Belarus in the Context of European Cyber Security

Fyodor Pavlyuchenko[a]
Translated from the Russian language by Kenneth Geers[b]
[a]*www.charter97.org*
[b]*Cooperative Cyber Defence Centre of Excellence*

Abstract. During the first decade of the 21st century, Internet censorship in Belarus has evolved into a government tool used to combat political dissent. State-sponsored denial of service (DoS) attacks against civil society have become a domestic crisis that threatens not only freedom of expression in Belarus, but also the integrity of Internet resources throughout Europe. The ongoing cyber conflict between state and non-state actors in Belarus is analogous to the struggle between the Russian government and its internal adversaries in cyberspace. In this essay, we recount the history of cyber censorship and attacks against Charter '97, a popular Belarusian website, and discuss the effectiveness of countermeasures.

Keywords. Belarus, Internet, censorship, charter '97, denial of service, cyber crime

Introduction

For over a decade, the Charter '97 website in Belarus has been a leading venue for Belarusian public policy discussion. Since its founding, however, the site has been forced to defend itself against practically all existing Internet censorship strategies. Following a disputed political referendum in Belarus in 1996, Alexander Lukashenko alone has governed the country. His government has suppressed freedom of speech, and Charter '97 is well-known for siding with Belarusian dissidents.

While modern technology has offered the world significantly improved communications, it also creates new threat vectors. Nation-states can abuse their power over telecommunications, creating dangerous precedents and fostering long-term political instability.

In cyberspace, the activities of the Belarusian secret services are reminiscent of their colleagues in Russia. It is critical that democratic states in Europe strengthen independent Internet resources in all European countries, and strive to extend the rule of law in the whole of European cyberspace.

1. Background: Internet Censorship in Belarus

For over a decade, there has been virtually no independent traditional media in Belarus. Under pressure from the authorities, the popular newspapers of the 1990's have ceased to exist or have seen their circulation greatly reduced. The independent FM radio stations have been closed, and an independent Belarusian television channel has never existed. It is therefore unsurprising that, despite its high cost, the Internet has been and remains the only source of objective information for the majority of Belarusians, and the number of Web users has grown to nearly one-quarter of the country's population.

09.09.2001

On September 9, 2001, at 1200, Belarusian Internet users came into conflict with the authorities for the first time – on the day of the national presidential elections. The national telecommunications firm Beltelecom – a monopoly provider in the country – intentionally blocked access to a range of popular political websites. By the following afternoon at 1600, all Internet censorship had ceased.

From a technical perspective, such information blocking is easy for a telecommunications monopoly to perform. The data packets can be filtered on the ISP's primary router based on their source or destination Internet Protocol (IP) addresses. With the help of the 'tracert' (traceroute) command, the point of network interruption was easy enough to find. During this event, the prohibited sites continued to be accessible outside Belarus, but not within the country.

Some of the popular but blocked sites, including *.home.by, *.minsk.by, *.org.by, *.unibel.by, *.nsys.by, and *.bdg.by were physically hosted on servers in Belarus, within the .by network domain. These sites were disabled by altering their Domain Name Service (DNS) records. In that context, it is important to note that the management of the .by Top Level Domain (TLD) is the responsibility of a special state agency, the Operations and Analysis Center, which falls under the direct control of the President of Belarus.

Some websites, including www.charter97.org, created multiple mirror sites in an effort to stay online. All such mirrors were promptly blocked by the government. Furthermore, popular 'anonymizer' websites and pages that published lists of free proxy servers were also blocked. In all (including the sites that were directly and indirectly blocked), over 100 websites were inaccessible.

It must be emphasized that there were no legal grounds to perform Internet censorship in this case. In fact, such censorship directly violated the Belarusian constitution. The official explanation from the Ministry of Communications and Beltelecom was that too many Belarusians were trying to access the sites in question at one time, and that this led to a self-inflicted denial of service. From a technical point of view, that explanation does not hold water. For its part, the Belarusian government had no comment, even though Internet censorship – in this case, computer sabotage – is an offense under Belarusian law. An official investigation into the facts of the case was never undertaken.

