# 8 Control and Resistance

## Attacks on Burmese Opposition Media

**Nart Villeneuve and Masashi Crete-Nishihata**

Burma is consistently identified by human rights organizations as one of the world's most repressive regimes. Human rights violations occur with regularity, especially in connection with the country's long-standing armed conflict. The ruling military junta, the State Peace and Development Council (SPDC), is best known for its political prisoners and its systematic denial of universal human rights such as freedom of expression.[1] The government's efforts to silence dissent pervade cyberspace and its system of Internet control is one of the most restrictive in Asia.

Despite the heavy hand that the regime wields over cyberspace, information communication technologies (ICTs) have provided Burmese opposition groups with the means to broadcast their message to the world and challenge the government. The ongoing battle between these two sides makes Burma a stark example of contested Asian cyberspace. The role of ICTs in this struggle can be framed by contrasting theories that view them either as "liberation technologies" that can empower grassroots political movements[2] or as tools that authoritarian governments can use to suppress these very same mobilizations.[3]

This contestation is dramatically illustrated by the series of protests that erupted across the country in 2007—in a movement popularly known as the "Saffron Revolution." During these protests, Burmese activists managed to bring the uprising to the world's attention by making images and videos of the demonstrations and subsequent government crackdown available on the Internet. Realizing the potential political impact of these images, the government severed Internet connectivity in the country for nearly two weeks.[4] This drastic action demonstrated that the regime had learned a significant lesson: although Burma's technical filtering system was successful in censoring access to information coming into the country from opposition media Web sites, it was unable to prevent information from flowing out of the country to these sites for global consumption.

As the one-year anniversary of the protests neared, the Web sites of the three main Burmese independent media organizations were attacked and effectively silenced. The Democratic Voice of Burma[5] and The Irrawaddy[6] were rendered inaccessible following

a distributed denial of service (DDoS) attack. While these attacks were under way, Mizzima News[7] was also compromised and its Web site was defaced.[8] Periodic attacks on Burmese opposition media sites continued through 2009 and 2010.[9] In late September 2010, around the third anniversary of the Saffron Revolution, Burmese opposition media were once again silenced by a series of DDoS attacks and Web site defacements.[10]

The timing of these attacks and the content of the messages in the Web site defacements indicate a political connection, and although the identity and capabilities of the attackers—as well as any relationships they may have with the government—remain unknown, it is widely believed that the government played a role in the attacks. This belief prevails because the Burmese government has consistently demonstrated an interest in controlling and censoring the communications environment in the country.

This chapter explores the complexities of information control and resistance in Burma based on an investigation conducted by the Information Warfare Monitor (IWM)[11] on the attacks launched against the Mizzima News Web site in 2008. Through technical evidence obtained from our investigation and field research conducted in Burma, we were able to uncover and analyze the characteristics and capabilities of the suspected attackers. We found that these attacks are consistent with government and military interest in information control and censorship of the Internet as well as a pattern of ongoing attacks against Burmese political opposition. However, they cannot be conclusively attributed to the military or government of Burma. Our investigation found that the attack on the Mizzima News Web site appeared to have been a result of a combination of two factors: political motivation and the availability of a target of opportunity. The attackers are certainly unfavorable toward the Burmese opposition media, but cannot be simplistically characterized as "progovernment" either. Their primary motivation appears to be nationalism and a belief that the opposition media demean the public image of their country. The timing of the attacks provided a strategic utility that would normally have been beyond the attackers' means. While Burma maintains a robust Internet censorship system that prevents its citizens from accessing alternative news media, these attacks effectively prevented global access to opposition media sites during a sensitive period.

We proceed by describing the spectrum of information controls in Burma that includes pervasive Internet filtering, repressive legal frameworks, and recurring cyber attacks. We then provide a detailed technical and contextual analysis of the Mizzima News defacement attacks and highlight the difficulty of determining the actors involved and motivations behind such attacks as well as questions surrounding state attribution. Finally, we situate the case study in the wider context of information controls in Burma and argue that gaining an understanding of threats to freedom of expression in cyberspace requires a holistic analysis that accounts for the unpredictable and contested nature of the domain.

## Information Controls in Burma

The SPDC maintains tight authoritarian rule over all forms of media and communications in the country. All local television, radio stations, and daily newspapers are owned and controlled by the state.[12] Within the country there are 100 private publications, which are also heavily restrained and censored by state authorities.[13] The Printers and Publishers Registration Act, implemented in 1965, prohibits printed publications from being critical of the government and requires all printers and publishers to register with the government and submit materials for review.[14] The Video and Television Law applies similar regulations to television and film media.[15] Together, these restrictions have stifled what was once a vibrant free press.[16]

Amid this repression of traditional media the Internet has become an important source of information on Burma. Beginning in the early 1990s, Burmese expatriates and journalists living in exile set up news groups, mailing lists, and Web sites to disseminate information on the human rights and political situation in the country.[17] Today, the most popular independent Burmese Web sites operate outside of the country, with Mizzima News based in India, The Irrawaddy in Thailand, and the Democratic Voice of Burma in Norway. These Web sites receive reports from citizens within the country and provide an alternative to state-controlled media that often includes content critical of the regime. While these media organizations have become important outlets for international audiences to receive information on Burma, they are heavily censored within the country.

The regime aggressively denies, shapes, and controls online information in Burma. Internet penetration is very limited with an estimated online population of less than 1 percent.[18] OpenNet Initiative (ONI) testing has consistently found that the only two Internet service providers (ISPs), Yatanarpon Teleport (or Myanmar Teleport, formerly known as Bagan Cybertech) and Myanmar Posts and Telecom, extensively filter Internet content by targeting circumvention technologies, foreign e-mail providers, communications tools such as Skype and Gtalk, material related to human rights and the Burmese democratic movement, and independent news Web sites.[19] The Web sites of Mizzima News, the Democratic Voice of Burma, and The Irrawaddy have been filtered by the country's ISPs for years. Filtering is achieved through technology linked to U.S. companies Fortinet and Bluecoat despite an embargo that places limits on exports to Burma.[20] These technical restrictions are paired with hard legal enforcement, and bloggers and journalists in the country face a constant threat of prosecution for publishing dissenting material. The Reporters Without Borders's Press Freedom Index of 2010 ranked Burma 174 out of 178 countries, and in 2009 the Committee to Protect Journalists deemed Burma the worst country in the world to be a blogger.[21] These repressive controls create a climate of self-censorship in which citizens avoid publishing and seeking out banned content.

