response to the Gaza flotilla incident.

31 Jose Nazario, "Politically Motivated Denial of Service Attacks," Arbor Networks, 2009, http://www.parliament.uk/documents/upload/F005ArborNazarioarticle131109.pdf, retrieved 3/3/2010.

32 The Korea Times, "Cyber tensions rise ahead of Liberation Day," August 13, 2010, http://www.koreatimes.co.kr/www/news/nation/2010/08/113_71421.html.

The following examples detail some of the most interesting politically motivated DDoS and hacking attacks of the past twelve months:

*The Iranian Cyber Army*

On December 17, 2009, attackers replaced the front page of Twitter.com with an image of the Iranian flag along with text including: "This site has been hacked by the Iranian Cyber Army." The attackers did not actually gain access to Twitter's servers, but instead changed the twitter.com domain name to point to a different IP address (the IP address of the machine hosting the "hacked by ..." page). Twitter took down its home page entirely within minutes and twitter.com remained down for a couple of hours.[33] A similar attack was executed a month later against Baidu,[34] the most popular search engine in China, with similar results: the hack page was taken down in a few minutes and the site was down for a couple of hours.

At the same time that Twitter was attacked, Green Movement site mowjcamp.com was attacked via a similar method,[35] and it featured an identical page claiming responsibility by the Iranian Cyber Army. Unlike Twitter and Baidu, which are among the core hypergiant websites, Mowjcamp is a small citizen media site living at the technical and organizational edge of the network. And unlike Twitter and Baidu, Mowjcamp remained down for fully six weeks after the initial attack.

To redirect mowjcamp.com to the hack page, the attackers had hacked into Mowjcamp's account at its DNS registrar—the company hosting its domain name—and changed the settings for the mowjcamp.com domain name so that they appeared to be the contacts. As the official contact, the attackers then successfully executed the process an owner would use when moving a domain name to a new registrar. They then changed the contact details to an entirely fake, but convincing, American identity. When Mowjcamp contacted their registrar to have the changes reversed, they found that not only were they not listed as the official owners, but the registrar themselves no longer had control of

33 Scott Peterson, "Twitter Hacked: 'Iranian Cyber Army' signs off with poem to Khameni," Christian Science Monitor, December 18, 2009, accessed October 15, 2010, http://www.csmonitor.com/World/Middle-East/2009/1218/Twitter-hacked-Iranian-Cyber-Army-signs-off-with-poem-to-Khamenei.

34 Robert Mackey, "'Iranian Cyber Army' Strikes Chinese Website," New York Times Lede Blog, January 12, 2010, accessed October 15, 2010, http://thelede.blogs.nytimes.com/2010/01/12/iranian-cyber-army-strikes-chinese-site/.

35 Robert Mackey, "Twitter Attacked by 'Iranian Cyber Army'," New York Times Lede Blog, December 18, 2009, http://thelede.blogs.nytimes.com/2009/12/18/twitter-hacked-by-iranian-cyber-army/.

the domain name. The registrar who now managed the domain name had a completely different US owner, who had apparently paid his dues, but was otherwise not contactable. Mowjcamp's original registrar told them to file a letter to begin a DNS dispute resolution process; a lengthy process designed to mediate trademark disputes and conflicts between registrars, but was not built to defend against politically motivated hacking. None of the participating players could expedite this process alone, despite the fact that the newly redirected page explicitly stated, "This site has been hacked...."

Mowjcamp was a small-scale client of its registrar. Unlike Twitter and Baidu, which were able to make their registrars respond within minutes, Mowjcamp encountered only bureaucratic brick walls while trying to get the problem solved quickly. The parties involved finally resolved the problem in response to a highly publicized blog post by one of the authors of this paper, and a complex series of technical and legal steps arbitrated by an independent third party, the Electronic Frontier Foundation. Ironically, the blog post accused the wrong company of inaction. That company—Yahoo!—was just as hamstrung by the hackers' actions, but to its credit, was able to use its own reputation to help bring the two relevant registrars to the table. Despite the final positive outcome, the net effect of this attack was a denial of service by bureaucracy.

A basic lesson learned from this attack: DNS service is a critical component of every website and is a likely weak point for attacks. A larger lesson: Attacks designed to silence a website are often much messier than the prototypical example of a large botnet flooding a website with network traffic. In this case, the actual technical attack was an intrusion into the Mowjcamp account used to control its DNS service, resulting in site defacement. The ultimate effect was a very prolonged denial of service. The underlying problem in this case was not technical, but the inability of Mowjcamp to cut through bureaucratic processes not designed to deal with these situations, a problem common for actors at the edge of the network.

*Vietnam versus Bauxite Vietnam?*

Bauxitevietnam.info is an activist site created to protest the environmental risks of bauxite mining in Vietnam. It is specifically intended to question the wisdom of a Chinese-backed project to mine bauxite

in an environmentally sensitive region of Vietnam.[36] In January 2010, a botnet DDoS attack took the site down. The botnet originating the attack consisted largely of computers infected by a Trojan Vietnamese keyboard input program.[37]

VPSKeys is the most popular Vietnamese keyboard input program. Distributed by the Vietnamese Professionals Society (VPS), it allows Vietnamese users to easily enter Vietnamese characters using Western keyboards. At some point in late 2009, the website hosting the software was hacked, and the VPSKeys program was replaced with a Trojan version that included code to infect the computer with botnet software. Thousands of VPSKeys users were also alerted via email that a new (infected) version of the software was available, and many updated their software in response. It is possible that the mailing list used to distribute the Trojan came either from a compromised VPS server or from email addresses collected from hacking attacks that seized membership databases of popular Vietnamese discussion forum sites in 2009.

Tens of thousands of users downloaded the Trojan software and were added to a botnet before the Trojan software was found and replaced on the VPSKeys site. That botnet was used to mount a DDoS on Bauxitevietnam.info and may have been used against other targets. It is unclear why attackers created their own botnet instead of renting a commercially available one; one possible explanation is that a botnet of computers based in Vietnam would be very hard for a site administrator to defeat through geographic filtering, as blocking requests from Vietnam would defeat the purpose of the site.

Bauxitevietnam defended itself by mirroring its content onto multiple sites at different hosting providers: bauxitevietnam.info, boxitvn.org, boxitvn.net, boxitvn.info, boxitvn.blogspot.com, and boxitvn.wordpress.com. The last two are especially important, because they are hosted by big blog hosts—Blogger and WordPress—which offer highly DDoS-resistant services at no financial cost to the activists. This example again shows how DDoS attacks are often entangled with intrusions and malware, as well as demonstrating the common pattern among attacked sites to diversify their hosting and especially to flee to large blog hosts when under attack.

36 Bauxite Vietnam, http://bauxitevietnam.info/.

37 Viet Tan, "Denial of Service: Cyberattacks by the Vietnamese Government," April 27, 2010, accessed October 14, 2010, http://www.viettan.org/spip.php?article9749.

It has been impossible to determine who controls the botnet used in the Bauxitevietnam attacks, but there are indications that some DDoS attacks focused on Vietnamese sites involve more than tacit approval of the Vietnamese government. Viet Tan, a dissident organization whose stated mission is to bring peaceful change to the Vietnamese government, reports that their site is routinely hit by DDoS attacks and that many of the attacking computers are based in Vietnam. As viettan.org is generally blocked in Vietnam, this implies that authorities are temporarily unblocking the site to permit attacks from Vietnamese zombie computers to take place.

*Anonymous and "Operation Titstorm"*

In February, 2010, a group of people loosely connected through Internet forums calling itself "Anonymous" executed a DDoS attack against the Australian Parliament's website. The attack took down the site for two days. On the same day that Anonymous attacked the parliament's website, the group also defaced the Prime Minister's website, briefly replacing the front page with pornographic images. The attack was termed "Operation Titstorm" by its organizers, referring to a mandatory Internet filtering policy proposed by Australia's ruling party designed in part to counter pornography.[38]

The DDoS attack was carried out by volunteers, organized via posts on sites like 4chan and Something Awful. Arbor Networks measured the attack at only 16.5 Mbps, small for a traffic-based attack but sufficient to disable the Parliament's site. The response of the attacked website was merely to weather the storm until the attack ceased.