24.10.2001

The Charter '97 website was completely deleted from its server by unidentified hackers. A few days after this incident, under pressure from the Belarusian secret services, the hosting company was forced to break its contract with Charter '97, and the site was no longer allowed space on its server.

20.01.2004

In January 2004, Charter '97 was the target of a massive distributed denial of service (DDoS)-attack for the first time, which lasted more than 3 weeks. The attack followed the publication of a journalistic investigation into a possible connection between high-ranking officials from the Belarusian Interior Ministry (from a department responsible for investigating computer crimes) and the trading of child pornography on the Internet. In a strange coincidence, Natalya Kolyada, a human rights activist working with our website at that time, was also convicted on misdemeanor charges.

The DDoS attack was supported by a botnet that included more than 55 thousand active IP addresses. This network of infected computers spanned the globe, and included compromised machines in Latin America, the United States, South-East Asia, China and India. The geographic dispersion of the botnet allowed the power of its attack to be spread across a 24-hour period. Further, the power and focus of the attack changed several times, which indicated an active command and control (C2) over the activity.

While it is impossible to affirm that this attack was politically motivated, a simultaneous campaign of harassment was organized against the employees of our site on official Belarusian television. Our employees were, among other things, accused of trading in online pornography.

14.07.2004, 21.07.2004

On July 21, 2004, there were mass protests in Minsk to mark the 10th anniversary of the Lukashenko government, and our website again came under a DDoS-attack. Charter '97 had planned to host a webcast to cover the protests. One week prior, on July 14, a 'test' cyber attack had paralyzed our server for 2 hours. On July 21, the main attack began at 1400 – 4 hours before the demonstrations began – and lasted until the political protests were over. The technology and power of the attack were similar to the attack in January of that year.

10.10.2004

The next large-scale attempt to block Charter '97 and other independent websites occurred in the autumn of 2004, during parliamentary elections and a national referendum on the lifting of presidential term limits in Belarus. On the day before the election, correspondents were unable to access our website and could not call us by mobile or landline telephone. At the same time, various opposition websites were again blocked by a filter on Beltelecom's primary router.

This time, many Belarusian network users were better prepared to combat censorship, and immediately switched to Internet proxies and anonymizers. But the Belarusian Internet authorities had an effective new weapon in their arsenal: the artificial stricture – or "shaping" – of Internet bandwidth. The use of this tactic meant that, in principle, forbidden sites were still available. However, it took anywhere from 5 to 10 minutes for the censored webpages to load in a browser. Thus, most Web users were unable to gain full access to Charter '97, as well as a range of other targeted sites. All other Internet resources were accessible as normal.

There was no announcement from the Ministry of Communications or Beltelecom regarding this incident, nor was any official investigation undertaken.

19.03.2006

The next time that websites were blocked in Belarus was on March 19, 2006 – the day of Belarusian presidential elections. Well before the election took place, in an initiative called 'Free Internet', Charter '97 began to offer site visitors information regarding various ways to circumvent censorship. This strategy ensured that all attempts to block information using IP-filtering failed. However, network 'shaping' – or the intentional stricture of specific streams of network bandwidth – was again the method employed.

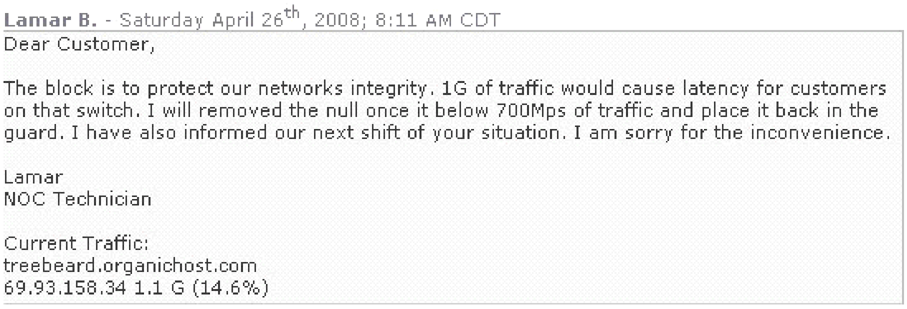
On March 18, the day before the election, a website filtering 'test' was conducted from 1600-1630. On election day, sites belonging to opposition presidential candidates and their political party websites, leading independent news sources, and www.livejournal.com (an international blogging site very popular with Belarusians) were blocked.