The Saffron Revolution was the scene of the most dramatic example of Internet controls and resistance in Burma. A small number of peaceful protests organized by Burmese social and political activists began on August 17, 2007, in reaction to a 500 percent increase in the retail price of fuel.[22] These initial demonstrations were quickly suppressed by the government, but peaceful protests spread throughout the country under the leadership of Buddhist monks. By mid-September the number of participants had swelled to 100,000, including 10,000 Buddhist monks.[23] The government reacted with a severe crackdown from September 26 to 29. During this time, a number of serious human rights violations occurred, including killings, mass beatings, and arrests.[24] Burmese independent media outlets, including Mizzima News, The Irrawaddy, and the Democratic Voice of Burma, along with numerous bloggers and citizen journalists, played a crucial role in disseminating reports of the crackdown to the international community. Despite the heavy restrictions enforced by the regime, activists and citizen journalists managed to upload images and videos of the protests and crackdown to the Internet. The dissemination of these images to the world did not go unnoticed by the SPDC, and on September 29, 2007, it employed a blunter tactic of information denial than its standard filtering practices.

Through its comprehensive control over Burma's international Internet gateways, the SPDC implemented a complete shutdown of Internet connectivity in the country that lasted for approximately two weeks.[25] Only two other states have taken such drastic measures. In February 2005, Nepal closed all international Internet connections following a declaration of martial law by the king.[26] On January 26, 2011, the Egyptian government ordered national ISPs to shut down in reaction to major protests in the country.[27] Severing national Internet connectivity in reaction to sensitive political events is an extreme example of *just-in-time-blocking*—a phenomenon in which access to information is denied exactly at times when the information may have the greatest potential impact, such as elections, protests, or anniversaries of social unrest.[28] The crude but effective means of information denial implemented by the SPDC shows the extent the junta is willing to go to restrict bidirectional flows of information in Burma. It also serves as an example of Internet control beyond filtering that is focused on denying information to international users rather than just blocking domestic access.

Silencing voices critical of the regime during key events is an ongoing occurrence in Burma, and there exists a long history of cyber attacks against Burmese activists and independent media organizations, which include a range of attack vectors from malware to DDoS attacks. In 2000, for instance, Burmese political activists received numerous e-mail messages containing viruses that many believe were part of an organized campaign perpetrated by state agents.[29] More recently, Burmese independent news organizations have confronted waves of attacks on their Web sites during the anniversaries of key political events in the country (table 8.1). As coverage of the one-year anniversary of the 2007 crackdown was emerging, the servers of The Irrawaddy

**Table 8.1**

**TIMELINE OF MAJOR POLITICAL EVENTS AND RECENT CYBER ATTACKS AGAINST BURMESE OPPOSITION WEB SITES**

| Date | Event |
|---|---|
| August 8, 1988 | Massive protests led by student activists in Burma known as the 8888 uprising |
| August–October 2007 | Series of antigovernment protests led by Buddhist monks in Burma dubbed the "Saffron Revolution" |
| September 27, 2007 | Military junta shutdown of access to the Internet within Burma |
| October 13, 2007 | Internet access in Burma reconnected |
| September 2007 | The Irrawaddy Web site infected with Trojan |
| July 2008 | DDoS attack on Mizzima News Web site |
| July 2008 | DDoS attack on Democratic Voice of Burma Web site |
| September 17, 2008 | DDoS attack on Democratic Voice of Burma Web site |
| September 17, 2008 | DDoS attack on New Era Journal Web site |
| September 17, 2008 | DDoS attack on The Irrawaddy Web site |
| October 2008 | Defacement attack on Mizzima News Web site |
| August 8, 2009 | DDoS attack on Mizzima News Web site |
| September 2010 | DDoS attack on Mizzima News Web site |
| September 2010 | DDoS attack on Democratic Voice of Burma Web site |
| September 2010 | DDoS attack on The Irrawaddy Web site |

*Sources:* "Burmese Exiles' Leading Media Websites under Attack 20 July 2008," Burma New International, July 30, 2008, http://www.bnionline.net/media-alert/4590-burmese-exiles-leading-media-websites-under-attack-30-july-2008.html; "Press Release: DVB Web Site Hit by DDoS Attack," Democratic Voice of Burma, July 25, 2008, http://www.dvb.no/uncategorized/press-release-dvb-web-site-hit-by-ddos-attack/1256; "Websites of Three Burmese News Agencies in Exile under Attack," All Burma IT Students' Union, September 17, 2008, http://www.abitsu.org/?p=2502; Aung Zaw, "The Burmese Regime's Cyber Offensive," The Irrawaddy, September 18, 2008, http://www.irrawaddy.org/opinion_story.php?art_id=14280; Muchancho Enfermo, "Burma: Sri Lanka–Based Myanmar Media Website Attacked Again," Ashin Mettacara, March 17, 2009, http://www.ashinmettacara.org/2009/03/burma-sri-lanka-based-myanmar-media.html; http://www.ashinmettacara.org/2009/01/burma-myanmar-sri-lanka-based-burmese.html; "Fresh Attack on Mizzima Website," Mizzima News, August 8, 2009, http://www.mizzima.com/news/inside-burma/2599-fresh-attack-on-mizzima-website.html; Alex Ellgee, "Another Opposition Website Shut Down by Hackers," The Irrawaddy, June 19, 2010, http://www.irrawaddy.org/article.php?art_id=18759; Committee to Protect Journalists, "Burma's Exile Media Hit by Cyber-attacks," http://cpj.org/2010/09/burmas-exile-media-hit-by-cyber-attacks.php.

and the Democratic Voice of Burma were hit with DDoS attacks that overloaded the Web sites and rendered them inaccessible.[30] Similar attacks have occurred on subsequent anniversaries of the Saffron Revolution and the 1988 student protest known as the "8888 Uprising." The timing and coordination of these attacks suggest that the motivation behind them may be to censor the Web sites from commemorating the protests and possibly mobilizing new political actions.

It is unclear who was behind the attacks, although it is widely believed that the military or government played a role, since the regime maintains a strong interest in information control and actively seeks to silence opposition voices.[31] Opposition groups have come under persistent cyber attacks over the years and many believe such attacks are part of a wider campaign of state-sanctioned harassment.[32] However, positively determining attribution, motivations, and the extent of the attackers' abilities is a difficult task.

### Mizzima News Defacement Attack

One example of the persistent attacks on Burmese independent media is the compromise and defacement of the Mizzima News Web site (http://www.mizzima.com) on October 1, 2008.[33] The original content of the site was replaced with a message from the attackers (figure 8.1):

Dear MIZZIMA Reader. . . . Listen please, Why Hack This Website? . . . Because We are Independence Hackers from Burma. We Born for Hack Those Fucking Media Website, Which are Ever Talk about Only Worse News For Our Country. We Very Sorry for Web Admin, You Need To More


**Figure 8.1**
A screen capture of the defacement of Mizzima.com.

Secure Your Website. New We Warn to All Media Webadmins That is "Prepare to more Secure your Work."