On September 18, 2010, a similar attack targeted the Motion Picture Association of America's website. The call to arms was issued on 4chan and promoted on popular Internet culture site Reddit. Participants were encouraged to download and install "Low Orbit Ion Cannon," an easy-to-use DDoS tool distributed via open source software hosting site SourceForge. The attack disabled MPAA's site for over twenty hours, and similar attacks on the Recording Industry Association of America disabled that site periodically for four days.[39] More recently, Anonymous has claimed responsibility for DDoS attacks on

38 David Kravetz, "Anonymous Unfurls 'Operation Titstorm'," Wired Threat Level Blog, February 10, 2010, accessed October 15, 2010, http://www.wired.com/threatlevel/2010/02/anonymous-unfurls-operation-titstorm/.

39 Declan McCullaugh, "Attack Disables Music Industry Website," CNET News, July 29, 2002, accessed October 14, 2010, http://news.cnet.com/2100-1023-947072.html.

companies that stopped providing service to Wikileaks in the face of government pressure, including Amazon, PayPal, Visa, MasterCard and PostBank.

These attacks suggest that DDoS attacks need not use amplifiers or botnets to wreak havoc; a relatively small number of volunteers working in coordination can disable a mid-sized site. One downside of this sort of attack for the attacker, however, is that a volunteer attack can be difficult to maintain, since it requires maintaining the interest and participation of the volunteers. It also suggests that attacks using this technique will be most likely to affect targets that can harness the ire of a large group.

*The Jester and Xerxes*

A hacker identified as "The Jester" (th3j35t3r) carried out several attacks during 2009 and 2010 against sites he identified as "jihadist" websites. Using a tool he'd designed, termed "Xerxes," he demonstrated to journalists the apparent ability to disable targeted sites using a single machine to launch the attacks.[40] We found accounts of attacks attributable to The Jester on 29 separate sites during the past year using a variety of techniques. The Jester announces his attacks on his Twitter feed—http://twitter.com/#!/th3j35t3r—and has claimed responsibility for the November 28th attacks against Wikileaks.org, which he condemned for endangering US troops.

The example of The Jester suggests that knowledgeable individuals may be capable of launching effective attacks by themselves without compromising third-party computers to act as zombies or recruiting a pack of volunteers. It is likely that The Jester's attacks are easy for an experienced system administrator to combat, as they originate from a small number of IP addresses, but the effectiveness of the attacks points out that many sites do not have an experienced system administrator and so do not have capability to conduct the most basic IP filtering.

**Observations**:

40 Jennifer Hesterman, "Cyber vigilantes: Citizen hackers go to war against terrorists," The Counter Terrorist, September 1, 2010, accessed October 14, 2010, http://www.homeland1.com/domestic-international-terrorism/articles/873689-Cyber-vigilantes-Citizen-hackers-go-to-war-against-terrorists/.

- There is no obvious connection between the ideology of an attacker and the choice of DDoS as an attack method. We saw attacks from ostensibly right and left wing groups, attacks that targeted governments and attacks that suggest government involvement.
- There is no apparent geographic pattern to the DDoS attacks we saw in our media analysis—we saw attacks reported in widely disparate corners of the world.
- While there is speculation that some attacks are traceable to governments—for instance, in the Vietnam and Iranian examples—it is unclear this is a safe assumption. Attacks on Russian independent media sites suggest pro-government youth may be at work (as Jose Nazario speculates in his report, suggesting that subtle cues in Russian government language can apparent trigger responses from nationalist youth).[41]
- DDoS is a technique used by individuals, groups, and perhaps by states. The accessibility of easy-to-use tools and the apparent success of single-user attacks on small websites, as well as the visibility of the technique in the media, suggests that aggrieved individuals may look to DDoS as an easy way of making a political point or settling a score.

### 4.2. Survey

We invited representatives of 317 independent media and human rights sites to participate in a survey on DDoS attacks against their organizations. We generated the sample by asking at least three local experts in each of the nine target countries for the most prominent independent media in their countries. We translated the survey into the primary Internet language of each surveyed country and also translated the recruitment email into the primary language of each site.

Forty-five of the sites responded to the survey, for a response rate of 14%. Though not high, this is an acceptable response rate for an online survey of this sort, especially given the difficulty of reaching key actors at each site, the inherent sensitivity of the survey subject, and the technical nature of the survey subject. In enlisting the help of experts to compile lists of sites, we used neutral language that did not refer to DDoS attacks, but some of the experts were familiar with our work. It is therefore possible that these experts biased their lists of independent media toward sites known to suffer DDoS attacks. It is also likely that the 14% of sites that responded to the survey over represents sites that have suffered a DDoS attack merely because a survey on the subject is more likely to be relevant and therefore

41 Jose Nazario, "Politically Motivated Denial of Service Attacks."

interesting to DDoS attack victims. These two factors make the results of the survey less useful for answering questions about overall prevalence of DDoS attacks (e.g., "What percent of all independent media sites have suffered DDoS attacks?"), but the responses remain useful for investigating the nature of attacks reported by the surveyed sites and the defenses used by those sites.

The full survey and aggregated responses to the survey are available at the following URL:

http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/DDoS Survey Public Results_0.pdf

A core finding is that DDoS attacks exist within a range of different attacks suffered by these sites, and that the same site usually suffers from multiple types of attacks. During the past year, of the surveyed sites:

- 72% have experienced national network filtering at the national level;
- 62% have experienced DDoS attacks;
- 39% have experienced an intrusion; and
- 32% have experienced defacement.
- Of those experiencing a DDoS attack, 81% also experienced at least one of filtering, intrusion, or defacement.

These numbers provide strong evidence that DDoS attacks are not an isolated problem for independent media sites, but instead exist within a larger problem of broad range of different kinds of attacks against the sites. In addition to the specific range of attacks reported above, the surveyed sites reported a high level of "unexplained downtime" (in other words, a period during which the site was inaccessible, neither for the reasons above nor for routine maintenance) during the past year:

- 61% experienced unexplained downtime.
- Of these, 48% experienced 7 or more days of unexplained downtime.

Unexplained downtime can be the result of factors other than attacks. Independent media sites often suffer from a lack of experienced system administration help that, predictably, leads to both downtime

and the inability to diagnose the downtime. Still, the very high amount of unexplained downtime experienced by these sites suggests more, and possibly more complex, attacks than described by the DDoS question above. These numbers contrast strikingly with the data from the 2009 Arbor survey of core Internet services, which reported that 76% of their respondents mitigate a typical attack within an hour.

The survey respondents had mixed luck with getting their ISP to defend them against attacks. Of those who experienced a DDoS attack in the past year:

- 55% had their site shut down by their ISPs in response to the attack; and
- 36% report that their ISP successfully defended them against a DDoS attack.

The number shut down by their ISPs is especially high considering that an ISP will usually only shut down an attacked site when subject to a traffic-based attack. The fact that 55% of respondents suffering a DDoS attack had been shut down by their ISPs first indicates that at least 55%, and almost certainly more, of the sites had been subject to a traffic-based attack. That fact, along with the fact that only 36% of the respondents subject to DDoS attack had an ISP that defended them against attack, indicates that for many independent media, the local ISP is a weak point rather than a strong ally. We do not know whether this poor defense of sites by their ISPs is because independent media sites are customers of ISPs outside of the core of ISPs able to respond to an attack in under an hour, or whether it is because the independent media sites are customers of the core ISPs but are unable to pay for DDoS protection.