Representatives from Beltelecom announced that the technical interruptions were caused by the overloading of particular circuits, and no formal investigation was ever undertaken.

25.04.2008

On the eve of massive street protests in Minsk, the government changed its strategy. At 1420, a test DDoS-attack on Charter '97 lasted 30 minutes. The following IP addresses were used in the attack: 89.211.3.3, 122.169.49.85, 84.228.92.1, 80.230.222.107, 212.34.43.10, 81.225.38.110, 62.215.154.167, and 62.215.117.15. For about 10 minutes, our site was difficult to access, but we were able to restore normal traffic before the attack ended.

On April 26, the main DDoS-attack took place. It began five hours before the start of the demonstration. Charter '97 had intended to conduct a live webcast of the protests, but the attack paralyzed our server. Our hosting company, www.theplanet.com, attempted unsuccessfully to mitigate the attack. Its hardware was designed to defend against an attack only up to 700 Mbps. The volume of this DDoS reached over 1 Gbps. We had no choice but to turn off the site and simply wait for the attack to end. The perpetrators were apparently satisfied with their achievement, and the attack was over by the next day. It is important to note that other independent online media were subjected to similar attacks at the same time, especially ‘Belarusian Partisan’ and the Belarusian-language version of ‘Radio Liberty’.



Lamar B. - Saturday April 26th, 2008; 8:11 AM CDT

Dear Customer,

The block is to protect our networks integrity. 1G of traffic would cause latency for customers on that switch. I will removed the null once it below 700Mps of traffic and place it back in the guard. I have also informed our next shift of your situation. I am sorry for the inconvenience.

Lamar
NOC Technician

Current Traffic:
treebeard.organichost.com
69.93.158.34 1.1 G (14.6%)

Figure 1. Explanatory email from the Internet Service Provider (ISP)

The server hosting ‘Belarusian Partisan’ crashed as a result of the DDoS-attack. Further, system administrators even temporarily lost control of the site, and for several days, unknown hackers used the website to publish fabricated, scandalous news stories. The Belarusian Partisan editors were forced to denounce the false reports on other websites. The level of expertise required for this attack was high enough that there is no doubt the Belarusian special services were involved in the incident.

The technical capabilities of the Radio Liberty (RL) server – home to the Belarusian, Albanian, Azerbaijani, Tajik, and Russian RL services – were sufficient to contain a similar attack for more than 3 days. However, the site was nonetheless difficult to access until 1500 on April 28, and that was enough to cause a minor diplomatic scandal. The U.S. mission to the Organization for Security and Cooperation in Europe (OSCE) issued a statement on the cyber attack. The Belarusian Ministry of Foreign Affairs publicly denied any official involvement.

Increasingly, experts believe that various political DDoS attacks share some common characteristics, and that there may be important links between discrete attacks such as those which hit Estonian and Georgian websites.

08.06.2009

The most recent example of a politically-motivated DDoS attack on Charter ’97 occurred in June 2009. The incident may have been related to the recent conflict between the governments of Russia and Belarus, which resulted in the imposition of economic sanctions against Belarus and a worsening political situation inside the country.

The DDoS attack lasted more than a week, and for a while it paralyzed our site completely. The strength of the DDoS-attack in this case had not been particularly high; about five thousand IP addresses took part in it. With the support of our ISP, the Charter ‘97 technical support staff was able to neutralize the attack.