This case demonstrates how attackers mask their identity, thus making it difficult to determine those responsible for the attacks. The attackers who defaced Mizzima News—which is blocked by ISPs in Burma—used censorship-circumvention software to perpetrate the attack hosted on servers that had IP addresses allocated to the United States, France, and Germany in order to make it appear as if the attacks originated in those countries.[34] Mizzima News reported on October 1, 2008, that the attacker's IP address originated in the United States. On October 10, 2008, Mizzima News reported: "While it is still difficult to technically trace who is behind the hacking attempts, Mizzima's technical staff said the main attempt is found to have originated from Russia with cooperation from other hackers in Germany, France and India."[35] The incident highlights the difficulty in tracing the geographic location of the attacks, let alone determining the identity and intent of the attackers. In the absence of sufficient evidence to attribute attacks, analysts often turn to the political context to fill in the gaps. In view of the persistent efforts by the government and military to crack down on political dissent, it is clear that they have an interest in silencing critics such as Mizzima News. However, a careful examination of the technical evidence, as well as an exploration of alternative explanations, is critical to understand the characteristics of the attackers.

### Investigating the Attack

Following the October 1, 2008, defacement of the Mizzima News Web site, the IWM offered to assist Mizzima News with an investigation of the attack, and the organization provided us with access to their Web server logs and sample copies of c99shell (a backdoor program that provides attackers with remote access to a victim's machine) that were found on the compromised Mizzima News Web server.[36] We processed these log files and isolated the IP addresses that connected to and issued commands on the c99shell backdoor program. We removed the IP addresses of the legitimate administrators who had later connected to test c99shell. We were left with a set of IP addresses that we identified as belonging to a censorship-circumvention proxy service. While some variation existed in the IP addresses, there were consistent browser user-agents[37] that (1) connected from the circumvention proxy service IP addresses and (2) connected to and executed commands on the c99shell backdoor. We collected and analyzed all log entries in which the identified IP addresses connected to and issued commands on instances of the c99shell backdoor.

We identified five attackers. The two primary attackers appeared to be working in tandem with one another. Although we believe that the remaining three attackers are

distinct individuals, there is the possibility that they are the two primary attackers using different browsers (and/or operating systems).

The log files indicate that in the days before and after the defacement, the attackers browsed the Mizzima News Web site from sites with Burma-related content such as http://komoethee.blogspot.com (September 10, 2008) and http://baganland.blogspot.com (September 30, 2008). They connected to Mizzima News from articles that referred to the ongoing DDoS attacks against The Irrawaddy and the Democratic Voice of Burma and were thus well aware of the scope of the attacks targeting opposition news media.[38] Just six hours before the defacement, the attackers visited Mizzima News from an article that detailed Burma's cyberwarfare capabilities and that claimed the attacks "may have been conducted by Myanmar military officers trained or undergoing training in Russia and China."[39] The attackers then accessed a variety of articles on the Mizzima News Web site. It is likely that at this stage they determined that the Mizzima News Web site was based on the Joomla! Customer Management System (CMS).[40]

Beginning on September 19, 2008, the attackers attempted to exploit a number of known vulnerabilities in the Joomla! CMS that the Mizzima News Web site was running on. After a series of unsuccessful attempts, Attacker 2 finally managed to exploit a password reset vulnerability in Joomla! and immediately logged in as the administrator. This "remote admin password change" exploit is very simple and can be conducted through any Web browser. The exploit was publicly available by August 12, 2008, about two months before it was used to compromise Mizzima News.[41]

After acquiring administrator privileges by exploiting the password reset vulnerability, Attacker 2 shared administrator access with Attacker 1. Both attackers attempted to download c99shell onto the compromised server, and within 20 minutes both attackers had set up the Trojan tool and began exploring the directories of the Mizzima News Web servers. Eventually, the attackers shared access with a third attacker and gained access to several My SQL databases. They deleted parts of the databases, and by 4:56 PM on September 30, 2008, they had defaced the Mizzima News Web site.

The attackers returned several times and installed more instances of c99shell as well as pBot, an Internet Relay Chat (IRC) bot with both Trojan and DDoS capabilities, while Mizzima's administrators attempted to delete the malicious files. The attackers also defaced the Mizzima News Web site repeatedly after Mizzima administrators tried to restore the original content. The attackers were finally locked out on October 4, 2008. They attempted—unsuccessfully—to return on October 5 and 6.

We approached the censorship-circumvention software provider that the attackers used with convincing evidence of the attacks and the use of their tool and asked if they could confirm that the attackers used the IPs we traced back to their services. The software provider confirmed that Attacker 1 and Attacker 2 logged in to the circumvention service from IP addresses assigned to Burma, which is interesting because the Mizzima News Web site is filtered by Burmese ISPs and inaccessible to Internet

users in Burma. Therefore, the attackers had to bypass this ISP-level filtering in order to attack the Web site. They also probably believed that using the service would shield their identities.

To summarize, the evidence suggests there were two primary attackers working in collaboration with one another other to exploit and "Trojan" the Mizzima News Web server. These attackers appear to have shared links to the Trojans that they had installed with additional attackers. In total, there appear to have been five attackers working together to maintain control over the Mizzima News Web server. The attackers deleted portions of Mizzima's database and defaced the Web site repeatedly. Over the course of seven days, they continued to attack Mizzima's server while the Mizzima administrators worked to delete the different backdoors that the attackers frequently installed. By the fifth day they were shut out of the system, although they continued to check for access on the sixth and seventh days but were denied. We further confirmed that the attacks originated from Burma and used the proxy service to bypass national-level filtering of Mizzima News.

### Investigating the Attackers

We investigated the identities of the attackers by analyzing the versions of the backdoor program c99shell and the IRC bot pBot they used, the specific attackers who downloaded these files, and the location they retrieved the programs from. What follows is an analysis of the data trail we followed by analyzing and linking the information contained in these files.

The c99shell backdoor program is a widely available Trojan backdoor written in the PHP programming language.[42] The versions of c99shell that the attackers tried to download to the Mizzima News Web server were slightly modified to include text in the interface reading, "Hacked by doscoder—oGc Security Team—#cyberw0rm @ oGc" (figure 8.2).

Based on this information, we could infer that the tool had been modified by "doscoder"—who is a member of the "oGc Security Team" and IRC channel "#cyberw0rm" on an IRC network called "oGc." However, these data points do not necessarily


**Figure 8.2**
Screen shot of the modified interface for the c99shell backdoor program.

attribute the attacks to these aliases, since it is possible the attackers could be using someone else's tools.