The survey included questions about which defenses had been tried by respondents suffering from DDoS attacks and how effective those defenses had been. These responses can be read as a map of how independent media escalate defenses against DDoS attacks:

- 83% had fixed problems with their existing web application software, with 80% reporting that this measure was “somewhat effective” or “effective”;
- 75% had installed security software or hardware on their existing servers, with 92% reporting this was “somewhat effective” or “effective”;

- 62% had upgraded their web server hardware, with 88% reporting this was “somewhat effective” or “effective”;
- 43% had downgraded the functionality on their existing sites, with 33% reporting this was “somewhat effective” or “effective”;
- 40% had subscribed to a denial of service protection or other security service, with 100% reporting this was “somewhat effective” or “effective”;
- 38% had hosted content temporarily on a large hosting provider (Blogger, LiveJournal, etc), with 67% “somewhat effective” or “effective”;
- 36% had changed their hosting providers, with 80% reporting this was “somewhat effective” or “effective”; and
- 29% had changed their web application software, with 75% reporting “somewhat effective” or “effective”.

The vast majority of sites that experience DDoS attacks try to update their local machine setups by fixing the existing web application software, installing local security hardware or software, and/or upgraded local web server hardware. These are all actions that can be taken by individual sites at the edge of the network without help from core network providers (though in some cases core technical expertise may be needed to properly apply these upgrades). Each of these approaches rates as at least somewhat effective, meaning that most sites respond to attacks by making changes to their local server infrastructure and that those changes are somewhat effective against further attacks.

A smaller number of sites escalate by either implementing more aggressive (and costly) defenses at the edge—downgrading functionality or changing web application software—or by moving closer to the core of the network—subscribing to expensive protection services, hosting content on large providers, or changing hosting providers. The success of these defenses is more mixed than the simple edge fixes, perhaps because these are the defenses that must be taken in response to network attacks, which are much more difficult to defend against.

Our results indicate that the number of attacks against each site increased for a slight majority of participating sites:

- 16% reported many more attacks this year;
- 36% reported somewhat more attacks this year;
- 20% reported the same number of attacks this year; and
- 28% reported fewer attacks this year.

Despite their prevalence, DDoS, intrusion, and defacement attacks are not the primary concern for most independent media sites. Asked the impact of various issues, participants placed DDoS, intrusion, and defacement attacks in the middle of the other issues. The issues were ranked in the following order, with the most important issue listed first and with the average rank out of 5 noted (a higher number implies a lower priority):

- blocking access to the publication's site by the government (2.47);
- persecution of authors, publishers, or sources by the government (2.53);
- intrusions, defacements, and denial of service attacks (2.89);
- financial support for the publication (3.00); and
- technical issues other than defending against attacks (3.89).

Only 11% of respondents chose DDoS, intrusion, and defacement attacks as the most pressing issue, and only 32% chose the attacks as one of the two most pressing issues. These are particularly interesting findings given the bias of the study toward respondents facing such attacks. By comparison, 68% of respondents chose persecution of authors, publishers, or sources by the government as one of the two most pressing issues.

Observations:

- The strong correlation between sites that experienced filtering and those that experienced DDoS suggests that a large percentage of the sites that answered our survey are perceived to be controversial in their local settings. We were seeking insight on precisely those sites, which suggests we might be able to generalize from our results to draw conclusions about other sites targeted by filtering.

- The strong correlation between DDoS, filtering, defacement and intrusion echoes a pattern we saw in our media analysis. These techniques often used in conjunction, and may have synergistic effects—making a site more DDoS resistant can make it more difficult to access via a web proxy, for instance, which makes state-based filtering more effective.
- Our finding that a significant number of sites have experienced 7 days or more of downtime suggests that there is a serious shortage of technical and human resources available to respond to threats to independent media and human rights websites. Arbor's annual survey of Tier 1 and Tier 2 network operators suggests that most core network operators are able to respond to a typical DDoS attack within an hour.
- Internet service providers—who are best positioned to defend sites against many types of DDoS attacks—are often unable or unwilling to defend their customers. This leads us to speculate that many of the sites we surveyed are hosted (or were, as many have been dropped by those providers) by either Tier 3 providers, who may lack a financial incentive to protect their customers, or by larger providers but without an add-on DDoS protection service. Many webhosting providers sell their services for a small margin over costs; the hour's worth of system administrator time necessary to fend off a DDoS attack is more costly than the annual profit for the average account. These providers evidently don't see a reputation risk in failing to fend off DDoS, and they find it more profitable to end relationships with “troublesome” customers than to provide protection to them.
- The apparent efficacy of upgrading servers and fixing web server software strongly suggests that attacks are not all based on clogging network connectivity (where these techniques would be ineffective) and point to application level vulnerabilities. These sorts of fixes are only really helpful for either very small traffic attacks or application attacks, both of which can be reasonably dealt with by individual publishers at the edge of the network.

### 4.3. Interviews

We conducted a combination of in-person, Skype, and email interviews with administrators of twelve sites that experienced DDoS attacks. We contacted every survey respondent who reported having been subject to a DDoS attack and asked to conduct a more in-depth interview. Six of the interview participants were recruited through this method. We found the rest of the interview participants through media reports of attacks or referrals from researchers and other contacts in the field. We

interviewed administrators of sites based in Australia, Burma, China, Iran, Russia, and Vietnam. The interviews involved a series of questions and answers digging into the technical details of attacks and the experiences of the administrators dealing with them. In a few cases, we were able to obtain and analyze logs of attacks. We cannot publish the interviews themselves for security reasons, but we include a number of findings from the interviews below. We also had the opportunity to study a DDoS attack on the servers hosting the Citizen Media Law Project, which are administered by colleagues at the Berkman Center. We are grateful to the unknown attackers for giving us this opportunity to study an attack in progress.

As a result of these interviews, we present the following findings:

**Hybrid attacks**: The interviews provided further confirmation from the findings in both the survey and the media research that DDoS attacks are often accompanies by intrusions, defacements, filtering, and even off-line attacks. One site admin reported DDoS attacks followed by off-line extortion, intended to force him to retract a story (he refused). That same admin reported being subject not only to DDoS attacks but also to daily virus-laden emails targeted to him personally and to topics of confidential interest to him; to weekly intrusion attacks based on guessed passwords; and to weekly defacement and complete deletion of sites. Another admin had been subject to weeks-long, multi-gigabit DDoS attacks but reported that a greater problem was the harassment of participants of the publication's discussion forums: attackers hacked into the discussion forum to steal and publish the identities of its users and also posted inflammatory content to the forum to trigger governmental prosecution. Another admin reported that intruders had repeatedly accessed internal databases to learn about stories before they were published. And another reported that attackers hacked into his site to insert malicious code with the intent of triggering anti-virus warnings for the site and thereby scaring users from accessing the site and slowing their Internet connections by causing them to download large packages of Trojan horse software.

**High and low bandwidth attacks**: Interview participants reported a mix of high bandwidth traffic attacks and low bandwidth application attacks. Five of the interview participants reported attacks in the range of 500 Mb–4 Gb. One participant, who was the administrator of a large service provider working for an independent media site, reported an attack of greater than 10 Gb. Some of these attacks may have been

bigger, since at greater than 1 Gb, many local ISPs become saturated and drop any additional traffic. One interview subject, whose site has experienced several DDoS attacks in the past four years, reported an escalation in size. The site had sustained a successful DDoS attack in 2007 with a 1 Gb attack, and moved to more robust, DDoS-resistant hosting. An attack in 2010 involved 4 Gb of traffic and exceeded the amount of protection the administrator had contracted for. The DDoS-resistant host stopped routing traffic when the administrator was unwilling and unable to pay for a higher level of service.

Three interview participants reported application attacks at low or even very low bandwidths that caused significant downtime. One was taken down by fewer than forty thousand requests per day, another by less than ten machines hitting his search page. Two participants reported long term success using mitigation strategies—caching and web application optimization—that would only help against relatively low bandwidth attacks.

**Evidence of botnets**: It is likely that most network attacks against independent media and human rights sites involved the use of botnets to generate sufficient incoming traffic. Other indicators suggest attacks from botnets rented to perform the attacks. Two interview subjects reported that attacks began and ended at the top of an hour, suggesting that a botnet had been rented for a specific duration.