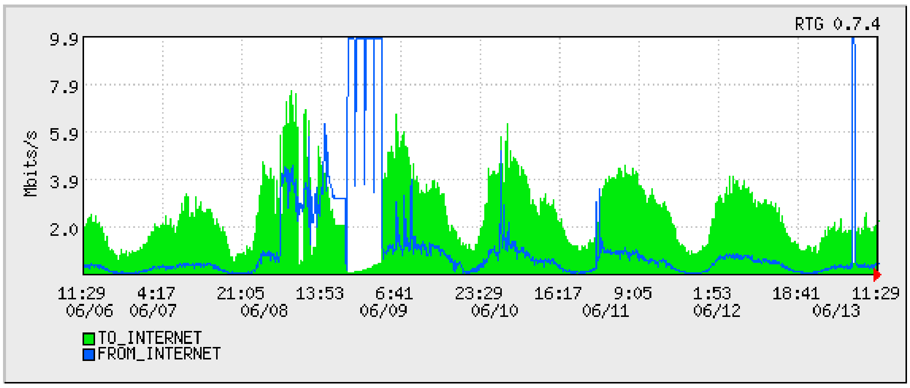


Figure 2. Timeline for the June 2009 attack against Charter '97

2. Countermeasures and their Effectiveness

Throughout the history of these DoS attacks, we have been looking for ways to counter censorship by the Belarusian authorities. We have tried many different methods, but none of them has been completely effective. Our situation might best be described as a competition to outmaneuver an opponent who has more resources than we do.

Initially, our strategy was to strengthen our technical capabilities and to increase our expertise in computer security. The site was moved to a relatively powerful, hardened server, and we created a system for monitoring vulnerabilities and attempted intrusions. We employed encryption, not only for access to the server itself, but also for access to our content management system. We created a multi-tiered system of access to the server and to the site, as well as the ability to quickly replace all passwords in the event administrators and/or journalists were arrested. We developed a distributed system for creating server data backups. Based on our experience so far, it is best to use simple, open-source technologies such as UNIX, PHP, and MySQL to help with site mobility (i.e. the rapid transfer of the site to another hosting platform). Firewall and caching technologies are sufficient to repulse DDoS-attacks of average strength. Combined, these efforts helped to prevent subsequent compromises.

Separately, Charter '97 launched the 'Free Internet' project. This website provides recommendations to site visitors for what to do in case the site is blocked, and explains how to use an Internet proxy, anonymizer, Virtual Private Network (VPN), and software such as Tor. Visitors are encouraged to disseminate information independently through their own blogs, forums, chat rooms, social networking sites, e-mail, and instant messengers. Site information is rebroadcast, for example, via RSS or email to mirror sites and partners. The successful use of these measures can overcome the simple blocking of IP addresses. However, with our limited resources, there is no current, solid countermeasure to DDoS.

We believe that the authorities have concluded that their most effective methods of censorship are DoS attacks and information manipulation. In support of the latter, specially-trained ‘visitors’ insert themselves into discussions on popular websites, and monitor or help ‘guide’ the course of discussion. During politically sensitive times, or whenever political dialogue becomes excessive, the site can be temporarily blocked by DDoS.

3. Government Power and Cyber Crime

The current power structure in Belarus not only attempts to suppress political dissent on the Internet, but also flagrantly violates the Belarusian constitution. In Belarus, there is no legal basis for Internet censorship, much less for computer hacking and DoS attacks on websites. There is only one case of censorship in Belarus that was officially acknowledged and at least somewhat justified: in 2005, Beltelecom blocked two Russian gay sites for possession of pornography, at the behest of the Ministry of Culture’s Republican Commission for the Prevention of Promoting Pornography, Violence and Cruelty. All other cases of Internet censorship involved the use of blatantly criminal methods.

DDoS-attack techniques against Belarusian independent Internet media could easily be used to block all sites covering current affairs in Belarus. Further, the lack of the rule of law within Belarusian Internet space could facilitate the growth of organized cyber crime on the international level.

There is active cooperation between Belarusian and Russian special services in cyberspace: the Agreement on Cooperation of the Commonwealth of Independent States (CIS) in Combating Cybercrime was signed in 2000. Finally, there are similarities in the cyber attack methods used against Estonia, Georgia, and the websites of human rights organizations in Belarus and Russia, which suggest that these crimes have common roots.

4. What is Required?

The challenge of DDoS attacks threatens civil society throughout Eastern Europe. In Belarus, Ukraine, Russia, Georgia, Armenia, and Azerbaijan, the government may already have used DDoS attacks as a tool for countering dissent on the Internet. To mitigate this threat, an international, collaborative approach is required. A good start would be the establishment of an international hosting platform designed to support freedom of speech throughout Europe, built by a team of international experts. They should investigate cyber crimes based on aggregate data, and work toward the development of effective defense methods and technologies. The mere creation of such a platform would be a helpful step, and could enhance the level of cyber security and freedom of expression throughout Europe.