Where the attackers downloaded the Trojan programs they used in the attack revealed further evidence. The attackers downloaded c99shell and pBot from two separate locations. The version of c99shell at both locations was identical. The pBot was functionally identical, but the connection information in the pBot configuration file was different. Attacker 1 and Attacker 3 both made attempts to download the same instance of c99shell from a compromised server. However, only Attacker 2 was able to successfully download c99shell from the Web site 0verkill.co.cc and upload it to the Mizzima Web server.

Attacker 2 made attempts to download an instance of c99shell as well as another file, an instance of pBot, from 0verkill.co.cc. 0verkill.co.cc was registered to "Charlie Root" with the e-mail address ir00t3r@gmail.com. It was registered from an IP address in Burma.[43]

The pBot that Attacker 1 attempted to download from 0verkill.co.cc was configured to connect to an IRC server, overkill.myanmarchat.org (with the prefix "vesali") to IRC channel "#jail." The pBot that Attackers 2 and 3 attempted to download from a compromised server, videovideo.it, was configured to connect to an IRC server at 64.18.129.9 with the prefix "soul" (figure 8.3).

To collect further information we attempted to connect to 64.18.129.9, but were unable to obtain access. We were able to briefly connect to the overkill.myanmarchat.org IRC server until we were kicked out and banned. The "overkill" subdomain was subsequently removed and failed to resolve. When connecting to the overkill.myanmarchat.org IRC server, the network names "irc.doscoder.org" and "irc.vesali.net" were displayed. Only one user was seen on the server:

[xer0] (~xero@overkill.name): xero
[xer0] @#jail
[xer0] irc.doscoder.org:Over Kill Over The WorlD
[xer0] is a Network Administrator
[xer0] is available for help.

The IRC server information indicated that there was some still-unknown relationship between "doscoder" and "0verkill." It is important to recall that modifications were made to c99shell by doscoder—a member of the "oGc Security Team" and the "#cyber-w0rm" channel on the oGc IRC network. Now, "doscoder" emerged as the host name for the overkill.myanmarchat.org IRC server. A Web search turned up a relationship between the file name and location path of the c99shell at now defunct locations on doscoder.t35.com. In addition, much of the code in the defacement page posted on the Mizzima News Web servers was similar to the code in another unrelated defacement by doscoder. However, no further information was found concerning the doscoder alias.

```
<?

set_time_limit(0);
error_reporting(0);
echo "ok!";
ini_set("max_execution_time",0);
class pBot
{
var $config = array("server"=>"overkill.myanmarchat.org",
                    "port"=>"443",
                    "pass"=>" ",
                    "prefix"=>"[]vesali[]",
                    "maxrand"=>"5",
                    "chan"=>"#jail",
                    "chan2"=>" ",
                    "key"=>" ",
                    "modes"=>"+p",
                    "password"=>"overkill",
                    "trigger"=>".",
                    "hostauth"=>"overkill.name"
                    );
var $users = array();
function start()
```

**Figure 8.3**
The configuration of Attacker 2's pBot.

Although the overkill.myanmarchat.org IRC server disappeared soon after we connected to it, we discovered another IRC server hosted on "irc.myanmarchat.org." This server is one of the IRC servers for the Olive Green Complex (oGc), an IRC network founded in 2004 by Burmese students studying at the Moscow Aviation Institute (MAI) in Russia, which provides advanced training in computer engineering and informatics[44] and is currently subject to a U.S. embargo for its alleged role in supplying nuclear weapons technology to Iran.[45] According to Aung Lin Htut, a former deputy ambassador to Washington, the attacks against the Burmese opposition Web sites were conducted by "Russian technicians" based in "Burma's West Point cyber city"—a reference to Myanmar's Academy of Defense Services in Pyin Oo Lwin, Mandalay Division, Myanmar.[46] Aung Lin Htut further stated that Burmese military officers are trained at the MAI.[47]

The oGc is described by members as being an IRC group for those interested in information technology and computer engineering.

oGc is a non-profit organization and it intends for all people who interest in Information Technology. We all are students and all of members are interesting in learning IT. The main of oGc Network is to give outs free psyBNC account, email and others free services to people in learning more about unix and linux features. We [would] be glad if you would find any useful information on oGc and trust that we will not have disappointed you with the fruits of our efforts. Finally, the oGc was born and we [would] like to thank to all people who [participated] and helped us get oGc off the ground. We dedicated to use Myanmar IRC gateway. We started it at November 2004.[48]

The students also operate an IRC server at irc.olivegreen.org that has the same IP address as irc.myanmarchat.org. The oGc IRC network is accessible by several domain names. According to registration information, some of these domains were registered by students at the MAI. The server is frequented by students studying in Burma, Russia, China, and Singapore. There is also a server, irc.mmustudent.org, for students of the Myanmar Maritime University, which has a computer science department.[49] The earliest domain name registrations indicated that oGc originated in Russia. However, the most recent activity on the server was traced to Burma.

In our observations of the oGc IRC network we found the group's members and frequent chatters were friendly and generally interested in information technology. There was the occasional discussion about an exploit or Web defacement, but that was not the focal point of the conversation. The oGc IRC network appears to be a legitimate IRC network as opposed to a specifically "hacker"-related network.

As our investigation progressed we provided the circumvention software provider with the aliases of several suspects from the oGc IRC network and asked to confirm if they had them in their system. We found that three of these nicknames were among some 20 account names on the circumvention software service utilized from the same installation as one of the attackers. Based on these correlations, we had substantial evidence that members of the oGc may have been involved in the attack.

On the oGc IRC network we found an operator identified as the administrator of oGc who, through our analysis, was revealed to be using multiple aliases associated with the alias found in the configuration of the pBot Trojan used in the attacks against Mizzima, as well as related accounts on the circumvention software service. We initiated IRC chats[50] with the oGc administrator and other oGc members and asked why they thought Mizzima News was defaced. Their general response was that the opposition highlights only the negative aspects of Burma and generally produces "nonsense." The oGc administrator suggested that there were "rules of every country" and implied that Mizzima News had broken those rules, noting "u should know, what kind of articles are written there." In general, the oGc administrator and other members of the group did not appear to be "progovernment" and acknowledged that issues of government corruption were legitimate. However, they were very proud of their

country and nationalistic, and they did not approve of the foreign media's portrayal of Burma. Although the oGc administrator denied being responsible for the defacement of Mizzima, he was often vague and implied that it may have been him. He was also aware of "doscoder" and "0verkill" but refused to discuss them.

Based on our correlative evidence, we directly accused the oGc administrator of defacing Mizzima in our IRC chat by linking his various aliases to the circumvention software used in the Mizzima attacks. The oGc administrator never directly accepted responsibility, but he used tongue-in-cheek responses that alluded to his involvement. For instance, although he said his involvement was "impossible," he added emoticon smiley faces to his replies. He also suggested that he was being framed and that a well-known hacker, Lynn Htun, was the person responsible for the attacks.