The DDoS attack Citizen Media Law Project suffered was an application attack using HTTP GET requests originating from a shifting set of exactly 500 IP addresses. The attack was highly effective, rendering the site inaccessible for 12 hours despite steady work from our skilled administrators to keep the site online. That the attack came from a round number of attacking IPs and that the IP addresses in use shifted during the attack suggests that the application attack came via a botnet.

Difficulty obtaining hard data: Though we were able to obtain logs of some attacks, many of the participants were unable to provide us with logs: they simply did not have access to them because they have outsourced system administration duties to an ISP or hosting provider. Multiple participants reported that their ISPs had told them they were under DDoS attack of a certain size, but they had no way of verifying the size or method of the attack.

**Bad ISPs and better ones**: As with our survey results, we found a pattern of participants getting little or no support from their ISPs in defending against DDoS attacks: four of the participants reported that their ISPs had removed their sites from the Internet in response to an attack. Some participants moved to new ISPs promising some level of DDoS protection, which in some cases is free, though can cost up to USD 2000 per month. The experience of the participants with their new ISPs did not correlate with the cost of the new ISPs. One site moving to the USD 30/month ISP reported no further downtime from DDoS attacks, though it's unclear whether that success is due to the site not getting attacked again (and if so whether the cessation of attacks was related to the move to the new ISP). One site moving to a USD 700/month ISP is unhappy with the service due to a lack of specific knowledge of or support for human rights sites. The site happiest with its service is paying nothing for the new ISP, which is hosting the site at no cost, both for charitable reasons and to study the data on incoming attacks to better understand how to fend off DDoS.

**Apportioning blame**: Most sites participating in the interviews expressed a strong belief that the national government of the country was ultimately responsible for the attacks, even though none had clear evidence for governmental responsibility. One participant noted that he reported a large, ongoing attack to the government security service but got no help because "it is very difficult to look into this because it is very difficult to catch yourself." In other words, he claimed that the government was not helping him defend against the attack because the government was responsible for the attack. He asserted that the security service shut down its own attack only when other publications better connected to the government complained. One Vietnamese site pointed to a press report of a Vietnamese military official claiming responsibility for the attacks. Another Vietnamese admin noted that his site was normally filtered from within Vietnam but that the filtering was taken down at precisely the time that a botnet from within Vietnam attacked the site. An Iranian site was attacked by malware hosted on a major site friendly with the Iranian government; visitors to the government's official newspaper triggered a JavaScript that flooded the opposition site with page requests.

**Local experts**: In three of the interviews, we found a pattern of local technical experts acting as hubs of technical expertise for their countries (Vietnam, China, and Iran). The most productive of these local experts was in the process of moving sites in his country to a common infrastructure well supported by a supportive hosting provider well connected to the core of the Internet. He was able to exert a great deal

of control over the structure of the moved sites, including imposing onerous security and posting restrictions on the administrators of the sites. The least happy of these local experts was struggling daily with many poorly written sites on broken, incompatible codebases, often reinstalling a site from scratch following an intrusion and manually fighting off the simpler of the constant DDoS attacks to the sites. He expressed desire to improve his architecture but did not have the resources to fix the underlying problems with the supported sites; he also expressed gratitude for the help he has received from other individuals but frustration at his inability to fend off high-bandwidth traffic attacks.

### 4.4. Working Meeting

We hosted a day-long working meeting to collaborate on responses to DDoS attacks against independent media. Thirty-five people attended the meeting, representing independent media sites who have suffered DDoS attacks, human rights technology NGOs and funders, academia, and the hosting and security industries. The goals of the meeting were to share knowledge about DDoS attacks from the different perspectives of the meeting's diverse participants and to critique a very early draft of this paper. We also had conversations with a number of people within core Internet hosting and security companies that were unable to attend the meeting but were willing to talk about the ways they might assist threatened independent media organizations.

*From media and human rights organizations*:

Independent media organizations participating in the working meeting repeated the same theme from the survey and the interviews: namely, that sites suffer from multiple types of attacks, including DDoS, with complicated impacts on one another. A key example of these impacts was the problems that a prominent independent site experienced between DDoS attacks and national filtering. The site has moved to a DDoS resistant hosting provider to protect itself against years of high bandwidth traffic attacks. The site is also filtered by its national government, so people within the country have to use proxies to access the site. It is typical for people within the same country to use the same few proxies discovered through word of mouth. All of the traffic from each of those proxies appears to come from the same IP address. Since the proxies submit many more requests than other IP addresses, the hosting provider often bans them, to the end effect of blocking many of the users from the country for which the site is written.

The non-DDoS attacks on a site are often more serious and less tractable that DDoS attacks. A common attack method for intrusions is to compromise the computer of someone who has administrator level access to the target server. Administrators of human rights related independent media consistently report being frequently subject to specifically targeted email viruses among other forms of attack. These specifically targeted attacks are very difficult to defend against, requiring a high level of training and support for the victims. But many or most of the independent media organizations struggle to maintain even very simple client-side technology infrastructures.

For example, one participant—an administrator of one of a handful of the most prominent and well-funded independent media organizations in its country—reported that it shared two desktop computers among its staff of over fifty people and that many of those staff members had never touched a computer before working for the publication. Defending client computers that are so widely shared and used by such inexperienced users against personalized, aggressive attacks is enormously difficult for even one organization, let alone for the field as a whole.

Another independent media participant argued forcefully that although DDoS attacks were a pressing concern for independent media in his country, other types of online and offline attacks were much more serious. One particularly effective type of attack used against multiple sites was to hack into their internal servers to gain access to confidential information about forthcoming stories and about the identities of authors, sources, and readers and then to use that information to harass those users offline, sometimes before the publication of a story.

Two of the independent media participants reported attacks coming from multiple different sources, as well as confusion as to where attacks were coming from. One participant was subject to a DDoS attack when he published a story about a prominent government actor; he was then approached separately by both the government actor with demands to take down the offending story and by the cybercriminals executing the attacks with demands for money. Another participant pointed out that his site is sometimes attacked by the government when it is unhappy with a particular story and sometimes attacked by activists in opposition to the government when they are unhappy with a story (and sometimes the activists have taken credit for attacks that the participant thought were certainly coming

from the government). Others pointed out that, in many cases, the goal of a DDoS attack is to generate press for the attackers rather than to take and keep a site down.

*From industry experts:*
A representative of a core company that sells DDoS protection services outlined the following possible responses to a DDoS attacks:

- "blackhole" the IP address of the attacked site, i.e, take the attacked site offline;
- deploy additional network and server infrastructure for the attacked site;
- downgrade the content and/or functionality of the attacked site to reduce resource consumption;
- filter out attack traffic; and
- use a service with a distributed architecture to scale and absorb attacks on demand.

Blackholing the IP address of the attacked site accomplishes the purpose of the attacker by making the site unavailable, but it also makes the attack traffic disappear entirely from the Internet, so it protects the network hosting the site. This is the approach taken by many ISPs who are faced with a large traffic based attack that is either too big or too expensive for them to defend against.

An attacked site may deploy additional servers and bandwidth to protect itself. Our survey results show that this is indeed the most popular method of protection. But for all but the biggest sites, deploying additional infrastructure for a single site is only cost effective for small, application-based attacks because the peak traffic of a large, traffic-based DDoS attack will be orders of magnitude larger than the peak legitimate traffic of a site. Adding additional infrastructure can help a small- or medium-sized site scale to meet the additional demands of an application attack or a small network attack, but adding enough infrastructure to handle a large network attack on a small- or medium-sized website would require hundreds of times more machine and network infrastructure to handle the load. The possibility of on-the-fly provisioning makes cloud services like Amazon Web Services an attractive option for short-term scaling to respond to attacks. Wikileaks moved servers to AWS briefly in early December 2010 to respond both to heavy load and a DDoS attack—Amazon controversially shut the site down under US government pressure.

An alternative to increasing the server resources is to reduce the resource consumption of each page, allowing the server to handle more traffic with the server hardware and network. There are some methods for reducing resource consumption that are effective and have little cost, such as caching dynamic content to reduce database queries. As attack size increases, though, an attacked site has to make changes that have costly side effects, like disabling site functions that require expensive database queries, reducing or eliminating images and streaming media, or creating an entirely separate failover site with simpler and less interactive content.

Another way to reduce resource consumption is to distinguish attacking traffic vs. legitimate user traffic and filter out the attack traffic. One common way to filter traffic is to filter out attacking IP addresses. Several of our meeting and interview participants reported success with this method, but only when the number of attacking machines is small and relatively static. It is simple for a competent system administrator to find and block 100 static IP addresses that are flooding a site with requests for a single page, but that job becomes much, much more difficult when tens of thousands of IP addresses are rotating every couple of hours. In these cases, it is sometimes possible to filter attacking traffic based on a signature for the particular traffic, but this approach can be very difficult against a moderately skilled attacker even for a highly skilled defender. It is possible to defend against a range of common attacks by using ModSecurity,[42]* an open source attack filtering system. But this sort of filtering only helps against generic attacks, and it uses up machine resources for the process of filtering and can therefore make the site more vulnerable to traffic-based attacks.

Finally, a site can protect itself by paying for a hosting or DDoS protection service. There are many services capable of handling all but the biggest attacks, and a few capable of handling the biggest observed attacks, simply because they have sufficient bandwidth and server resources to accept and process the attack traffic. The advantage of using such a service is that these services have economies of scale both in learning how to defend against particular attacks and in the necessary bandwidth and servers. When using such a service, the attacked site only needs to pay for the peak attack traffic while the attack is happening, rather than paying for the entirety of the resources need to handle peak attack traffic.

42 ModSecurity, http://www.modsecurity.org/.

These services, however, can have a very high markup on those resources, and even without the high markup simply paying for the bandwidth to handle the peak attack traffic can be prohibitively expensive. An attacked site may be able to pay a provider to handle millions of requests per second, but most sites cannot afford the resulting bandwidth charges.

The economies of scale work best for the these services if a large proportion of their sites is not likely to be attacked at the same time, which fact is important to keep in mind given the model we found in interviews of a single local expert managing many sites from a given area (meaning that all or many of those are likely to be attacked at critical times for the country).

Given the tradeoffs of the various defense mechanisms, it is critical for sites that know they are likely to be attacked to weigh the various options before getting attacked, for instance whether to pay the startup costs to hire a protection service, how much to pay a service to withstand a traffic-based attack, and at what point to accept that the cost of defending against a given attack is too high.

*On cooperation:*
A main theme that we have heard from respondents was the need to bridge the divide between technology organizations capable of protecting against attacks and the independent media who need protection.

A model for providing support for far-flung independent media publications in the past has been to fly smart technical people around the world to provide help, advice, and training for independent organizations subject to DDoS attacks. But this model is very expensive and not very effective because of the difficulty for even a very smart technical person to quickly and thoroughly understand both the particular technical setup and the particular organization using the technology.

From the independent media side, many actions needed to protect against DDoS and other attacks involve some fundamental changes in how the publication works, and it is difficult for them to understand and trust operational changes from an unknown person who is not a member of their community.

In discussions about how to solve this divide, a recurring theme was the need to build up and connect communities among and between core network organizations and independent media organizations. Independent media organizations are resistant to talk to and take the advice of strangers, but are much more willing to place trust in a technical expert with known ties to their community. On the core network organizations side, fending off large scale DDoS attacks often requires the ability to communicate with other core network operators at large ISPs. As with the independent media organizations, these core network operators operate within closed communities of people they know and trust. In between these two groups there are impossibly large gaps of language, of cultures, and of knowledge.

One possible solution to this divide is to identify and strengthen communities of independent media built around local technical experts on the one side and to grow communities of core network organizations willing to help independent media on the other side. We will explore this idea further in the recommendations section below.

## 5. Recommendations

Based on our findings, we offered a set of possible recommendations to participants in our meeting. Four breakout groups offered feedback on those suggestions, which we've incorporated into a revised set of recommendations. These are likely to evolve and improve as we seek feedback from a larger audience with the publication of this research.

These recommendations are not designed as a “one size fits all” policy for entities that might experience DDoS—they're specific to the independent media and human rights organizations that were the target of our study. As such, we assume the financial and expertise constraints that characterize many of these organizations and look for recommendations that are appropriate given these constraints.

Note also that these recommendations address only DDoS attacks directly. For example, the first recommendation for all sites under threat from general cyber attacks would be to robustly backup all valuable data, but we do not include this or other such general security or systems recommendations below.

**For organizations**:

- Every independent media organization should consider carefully whether it is likely to be the target of a DDoS attack in advance of an attack, keeping in mind that a core finding of this paper is that DDoS attacks are common against a broad range of independent media and human rights sites in a broad range of countries even outside protests, elections, and military actions. Any organization which might be targeted by DDoS should make decisions about hosting based on a combination of expertise and financial constraints. Expertise is probably a more important factor than financial constraint; administrators who are not comfortable configuring front-end proxy servers or using iptables (a user space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall and the chains and rules it stores) to block abuse from specific IP addresses should seek a hosting arrangement where an experienced system administrator is able to offer these services.
- For organizations with little technical expertise and few financial resources, the appropriate path is likely to be hosting websites on Blogger, WordPress, or other major hosting platforms

that provide high levels of DDoS resistance at no financial cost to the organization. There are many compromises involved with hosting on Blogger, WordPress, or another large blog host—increased risk of filtering in some countries as some countries block entire blog hosting domains, reduced functionality, limits on user management—but smaller publications that risk frequent attack may find the benefit of free, high quality DDoS resistance to be worth these compromises. Amazon's decision to suspend services to Wikileaks is a reminder of an additional concern—should a site host content that falls afoul of the hosting company's terms of service, the site may be disabled with little notice or recourse. Unfortunately this concern applies to all webhosting companies, not just to large providers like Amazon, Wordpress or Google.

- Organizations with expertise constraints but fewer financial constraints should consider using existing DDoS-resistant hosts, with the caveat that few can guarantee uptime in the face of high-volume, sustained DDoS. Organizations should ensure that the site is mirrored on platforms like Blogger or WordPress and configured so that it can fail over to these more resistant (likely lower-functionality) backups in the face of an attack.
- Organizations with high levels of in-house expertise should consider using customized publishing platforms that allow for graceful degradation in response to high load and automated failover to mirror sites. They should implement caching strategies than minimize the impact of application attacks. They should work closely with local technical experts who have built relationships with core network operators so they can seek upstream assistance in fighting off network attacks.

**Every organization should**:

- Have a live mirror of its site that is not publicly announced. This mirror should use infrastructure that's independent of the infrastructure used to host the main site. In many cases, the appropriate mirror is one hosted with a larger, DDoS-resistant site close to the core, like Blogger.
- Decide well in advance of an attack a failover strategy in the face of sustained DDoS. In developing the strategy, organizations should consider what level of downtime they consider acceptable, and recognize that 99.9% uptime may be very expensive to ensure for a site that experiences frequent attack. Some sites may simply choose to remain inaccessible in the face of a large-scale attack. Others might permit different levels of downtime depending on

circumstances—a site promoting an opposition candidate might be willing to pay for high uptime in the period immediately before an election, but not all the time.

- Implement a monitoring strategy that is sensitive both to page load times and to changes in page contents. If page load is slowed significantly or the contents of a page changes unexpectedly—from defacement or insertion of malware—the monitoring system should warn the administrator and be able to trigger failover to a mirror site. CyberSpark.net is one provider promising this functionality for human rights and independent media sites.
- Ensure that it has clear and indisputable ownership of its domain name, and that it can quickly redirect and alter the time to live (TTL) of the IP/domain name association. Organizations that are at high rirsk of attack should maintain the TTL of their domains as a very short interval (less than five minutes) to allow quick recovery in the case of a domain hijack. Organizations should establish procedures with their registrars designed to prevent domain name hijacking. This might include requiring approval for a change via PGP-signed email or requiring the registrar to call a specific phone number to seek change authorization. This recommendation would have helped mowjcamp.org avoid a long DDoS by bureacracy attack.
- Disclose the risk of DDoS attack to its hosting company, and ask if the host will promise not to null route in the face of an attack. Organizations should also ask if the host has alternative routes if a main route is congested via DDoS attack, and how the host generally escalates responses to DDoS.