Lynn Htun, better known by his handle "Fluffi Bunni," defaced high-profile information-security-industry Web sites such as the SANS Institute with humorous, taunting text and images between 2000 and 2003. Lynn Htun was arrested in London on April 29, 2003, while attending the InfoSecurity computer security conference, for his failure to appear in court on (unrelated) forgery charges. He formerly worked in the U.K. offices of Siemens Communications.[51]

In response to a post on Myanmar IT Pros (http://myanmaritpros.com)—a popular forum for Burmese information technology professionals—Lynn Htun posted the following analysis of the oGc:

> Their server is called irc.olivegreen.org . . . they set up irc servers and rent them out to botnet owners, in return, they are allowed to use the botnet to ddos once a month or so. They didn't hacked the drones for the botnet, they are simply providing the server(s) for harvesting the botnet. So in other words, there's no real skills there. . . . You should contact their service provider and tell them to shutdown the botnet hub that is running on the following VPS. . . . All the above IPs are bound to a FreeBSD box running on a VPS. You wont find the bots on their server when you join because they are all in a secret channel with umode flags set to hide them from normal users.[52]

Lynn Htun's accusation that the oGc occasionally uses a botnet constructed by others for DDoS attacks as a form of payment infuriated the oGc administrator, who denied the claims vigorously when we mentioned them during our IRC chats with him. During one chat a strange coincidence occurred when an IRC user with the nickname "lynn" appeared in the oGc IRC channel, purporting to be Lynn Htun. The two times that "lynn" connected to the server, the following information was displayed:

```
lynn (~xero@bagan-3634EE84.childminder.co.uk)
Lynn (humm@bagan-888BA9F1.uk2net.com) has joined #Bagan
[Lynn] (humm@bagan-888BA9F1.uk2net.com): xero
```

Recall that the information seen when a user enters the overkill.myanmarchat.org server was "~xero overkill.name irc.doscoder.org xer0 H*:1 xero." It may be a coincidence but the "xero" is present in both. It is difficult to assess whether lynn was in fact Lynn Htun. In the chat, "lynn" appeared to backpeddle from the post made on Myanmaritpros.com, raising questions about whether the user was actually Lynn Htun.

Lynn Htun's profile on Myanmaritpros.com indicates that he works for Myanmar Online. The IRC group for Myanmar Online has an apparent rivalry with oGc, and if anyone creates a channel with a name associated with oGc, such as "ogc," he or she is kicked from the channel and given the following message: "You have been kicked from the chat room by ChanServ with the reason 'lamer channel' and cannot send further messages without rejoining."

In some of his posts on Myanmaritpros.com, Lynn Htun expresses views that appear unfavorable toward the Burmese political opposition but do not necessarily reflect a "progovernment" position either. His perspective appears to be nuanced and stems from what he refers to as the "excessive politicization of our daily lives"[53] as well as the "collateral damage" that emerges as a result of tying economics to political reform through the use of sanctions:

> Unfortunately our beloved politicians have [intertwined] the development of the country with political process. As such, as long as there are political deadlocks, our country's developments will be [hampered] and our IT industry will be stuck in a limbo forever more. I would like to show your posting to those who claim that sanctions are working and that they are essential for political transition. Insisting that economic and social development goes hand in hand with political progress is like saying prostrate cancer can be cure[d] with cough medicine. Yet, knowingly many insist that enforcing sanctions on Myanmar is a good thing because it serve[s] the greater cause and of course all the negative side effects are acceptable collateral damage.[54]

General discontent with opposition media is reflected in a thread on Myanmaritpros.com in which Lynn Htun and others expressed frustration over the coverage of a competition to develop a search engine sponsored by the Myanmar Computer Professional Association. After The Irrawaddy posted an article suggesting that the competition may have been "designed by the Burmese military junta in order to increase its Internet restriction technology and ability to control Web sites and blogs,"[55] Lynn Htun called them "democrazies" and suggested that The Irrawaddy was opposed to improving the state of information technologies in Burma: "I don't think that is on the agenda of the 'democrazies,' politicians and exiled media outlets. . . . Looks like they already cooked up some nasty accusations:-(."[56] This incident appears to illustrate a tension in the Burmese IT community that suggests how viewing the sociopolitical climate and its relation to technology in the country in black-and-white terms may overly simplify the situation.

### Burmese Hacker Community

As part of our investigation, an IWM researcher traveled to Burma to gain insight into the local hacker community and assess their motivations. The hacker culture in Burma, as in many places around the world, appears to be oriented toward touting one's skills in order to improve business opportunities. One source within the information technology community indicated that the motives behind the attacks on Mizzima News may very well not have been political. Instead, they may have been motivated by a desire to demonstrate the hackers' skills online for personal gratification as well as to advance personal economic interests. He explained that by drawing attention to their expertise through such attacks, hackers may have hoped to attract demands for "protection" from network administrators. Essentially, they could have been creating a demand and, in turn, supplying the protection.

Hackers such as Fluffi Bunni have become respected members of Burma's information technology community and have commercialized their skills. While they do not support the political opposition, they are not necessarily hostile to it. Rather, they seem to believe that apolitical policies are better suited toward advancing both the economy and the ICT sector within Burma. As a result, they are critical of expatriate Burmese media that oppose the country's government and military.

In contrast, other sources within Burma indicated that political motivations were behind the attacks. They said that since very few people within Burma actually have an Internet connection, these attacks are likely the work of Russian-trained hackers. This view aligns with the charges made by Burmese opposition groups.

Ultimately, none of our sources could clarify whether those behind the attacks acted independently or alongside government interests. What we found in our field investigation is that there is a lively hacker community in Burma, but information regarding their relationship with the government and military is extremely scarce, and the information that is available is inconclusive.

The information obtained during the field investigation also provides context to the ongoing attacks against the Burmese opposition media. As we mentioned, the opposition Web sites are already blocked and inaccessible to Internet users in Burma. According to our sources in the country, the political opposition in Burma actually avoids using the Internet because they perceive communications over the Internet as being insecure, and using the Internet, as opposed to other forms of communication, makes them more vulnerable to government interception. In addition, computer literacy levels are very low, and few of those who use the Internet are familiar with security practices such as encryption. As a result, the opposition within Burma uses the Internet primarily for the dissemination of information through anonymous blogs and news reporting. The importance of sites like Mizzima News is not necessarily that they provide information to people within Burma, but rather that they provide

information about Burma to a global audience. This observation helps to explain why opposition media sites are routinely attacked despite the fact that they are inaccessible to Internet users within Burma.