**Every high expertise organizations should consider**:

- Implementing mod_security within its web server or as a reverse proxy that brokers requests to the main web server. Mod_security is able to fend off some common application attacks, and enables better analysis of attacks after the fact.
- Caching content using a reverse proxy like Squid or ngnix.[43] Aggressive caching is a good defense against small HTTP GET attacks and also offers protection against certain Apache-specific attacks, like slowloris.
- Tuning maximum connection settings on its web servers using load testing well in advance of an attack.

43 Squid, http://www.squid-cache.org/; ngnix, http://nginx.org/.

- Using caching plugins specific to content management systems to reduce server load in periods of legitimate high traffic and during attacks.
- Creating a static HTML version of its sites to which it can failover on its server infrastructure before failing over to a mirror site.
- Outsourcing its search to Google or another provider, given the vulnerability of search to application attacks.
- Severely restricting access to its servers by staff and ensuring that access comes from "clean" machines. Students for a Free Tibet have implemented a policy that no laptops can be used in its offices until they are re-imaged with a trusted software distribution. Each time a laptop comes back into the office from use in the field, it is wiped clean.
- Establishing a relationship with core network administrators, likely through a local technical expert who is in regular touch with one or more administrators.
- Implementing a log collection strategy, based on recommendations from core network administrators, to allow post-attack analysis.

**The broader technical community should consider**:

- Developing graceful failure modes for Drupal, WordPress, and other CMSes, which can disable database intensive activities and failover to static, cached content when triggered by an administrator or an outside monitoring system. This would likely involve collaboration between authors of these tools and funders from the human rights community willing to sponsor this custom development.
- Working with monitoring providers like Cyberspark to design and implement monitoring systems that can trigger failover modes on systems that have graceful failure modes or can trigger redirection of the site to a mirror site.
- Developing a set of best practices to collect relevant logfiles* from attacks. This might include developing a tool that could be deployed to package relevant log information for forensic analysis after an attack. (We recognize that the logfiles associated with human rights and independent media sites can be extremely sensitive documents. Design of tools for forensic analysis need to consider these security and privacy concerns.)

- Identifying a set of DDoS experts, people with close contacts to core administrators who are willing to filter and interpret requests for help from local technology experts and individual system administrators and to escalate appropriate requests to core network administrators. These might include the networking experts associated with Team Cymru and other groups dedicated to helping groups respond to and recover from DDoS attacks.
- Exploring mutual aid systems. Jonathan Zittrain has proposed that websites agree to cache and serve the content of every page they link to. Others in the working meeting proposed that DDoS-resistant hosting providers mirror each other's content.[44]
- Exploring the possibility of using Amazon's cloud architecture to mirror content on sites hosted elsewhere, perhaps through a modified CMS system that synchronizes changes to an Amazon mirror automatically, again with caveats about Amazon's terms of service.

**Funders and support organizations in the human rights and independent media field should**:

- Develop a list of key people at large core ISP and web companies who can give high-priority attention to human rights and independent media organizations under attack, like Ebele Okobi-Harris, the Director of Yahoo's Business and Human Rights program. Urge large ISPs and web companies to appoint people to these positions if they do not already exist.
- Maintain a list of inexpensive commercial webhosting providers who have agreed to host sensitive sites and not null route in the case of DDoS attack.
- Maintain a list of dedicated DDoS-resistant hosts willing to accept new clients from the human rights and independent media field.
- Understand and accept that hosting costs for vulnerable sites that choose to host their sites independently may be two orders of magnitude more expensive than conventional hosting. This raises the question of whether it's best to fund DDoS-resistant hosting for the field directly, or to fund independent media and human rights organizations at a sufficiently high level that they can afford the high costs of this hosting.
- Build relationships between organizations at risk of attack and local technology experts. This may require paying these local experts a salary to take on this work; our interviews suggest that some are employed full-time in the technology field and work with attacked sites in their free

44 Jonathan Zittrain, "What Web Sites Can Do," New York Times, January 15, 2010, accessed October 22, 2010, http://roomfordebate.blogs.nytimes.com/2010/01/15/can-google-beat-china/.

time. It's worth cautioning that the most helpful local technology experts are experienced professionals, not novices; supporting their work is likely to be expensive. It's unclear whether technology experts can work across communities. For example, it's not clear whether an Iranian could be a trusted contact for Vietnamese administrators.

- Explore ways local experts can meet and share information and best practices.
- Build relationships between local technical experts and the broader Internet security community so that, when attacks occur, experts can quickly escalate requests for assistance to appropriate network administrators. This may point to the need for a second group of experts—experienced network administrators who have open channels to core network administrators and who understand the unique needs of the human rights community.
- Consider funding a coordinator specifically to identify and work as a liaison between local technology experts and core Internet organizations that are willing to help independent media suffering from attacks. This coordinator could serve the much needed role of identifying the needs of vulnerable independent media sites through the local technology experts and of identifying what services core Internet organizations are willing and able to offer to those sites.

**The public and the policy-making community should consider a range of possible options for addressing these issues as the incidence and importance of DDOS rises**:

- Substantive legal protections might involve making certain types of DDOS attacks unlawful under national or international legal regimes. These substantive changes might also alter existing rules, such as intermediary liability protections (such as the Communications Decency Act Section 230 under United States law) to require intermediaries to observe certain speech-based protections in order to gain the benefit of the safe harbor.
- Procedural legal protections might establish steps that a hosting or cloud computing services provider might have to follow before pulling service from a given web site.
- Competitive, Market-Based Approach: Pressure from a forward-looking company, the state, or the public at large might lead companies that offer hosting services to state in advance their policies with respect to when they would or would not take down a site that they are hosting, with corresponding pressure to urge companies to honor those commitments.

- Collaborative, Market-Based Approach: An approach that establishes common principles for ensuring that web sites can rely upon web hosting providers, which might be built into existing systems such as the Global Network Initiative or through a separate mechanisms. These types of emergent principles can, over time, become enshrined into national or international rules over time, as in the case of the Sullivan Principles.
- Citizen-Based Pressure Mechanisms: The public can bring pressure upon those firms that act badly in terms of failing to state up front their principles with respect to arbitrary take-down of web sites or which make decisions that run counter to norms of free expression.

Legal and policy approaches rarely work well in the immediate aftermath of hard, highly public cases—there is a strong tendency to overreact to the specific situation at hand and not to consider a wider sphere of options. We believe a dialog involving organizations focused on free speech, commercial interests and the general public should precede specific legislative proposals.

**Dedicated hosting for the human rights community?**

Discussions at our meeting and conversations with IT experts focused on the human rights field often included consideration of the idea of establishing a dedicated DDoS-resistant hosting service for the human rights field. One version of this proposal focused on the specific solutions deployed by Prolexic, a prominent anti-DDoS provider. Other versions of the proposal were more general and simply suggested protecting multiple sites under the shelter offered by a team of administrators experienced in fending off DDoS attacks. We are cautiously supportive of the second proposal, and less supportive of the first proposal.

The advantages of a shared infrastructure are obvious. Experienced system administrators are the scarce resource in this equation. Skilled administrators who have little experience in fending off DDoS often need hours to understand and combat a novel attack. Administrators who've seen an attack before can typically fend it off within an hour. By hosting multiple sites under the aegis of experienced administrators, we can also take advantage of economies of scale—the cost of a second high-bandwidth connection as a backup to the primary Internet connection can be shared across clients, as can the costs of a farm of reverse-proxy servers.

The disadvantages are obvious as well. If several sensitive sites are hosted using the same infrastructure, an attack on one could adversely affect all. A shared architecture may be subject to more aggressive filtering, as a government attempting to block a controversial website hosted on the shared servers may block all sites hosted there. Similarly, the shared architecture may attract multiple attacks at the same time, which could have negative and synergistic effects. Finally, dependency on a single institution could create a major vulnerability for the human rights field. This risk consolidation into a single service applies as well to our general recommendation to host independent media sites on core Internet providers. But a single human rights-specific hosting service, unlike those core Internet providers, does not benefit from the economies of scale (in technical and non-technical resources) that mitigate the risk of consolidation on the core Internet services.

We know of several websites that have moved to a shared, DDoS-resistant architecture that has been offered for no cost by a firm that benefits from the ability to study and learn from the attacks the sites experience. While those sites have reported positive experiences with this webhost, we are concerned that this organization may not be able to fill the needs of the entire human rights and independent media space. In the meantime, their ability to offer high-quality services at no cost distorts the marketplace and is making it difficult for other providers to offer services at a price that allows them to recover costs.

To provide services for the human rights community at a price that organizations can afford, it is unlikely that hosting providers could offer the dynamic rerouting and scrubbing servers that a commercial firm like Prolexic offers. We question whether these services are as essential for sites that can afford brief periods of downtime; the value of Prolexic appears to be primarily to eCommerce firms that can tolerate no downtime periods. We worry about accepting a paradigm in which sites are protected from DDoS only once they demonstrate an ability to pay additional charges in the face of an attack. We also worry that the Prolexic services—while very effective against network attacks—provide little in the way of defense against application attacks, which we see as a serious threat to the sites we studied.

We recommend that human rights funders look for a solution that allows them to support more than one hosting company that provides affordable solutions to human rights and independent media groups. These companies might provide reduced rates to the target sites, but we are concerned that

providing zero-cost hosting may force otherwise willing providers not to participate. We would urge close cooperation between these hosting companies and the technical experts we've identified and would suggest a system that allowed these hosting companies to share best practices and, if possible, to mirror each other's human rights and independent media content through a mutual aid pact. We offer this recommendation knowing that it will be difficult to implement; most hosting companies consider their DDoS mitigation techniques to be highly proprietary business secrets. We hope that the identification of a set of sites with similar needs might lead to increased communication between these businesses.

Rather than founding one or more dedicated human rights hosting sites, we would prefer to see the funding community focus on building better relationships between community technology experts and existing core Internet providers. These providers will necessarily be on the cutting edge of DDoS research and will remain the best positioned to fight off massive DDoS attacks. We believe that many of the companies best positioned to assist human rights and independent media sites are willing to do so. Human rights funders might take on the critical coordination challenge, making it possible for groups of human rights and independent media sites to approach core Internet organizations through a small group of technology experts and build relationships that are easier to manage than relationships between individual organizations and large ISPs.

**Closing Note**

DDoS is inextricable from other Internet security challenges that independent media and human rights sites face. Despite the high-profile nature and seriousness of DDoS attacks, it may not be the most serious challenge these organizations face. Our survey results indicate that a large majority of independent media sites subject to DDoS attacks were also subject to filtering, intrusions, or defacements and that, even though DDoS attacks are a significant concern for independent media, filtering of sites and off-line persecution of authors and sources (sometimes resulting from online intrusions) are a higher priority. And we found in our media research, interviews, and working meeting many stories of complex interactions between different vectors of attack against independent media and human sites, including filtering, off-line persecution, intrusions, defacements, malware, and DDoS attacks. These results suggest that DDoS needs to be considered in conjunction with other vectors of attack, and that these attacks can have synergistic effects that can be difficult to mitigate individually.

The rise of DDoS as a technique for silencing human rights and independent media sites is the symptom of a larger problem: the shortage of technical talent in administering these websites and the increasing isolation of the websites from the core of the network. There is no simple technical solution to this problem. Moving to dedicated DDoS-resistant hosting leaves serious vulnerabilities open, like keylogging software targeted specifically to site administrators. We cannot consider DDoS alone, rather, we need to approach IT security for human rights and independent media sites as a whole.

# 6. Glossary

**Content management system (CMS)**

A content management system (CMS) is a web application that allows a web site editor to post web content directly through the web site itself rather than by hand editing HTML files. The past ten years have seen dramatic growth in the functionality of CMSs, to the point that there are many freely available CMSs that have evolved into highly complex publishing platforms, including not only simply content management but also sophisticated discussion, syndication, and user registration functionality out of the box. WordPress and Drupal are among the two most popular (and free) CMSs in use currently.

**HTML**

HTML (HyperText Markup Language) is the markup language used to describe the content and appearance of almost every web page in existence.

**Caching**

Caching is the practice of storing a copy of a frequently requested resource in a location from which it can be retrieved quickly. For a real life example, a college student might choose to cache a case of beer in his dorm fridge to avoid walking to the convenience store every time he wants a beer. Caching is used in many ways to speed up the serving of web pages. One caching method is to store temporary copies of pages that are expensive to generate; for example, a busy site whose home page takes five seconds to generate (perhaps because of many expensive database queries) might cache that page every five minutes, so that other than one request every five minutes to fill the cache, the front page can be returned from the cached (and therefore very easy/quick to retrieve) version in a hundredth of a second or less. Caching is very valuable for handling high traffic loads (whether through DDoS or through legitimate traffic) because the much faster request times allow the same machine to handle many more users.

**Hosting Service**

A hosting service provides a home from which a web site can serve its content. A hosting service like Amazon Web Services might simply provide access to a machine, requiring the user to install and run the applications like a web server that actually serve web content. Or a hosting service like Blogger might provide a sophisticated content management system so that a user need only post content rather than administer a web server.

**Web server**

The web works via a basic request / response mechanism -- a web browser requests a web page from a web server and the web server responds with either the content requested or a message indicating why it could not return the requested content. Every web page viewed over the Internet is returned by a web server of some sort. The term "web server" may also refer to the physical machine that runs the web server application software.

**Internet service provider (ISP)**

An Internet service provider is an organization that provides consumers or businesses access to the Internet. The Internet is often referred to as a network of networks. ISPs constitute the large majority "of networks" in that definition of the Internet. Common consumer ISPs in the use include AT&T and Comcast.

**Content distribution network**

A content distribution network distributes cached versions of content to many (up to tens of thousands) of data centers physically located around the world for the purpose of serving the cached content closer to each user. For example, a content distribution network might store a copy of the current nytimes.com website in a data center in London so that requests for nytimes.com from with England need only request nytimes.com pages from the local London caching server rather than traveling over an expensive backbone connection under the ocean. This practice of "edge caching" can drastically improve the performance of sites with significant international traffic.

**Unix**

Unix is a type of operating system that runs on many of the servers that operate the basic services of the Internet, including web, mail, and file servers. An operating system is the most fundamental level of

software that runs a computer, controlling basic operations like reading and writing files, drawing windows on the screen, and connecting to and talking over networks. Unix actually refers to a family of operating systems with a core set of very similar functionalities and architectures. Linux is currently the most popular form of Unix.

**Computer Emergency Response Team (CERT)**

The Computer Emergency Response Team is a project at Carnegie Mellon funded by the US federal government to coordinate the response of experts to Internet attacks of various sorts. CERT was originally founded in 1988 in response to the Morris Worm incident, through which a worm written to test the size of the Internet inadvertently shut down about ten percent of the hosts on the early Internet. CERT's most visible role is to publish bulletins about security vulnerabilities in major Internet server operating systems and applications.

**SYN flood**

A SYN flood is a denial of server attack that exploits a vulnerability in the process of establishing a connection between two machines over the Internet. The protocol used for most connections on the Internet is TCP/IP. TCP/IP connections require a "handshake" before exchanging any data. The handshake verifies that both machines are aware of and participating in the connection. To complete this handshake, the first machine sends an initial handshake request, the second machine sends an acknowledgement that it will open a connection, and then the first machine sends its own acknowledgement that it is ready to start the connection. This three way handshake is necessary for both sides of the connection to know that the other side has received and agreed to participate in the connection.