### Assessing Threat and Attribution

To assess the capabilities of computer network attackers, John Arquilla has defined three useful categories that indicate the skill and resources required to carry out various levels of attacks:

*Simple-Unstructured* The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.
*Advanced-Structured* The capability to conduct more sophisticated attacks against multiple systems or networks and possibly to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.
*Complex-Coordinated* The capability for coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organizational learning capability.[57]

Analyzing the attacks within this framework grounds political context in technical data in a way that provides a clearer picture of the identity and intent of the attackers.

Our analysis suggests that the attackers have significant knowledge of information technology, which enables them to launch attacks by leveraging basic, publicly available exploits and software tools. They may also have access to botnets capable of DDoS attacks, but they do not create or own the botnets themselves. In the attack against Mizzima News, the attackers employed basic means to mask their identities, but did not or were unable to escalate their user privileges to "root" administrator level on the server or successfully cover their digital tracks. They maintained a low level of operational security and left behind significant pieces of evidence. The evidence implicates members of the oGc in the attacks, and in particular the oGc's administrator. The relatively low sophistication of the attack and the capabilities of the attackers indicate that they are best placed within the "Simple-Unstructured" category of Arquilla's framework. However, the fortuitous timing of the attack provided the attackers with a "strategic utility" that would normally be beyond their means.

Despite the correlative evidence, there are several alternative explanations concerning attribution that we have to explore. The administrator of the oGc often suggested in our IRC chats that Lynn Htun was responsible for the attacks. Lynn Htun has a

history of prolific defacements and is critical of opposition media sites. An IRC user reporting to be Lynn Htun had xer0 in his connection information, which matched a user in a channel on "overkill.myanmarchat.org" that was used by the attackers. However, it is unclear if the user we spoke with was really Lynn Htun. In addition, oGc and Lynn Htun's Myanmar Online appear to be rival IRC networks, a fact that may explain why the oGc administrator implicated Lynn Htun in the attacks.

Another explanation concerns the use of the oGc's IRC infrastructure as a platform for the attackers. It is possible that the attackers used the oGc infrastructure through some arrangement with oGc or that the oGc simply tolerated their presence. This scenario is consistent with Lynn Htun's charge that the oGc provides hosting for botnets in return for the ability to occasionally use them for DDoS targets. Another consistent explanation is that the oGc could have also supplied access to censorship-circumvention proxies to their general membership. The administrator's accounts of oGc on the circumvention software network could have been shared across members of the oGc.

Based on the evidence we collected, we assessed that the suspected attackers in this case are not particularly favorable to the Burmese opposition but cannot be simplistically characterized as "progovernment" either. Their hostility toward the Burmese opposition appears to stem from feelings of nationalism and a belief that the opposition promotes a negative image of their country. Most appear to be concerned with gaining employment and improving the state of information and communications technology in Burma. Although they have both the skills and motivation to attack opposition Web sites, they may have attacked such Web sites without formal connections to the government. While our investigation provides indications of the possible identities of the attackers, it presents more questions than answers around state involvement in the ongoing cyber attacks against Burmese opposition groups.

The characteristics of the attackers and the opportunistic nature of the attacks may reflect a "swarming effect" in which private individuals, inspired by patriotic sentiments, voluntarily participate in cyber attacks during political events without clear approval or direction from state entities. This phenomenon has been observed in a number of recent conflicts and political events, including the 2008 Russia-Georgia war, the 2009 Gaza conflict, and the 2009 Iranian elections.[58] Our investigation shows that even a relatively simplistic attack can have significant effects if it is executed at a sensitive time. The attackers in this case were able to deface Mizzima News because it was running a version of Joomla! that was known to be vulnerable. In effect, this was a preventable attack—a known vulnerability that was exploited by opportunistic attackers. However, the timing of the attack coincided with ongoing DDoS attacks, and the addition of a visible threat (defacement) compounded the effect on the political opposition and their supporters. The involvement of private individuals in cyber attacks during political events demonstrates the chaotic nature of cyberspace and shows that

while it is possible that states may be instigating attacks, they cannot control outside participants from contributing to them, and such contributions can lead to unpredictable outcomes.[59]

Although we did not find evidence of state attribution in our investigation, it does not rule out the possibility that the SPDC is somehow involved in the recurring attacks against Burmese opposition groups. However, their involvement may be more subtle and indirect than speculations of elite military units leading cyber attacks on dissident Web sites convey. It is possible that the SPDC is engaged with individuals and groups in the Burmese hacker community and either subtly encourages them to participate in attacks against opposition groups or at least condones their actions. State-sanctioned patriotic hackers have been suspected in other cyber attacks originating from Russia, China, and Vietnam, but direct evidence is elusive.[60] The state may also be employing third-party actors to conduct cyber attacks through a crime-as-a-service model in which they hire criminal groups to perpetrate the attacks or rent necessary resources such as botnets from them.

The use of technical infrastructure related to criminal activities in seemingly politically motivated cyber attacks has been observed in high-profile cases such as attacks on Georgian government Web sites during the 2008 Russia-Georgia conflict.[61] This model of privateering is potentially attractive to nation-states because it permits them plausible deniability: actions take place in a criminal ecosystem that is removed from state entities and difficult—if not impossible—to trace back to them. Confirming these speculative scenarios in Burma is difficult, since much remains unknown about the attacks, the possible actors, and the motivations behind them. However, situating these events within the wider context of recent cyber attacks in other countries shows they are part of a troubling global trend that needs to be analyzed across both the technical and political complexities of cyberspace.[62]

## Conclusion

Unlike Internet filtering at the ISP level that is limited to local control, cyber attacks conducted at strategically sensitive times have the ability to disrupt information flows to international audiences right when the content may have the most impact. States are obvious units of analysis when examining attribution and intent behind national filtering regimes. However, actors and their intentions are not as readily apparent in politically motivated cyber attacks. Despite the difficulties, due to the political nature of attacks against civil society organizations, many observers attribute these incidents to government and military entities. As a result, the attackers' capabilities are often overestimated, and their motivations are unknown. Although the issue of attribution is essential to analysis of such attacks, it remains the most difficult and ambiguous component of any investigation.

Our research illustrates the need to utilize a holistic approach that incorporates historical and political context into incident response and technical investigations, especially in cases where the attackers face little or no likelihood of being prosecuted. This analytical approach is especially applicable to civil society organizations that confront ongoing, politically motivated attacks originating from attackers who leverage geography, adversarial political relationships, and the lack of international cooperation to avoid prosecution. Careful technical analysis is required to properly assess the threat posed by attackers. However, if security incidents are treated as isolated cases focused solely on technical forensics, the bigger picture and broader implications of the attacks cannot be properly understood.