A SYN flood attack exploits the assumption that the other side of the handshake is acting in good faith. To execute a SYN flood, a machine just sends many initial handshake requests (called "SYN" for "SYNchronization" requests) without ever responding to the corresponding acknowledgements. This flood of unacknowledged handshake requests exhaustes the small number of available resources for open handshake requests. Until the first use of SYN attacks, all early implementations of TCP/IP had only a few resources set aside for these handshakes and so were easily overwhelmed by a SYN flood. Every modern operating system includes effective defenses against this attack, for instance by closing

handshakes that have been open for too long or by limiting the number of handshake requests open from any given other machine. The larger attack method -- of exhausting a limited pool of resources available for initiating a network request -- has been used for many other types of DoS and DDoS attacks over the years, including the SlowLoris attack that we describe in this paper.

**Internet Relay Chat (IRC)**

IRC is an early but still popular form of real time, multi-user chat over the Internet. IRC users connect with each other on IRC servers to chat both individually and as groups in IRC rooms. Automated clients on IRC are called "bots." IRC bots were the first widely used channel for controlling large "botnets" of infected computers.

**Worms**

A worm is a program that propagates itself on the Internet by installing itself on one machine, using that machine to install itself on other machines, using those machines to install itself on yet more machines, and so on. A worm is distinct from a virus in that it propagates itself from machine to machine by actively contacting and infiltrating the other machines, whereas a virus generally only infects local files and relies on the user to propagate those files to other machines.

**Trojan horse program**

A Trojan horse program is an application that secretly performs some malicious task when installed. For instance, a Trojan horse peer-to-peer program might purport to allow a user to access a peer-to-peer network to download files but might (instead or also) install a keylogger, virus, or other sort of malware on the unsuspecting user's computer.

**IRC bot**

An IRC bot is an automated client on an IRC server. IRC bots were the first widely used channel for controlling large "botnets" of infected computers.

**Botnet**

A botnet is a network of compromised computers that can be controlled in real time by a central command and control system. There have been many reports of botnets numbering in the millions of

computers, and there are many, many more botnets of tens of thousands of computers. In addition to executing DDoS attacks, botnets are used for a variety of unsavory Internet activities, including spam, credit card theft, software license theft, and advertising click fraud.

**IP address**

An IP address is the unique number used to identify a specific host on the Internet, roughly analogous to how a phone number uniquely identifies a specific phone within a phone network. An IP address is a series of four numbers from 1 to 256, for example 247.128.12.4. Every computer on the Internet is connecting through an IP address, so IP addresses are often used as a method of identifying a unique actor on the Internet, including for identifying who legitimate versus illegitimate users during a DDoS attack.

**Mbps**

"Megabits per second" is a measurement of network bandwidth (the amount of data that can be served through a network in a given period of time). A megabit equals about one million bits, where a bit is the most fundamental unit of computer data, representing either a 1 or a 0. Eight bits make up one byte, so 1 Mbps is the equivalent of about 125 KBps (Kilobytes per second, where a kilobyte is about one thousand bytes).

**Gbps**

"Megabits per second" is a measurement of network bandwidth (the amount of data that can be served through a network in a given period of time). A megabit equals about one billion bits, where a bit is the most fundamental unit of computer data, representing either a 1 or a 0. Eight bits make up one byte, so 1 Gbps is the equivalent of about 125 MBps (megabytes per second, where a megabyte is about one million bytes).

**TCP/IP**

TCP/IP is a combination of the two protocols underlying most Internet traffic. IP (Internet protocol) is the foundational protocol of the Internet and describes how hosts route traffic to one another over the Internet using IP addresses. TCP (transmission control protocol) is used in addition to IP by most Internet connections to provide reliable communication between specific applications on specific hosts.

**Domain Name System (DNS)**

All Internet traffic must be addressed to a specific IP address, but IP addresses are large numbers and so not easily human readable. The domain name system allows automatic translation from human readable names to numerical IP addresses. Web browsers and other Internet applications use DNS to allow users to access Internet services via the human readable DNS names by automatically translating DNS names to IP addresses. So a user can access the New York Times by entering 'nytimes.com' into the browser, and the browser uses DNS to translate 'nytimes.com' into the IP address '199.239.136.200' that is necessary for the browser to create a connection to the New York Times server.

**Ping**

A ping is a simple, minimal network request that merely establishes that a given machine is connected to the network and responding to requests.

**HTTP**

The HyperText Transfer Protocol is the language and process that web browsers and web servers used to talk to one another to exchange requests and responses for web pages. For example, an HTTP request and response for a very simple page might look like:

Request:

GET /hello.html HTTP/1.0

Response:

HTTP/1.0 200 OK

<body><html>Hello</html></body>

**Static HTML**

A static HTML page is a web page that is served directly from a file on disk. Most sophisticated websites do not use static HTML pages but rather use dynamic pages that are generated by a server application for each request, often by querying a database. Dynamic pages allow much great functionality but are almost always much more expensive to serve that simple static HTML pages (and so reduce the number of requests that a server can handle at one time).

**Routing**

The Internet works like a giant game of hot potato rather than like a giant switchboard. Instead of being directly connected to one another through anything like a switchboard, two hosts talking to one another over the Internet pass their data through a series of intermediary machines (called "routers") which are each responsible for passing the data to some other machine closer to the ultimate destination. Internet routing is the process of determining the series of routers that will pass data along to one another in route between any two Internet hosts.

**Null route**

Internet routes are established by advertising. The network hosting any given host that wants to participate in the Internet sends an advertisement to the rest of the Internet announcing where the host can be found. A null route is a route advertisement that tells either the whole Internet or some specific subset of the Internet that there is no valid route to the given host. A global null route is often used as a last resort during a DDoS attack to effectively remove a target host from the Internet (by advertising to the whole Internet that there is no valid route to the target machine) in order to protect the other hosts on the network from the attack. Sophisticated network operators can also send null routes only to specific networks, preventing just those networks from reaching a target host, which can be useful if a DDoS attack is coming from a small number of destination networks.

**Malware**

Malware ("malicious software") refers to any of a number of types of software that access a computer without the owner's knowledge or consent. Malware is an umbrella term that includes viruses, worms, and trojan software, among other forms.

**Rate limiting**

Rate limiting is the practice of limiting the resources available to a specific single machine or specific group of machines. For example, a web server might use rate limiting to allow any given host to make only up to 50 requests per minute, under the theory that any host making more than 50 requests per minute is probably executing a DDoS attack.

**Blacklists**

A blacklist is a list of hosts to be banned from participating in a given activity. Blacklists are most commonly used on the Internet to identify hosts suspected of sending or facilitating the sending of spam, but they can also be used to identify hosts that are executing DDoS attacks. The maintenance of blacklists is very tricky, requiring an impossible balance between false negatives and false positives.

**Proxies**

A proxy is a host that acts as a middleman between two other hosts. Web proxies are used to allow users to connect to web sites anonymously or to access otherwise blocked sites. For example, the great firewall of China blocks access to falundafa.org from within China. But a Chinese user can use a proxy to access falundafa.org by first contacting the hypothetical superproxy.com and asking superproxy.com to request falundafa.org on behalf of the user and to pass the contents back to the original user. As long as superproxy.com is located outside of China, the great firewall can only see the connection to superproxy.com, not to falundafa.org. And so the user can access the otherwise blocked content through the proxy (though not if the proxy itself is blocked as well).

**ModSecurity**

ModSecurity is a firewall application that sits in front web servers, preventing known bad requests (for instance requests that look like specific types of DDoS attacks) from reaching a web server. It is the most popular firewall for mitigation of application-based DDoS attacks because it has an extensive set of filters that are updated daily to protect against new types of application attacks.

**Logfiles**

A logfile contains the ongoing output of an application or system. Operating systems generally and web servers specifically all generate a range of different logfiles that allow a system administrator to monitor what is happening on the system both now and for as long in the past as the logfile are available. For

instance, a web server logfile usually includes an entry for every request to the web server, including information about which IP address requested the web page, which browser was used for the request, which specific page was requested, whether the web page was successfully returned to the user, and even which web page hosted the link that the user clicked on to get to the requested web page. Logfiles are usually critical in diagnosing a DDoS attack because they provide the basic operational data necessary to diagnose the source and nature of an attack.