The struggle between information control and resistance in Burma takes place on a contested terrain that reveals unique characteristics of cyberspace that preclude simplistic explanations and frames. The opposition between state and citizen that is emphasized by images of military crackdowns on peaceful protesters can obfuscate the complexities of political power in cyberspace. The Burma case shows that even in a country with one of the world's most restrictive communications environments, an authoritarian state cannot maintain full control over the Internet without disconnecting from the global network all together. Conversely, the same dynamic properties of cyberspace that make it resistant to complete control are also what make vectors like denial of service attacks such effective and vexing threats against freedom of expression.

These attacks may be the product of users motivated by patriotism swarming in from the edges of the network to disrupt key information outlets, state-sanctioned military operations, or collusion between states and criminal groups operating in the shadows of the Internet. Any one or combination of these scenarios may be at work, making the study of these attacks all the more difficult.

Burma shows that Asian cyberspace cannot be simply classified as either a locus of control or resistance, but rather is better understood as the site of a constantly evolving and dynamic contest between a range of actors and agendas. Understanding how freedom of expression can be equally repressed and advocated in this environment requires studying it holistically and examining the subtle interrelations between the social, political, and technical facets of the network. Approaching the domain in this way presents significant practical and methodological difficulties for consortiums like the ONI, IWM, and the research and policy community at large, but confronting these challenges and peering into the subterranean depths of cyberspace are essential for revealing the contests being fought and the stakes involved in them.

## Notes

1. Human Rights Watch, "Burma," 2009, http://www.hrw.org/en/world-report-2010/burma; Amnesty International, "Burma, Amnesty International Report 2009," http://report2009.amnesty.org/en/regions/asia-pacific/myanmar.

2. Larry Diamond, "Liberation Technology," *Journal of Democracy* 21, no. 3 (2010): 69–82.

3. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011).

4. Mirdul Chowdhury, "The Role of the Internet in Burma's Saffron Revolution," Berkman Center for Internet and Society, September 28, 2008, http://cyber.law.harvard.edu/publications/2008/Role_of_the_Internet_in_Burmas_Saffron_Revolution; OpenNet Initiative, "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma," October 15, 2007, http://opennet.net/research/bulletins/013.

5. The Democratic Voice of Burma Web site is http://www.dvb.no.

6. The Irrawaddy Web site is http://www.irrawaddy.org.

7. The Mizzima News Web site is http://www.mizzima.com.

8. A Web site defacement is an attack in which the visual content of a page is altered.

9. For a listing of reported attacks on Burmese opposition groups, see the DoS Watch project, http://www.doswatch.org/search/label/burma.

10. Committee to Protect Journalists, "Burma's Exile Media Hit by Cyber-attacks," September 27, 2010, http://cpj.org/2010/09/burmas-exile-media-hit-by-cyber-attacks.php.

11. The Information Warfare Monitor is a sister project to the OpenNet Initiative that studies the emergence of cyberspace as a strategic domain and analyzes politically motivated cyber attacks and espionage. See Information Warfare Monitor, http://www.infowar-monitor.net.

12. Freedom House, "Burma (Myanmar) Country Report 2010," http://www.freedomhouse.org/template.cfm?page=22&year=2010&country=7792.

13. Roy Greenslade, "How Burma Quashes Press Freedom," Guardian Greenslade Blog, September 26, 2007, http://www.guardian.co.uk/media/greenslade/2007/sep/26/howburmaquashespressfreedom.

14. Printers and Publishers Registration Act (1962), http://www.burmalibrary.org/docs6/Printers_and_Publishers_Registation_Act.pdf.

15. Article 32, Television and Video Law (The State Law and Order Restoration Council Law No. 8/96), July 26, 1996, http://www.blc-burma.org/html/Myanmar%20Law/lr_e_ml96_08.html.

16. Chowdhury, "The Role of the Internet in Burma's Saffron Revolution."

17. Ibid.

18. International Telecommunications Union (ITU), "Internet Indicators: Subscribers, Users and Broadband Subscribers," 2009 figures. http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

19. See the Burma country profile in this volume; Reporters Without Borders, "Internet Enemies: Burma," 2010, http://www.rsf.org/en-ennemi26126-Burma.html.

20. Nart Villeneuve, "Fortinet for Who?" Nart Villeneuve: Malware Explorer, October 13, 2005, http://www.nartv.org/2005/10/13/fortinet-for-who/; United States Department of the Treasury, "Burma Sanctions," http://www.treasury.gov/resource-center/sanctions/Programs/pages/burma.aspx.

21. Reporters Without Borders, "Press Freedom Index 2010," 2010, http://en.rsf.org/press-freedom-index-2010,1034.html; Committee to Protect Journalists, "Ten Worst Countries to Be a Blogger," April 30, 2009, http://cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php.

22. Seth Mydans, "Steep Rise in Fuel Costs Prompts Rare Public Protest in Myanmar," *New York Times*, August 23, 2007, http://www.nytimes.com/2007/08/23/world/asia/23myanmar.html?_r=1&scp.

23. Ardeth Maung Thawnghmung and Maung Aung Myoe, "Myanmar in 2007," *Asian Survey* 48, no. 1 (2008): 13–19.

24. Ibid.

25. OpenNet Initiative, "Pulling the Plug."

26. OpenNet Initiative, "Nepal Country Profile," 2007, http://opennet.net/research/profiles/nepal.

27. James Cowie, "Egypt Leaves the Net," Renesys, January 27, 2011, http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.

28. Ronald Deibert and Rafal Rohozinski, "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet,'' in *Access Denied: The Practice and Policy of Global Internet Filtering,* ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), 123–149.

29. Brian McCartan, "Myanmar on the Cyber-offensive," *Asia Times*, October 1, 2008, http://www.atimes.com/atimes/Southeast_Asia/JJ01Ae01.html.

30. Mizzima News also previously reported being the target of DDoS attacks on July 29, 2008. Saw Yan Nang, "The Irrawaddy Hopes to Defeat the Hackers Soon," The Irrawaddy, September 19, 2008, http://www.irrawaddy.org/article.php?art_id=14283; "Websites of Three Burmese News Agencies in Exile under Attack," Mizzima News, September 17, 2008, http://www.mizzima.com/news/regional/1052-websites-of-three-burmese-news-agencies-in-exile-under-attack.html; Connie Levett, "Burmese Dissident Websites Shut Down," *The Age*, September 20, 2008, http://www.theage.com.au/news/web/burmese-dissident-websites-shut-down/2008/09/19/1221935424916.html; and Kenneth Denby, "Dissident Websites Crippled by Burma on Anniversary of Revolt," *The Times*, September 22, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4799375.ece.

31. "Burma's IT Generation Combats Regime Repression," The Irrawaddy, October 7, 2008, http://www.irrawaddy.org/print_article.php?art_id=14399; "Mizzima Websites Hacked," Mizzima News, October 1, 2008, http://www.mizzima.com/news/inside-burma/1092-mizzima-websites-hacked.html; McCartan, "Myanmar on the Cyber-offensive."

32. McCartan, "Myanmar on the Cyber-offensive."

33. "Mizzima Websites Hacked," Mizzima News; Saw Yan Naing, "Burmese Exile Media Web Site Again under Attack," The Irrawaddy, October 1, 2008, http://www.irrawaddy.org/article.php?art_id=14348.

34. "Mizzima Websites Hacked," Mizzima News.

35. "Hack Attempts Suspend Mizzima Websites," Mizzima News, October 10, 2008, http://mizzima-english.blogspot.com/2008/10/hack-attempts-suspend-mizzima-websites.html.

36. "Backdoor programs" refer to malicious software designed to provide attackers with unauthorized remote access to computer systems. For a detailed technical description of the c99shell backdoor program, see "Backdoor.PHP.C99Shell.w," Secure List, July 15, 2008, http://www.securelist.com/en/descriptions/old188613.

37. The user-agent header is sent by your browser to the Web server you are connecting to. The user-agent header commonly identifies the operating system and browser that you are using.

38. In fact, they appeared to be monitoring news of attacks on opposition Web sites, with one user posting this article into the IRC chat Myanmar ISP, "Military Government Paralyses Internet," October 9, 2008, http://www.myanmarisp.com/20080816/ICTN/ictnews0101/, authored by Reporters Without Borders, which details the ongoing attacks and suggests that the military and government were behind the attacks.

39. "Myanmar on the Cyber-offensive," BaganLand, http://baganland.blogspot.com/2008/09/myanmar-on-cyber-offensive.html.

40. Joomla! is an open-source content management system. See, Joomla! http://www.joomla.org/.

41. The following instructions demonstrate the simplicity of this browser exploit:

1. Go to URL target.com/index.php?option=com_user&view=reset&layout=confirm.
2. Write into field "token" char ' and click OK.
3. Write new password for admin.
4. Go to url: target.com/administrator/.
5. Login as admin with new password.

42. "Backdoor.PHP.C99Shell.w," Secure List, July 15, 2008, http://www.securelist.com/en/descriptions/old188613.

43. See Co.cc lookup, https://www.co.cc/whois/whois.php?domain=0verkill.

44. Moscow Aviation Institute, "Faculty of Applied Mathematics and Physics," http://www.mai.ru/english/fac_8/computer_eng.htm; Moscow Aviation Institute, "Informatics and Mathematics," http://www.mai.ru/english/fac_8/informatics_eng.htm.

45. U.S. Department of Treasury OFAC, "Nonproliferation: What You Need to Know about Treasury Sanctions," April 7, 2009, http://www.treas.gov/offices/enforcement/ofac/programs/wmd/wmd.pdf; Federation of American Scientists, "A Sourcebook on Allegations of Cooperation between Myanmar (Burma) and North Korea on Nuclear Projects," February 14, 2011, http://

www.fas.org/man/eprint/burma.pdf; Charles G. Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States," Institute for Security Technology Studies at Dartmouth College, December 2004, http://www.ists.dartmouth.edu/library/212.pdf.

46. Htet Aung Kyaw, "Burma's Generals Are Afraid of Telephones and the Internet," *The Nation*, March 24, 2009, http://www.nationmultimedia.com/2009/03/24/opinion/opinion_30098633.php.

47. Ibid.

48. See an archive of the oGc homepage at http://web.archive.org/web/20070227151313/http://www.globalogc.org.

49. Myanmar Marine University, http://www.mot.gov.mm/mmu/organization.html.

50. Before initiating conversations with members of the IRC group, we identified ourselves as researchers at the University of Toronto and explained that we were analyzing attacks against Burmese independent media Web sites.

51. Paul Roberts, "Alleged Fluffi Bunni Leader Worked for Siemens," *Computer World*, May 8, 2003, http://www.computerworld.com/s/article/81043/Alleged_Fluffi_Bunni_leader_worked_for_Siemens; Lain Tomson, "Infosec Hit by Arrest and Virus Attack," April 30, 2003, V3.co.uk, http://www.v3.co.uk/vnunet/news/2122174/infosec-hit-arrest-virus-attack; Drew Cullen, "Fluffi Bunni Nabbed at Infosec," The Register, April 3, 2003, http://www.theregister.co.uk/2003/04/30/fluffi_bunni_nabbed_at_infosec/; Gillian Law and Paul Roberts, "U.K. Police Nab Fluffi Bunni Hacker," *Computer World*, April 30, 2003, http://www.computerworld.com/s/article/80811/U.K._police_nab_Fluffi_Bunni_hacker?taxonomyId=017.

52. Myanmar IT Pros, October 23, 2008, http://www.myanmaritpro.com/forum/topics/1445004:Topic:79509?commentId=1445004%3AComment%3A79990.

53. Myanmar IT Pros, September 9, 2009, http://www.myanmaritpro.com/forum/topics/1445004:Topic:156949?commentId=1445004%3AComment%3A157606.

54. Myanmar IT Pros, August 10, 2009, http://www.myanmaritpro.com/forum/topics/1445004:Topic:148136?commentId=1445004%3AComment%3A149799.

55. Arkar Moe, "Burmese IT Contest to Aid Junta?" The Irrawaddy, August 25, 2009, http://www.irrawaddy.org/article.php?art_id=16633.

56. Myanmar IT Pros, August 26, 2009, http://www.myanmaritpro.com/forum/topics/1445004:Topic:152929?commentId=1445004%3AComment%3A153346.

57. Naval Post Graduate School, *Cyberterror Prospects and Implications*, October 1999, http://www.nps.edu/Academics/Centers/CTIW/files/Cyberterror%20Prospects%20and%20Implications.pdf.

58. Ronald Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 South Ossetia War," paper presented at 51st Annual

International Studies Association Convention, February 2010, New Orleans, LA; Jose Nazario, "Politically Motivated Denial of Service Attacks," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009), 163–181.

59. Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace."

60. Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010); Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network*, March 29, 2009, http://tracking-ghost.net; Information Warfare Monitor and Shadowserver Foundation, "Shadows in the Cloud: An Investigation into Cyber Espionage 2.0," April 6, 2010, http://shadows-in-the-cloud.net; Nart Villeneuve, "Vietnam and Aurora," Nart Villeneuve Malware Explorer, April 5, 2010, http://www.nartv.org/2010/04/05/vietnam-aurora.

61. Mike Johnson, "Georgian Websites under Attack—Don't Believe the Hype," Shadowserver Foundation, August 12, 2008, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080812.

62. For further analysis of the global prevalence and effect of DDoS attacks against civil society groups, see Hal Roberts, Ethan Zuckerman, and John Palfrey, "Interconnected Contests: Distributed Denial of Service Attacks and Other Digital Control Measures in Asia," chapter 7 in this volume.