A US-CCU Special Report

August 2009

Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008

The ramifications of the August 2008 cyber campaign against Georgia are still being felt a year after the actual conflict. A delayed echo of the conflict interrupted Twitter and Facebook on August 6th and 7th of 2009, temporarily inconveniencing millions. More important, the cyber campaign against Georgia, along with the cyber campaigns against Estonia in 2007, Lithuania in 2008, and Kazakhstan in early 2009, has helped put cyber attacks on the international agenda to a much greater extent than previously. The European Union held its first ministerial meeting devoted to critical infrastructures and cyber security on April 27th and 28th, 2009. Many other conferences and meetings have featured the Georgian experience. Given the frequency with which the cyber campaign against Georgia is cited and discussed, it is important for people both to get the facts right and to appreciate how many of the questions that arose earlier about this conflict have now been answered. In many important respects, the cyber campaign against Georgian presents a pattern that can be expected in future conflicts.

THE US-CCU REPORT ON THE GEORGIAN CYBER CAMPAIGN

The U.S. Cyber Consequences Unit (US-CCU), an independent, non-profit research institute, is in an unusually good position to report on the cyber campaign against Georgia. It was informed of the cyber attacks the almost immediately after they began and many hours before they were publicly reported. The US-CCU was able to monitor much of the attack activity over the internet as it was taking place. It was also able to collect data after the conflict from web caches, the Georgians, the companies hosting their websites, the forums and websites used by attackers, an informal global network of cyber-security professionals, and many of the other participants. This data included extensive network traffic logs and security logs. Much of the more accurate information on the Georgian cyber attacks that appeared in the world news media, both while the attacks were in progress and immediately after, was provided by the US-CCU. When the cyber campaign ended, the US-CCU continued its investigation into the attacks, gradually building up a fairly comprehensive picture of what happened and when.

John Bumgarner, the US-CCU's chief technical officer, led the research effort, carried out most of the analysis, and wrote the US-CCU's comprehensive technical report on the campaign. This report is roughly a hundred pages long and contains detailed information on the attack techniques, their chronology in relation to the military events, the actual attack scripts, screen captures of the defaced websites, the websites and forums used organize and launch the attacks, the specific domain addresses employed by the attackers, and information pointing to the probable identities of many of the attackers. Because of the sensitive nature of much of this information, the full report is being released only to officials within the U.S. government and to certain cyber-security professionals.

This current document containing the conclusions and highlights from the report is being provided to selected journalists and policy makers on the anniversary of the campaign. The report offers no judgments about the extent to which the cyber campaign against Georgia should be condemned, tolerated, or justified. It merely tries to answer, as completely as possible, the basic questions about the cyber campaign carried out against Georgia between August 7th and August 16th, and the consequences of this campaign.

CONCLUSIONS AND HIGHLIGHTS FROM THE US-CCU'S ANALYSIS OF THE GEORGIAN CYBER CAMPAIGN

The Nature and Identity of the Cyber Attackers

- The cyber attacks against Georgian targets were carried out by civilians with little or no direct involvement on the part of the Russian government or military.

> The US-CCU was able to collect a considerable amount of information on the recruitment of the attackers and their specific attack activities. All of the attackers and activities showed every sign of being civilian. Most of those carrying out the cyber attacks were Russians, but as the attacks continued, an increasing number of Russian sympathizers in

other countries became involved. Outside of Russia itself, the largest numbers of participants were from the Ukraine and Latvia. Although it would in principle have been possible for the Russian military to have carried out some of these cyber attacks, disguising their involvement convincingly would have been very difficult and expensive. The cyber attacks included many different actions in many different locations by many different people. The attackers displayed a convincing amount of disorder without being at all random. Most important, given the verifiable quantity of civilian cyber-attack activity, any direct Russian military involvement was simply unnecessary.

- The organizers of the cyber attacks had advance notice of Russian military intentions, and they were tipped off about the timing of the Russian military operations while these operations were being carried out.

  Many of the cyber attacks were so close in time to the corresponding military operations that there had to be close cooperation between people in the Russian military and the civilian cyber attackers. When the cyber attacks began, they did not involve any reconnaissance or mapping stage, but jumped directly to the sort of packets that were best suited to jamming the websites under attack. This indicates that the necessary reconnaissance and the writing of attack scripts had to have been done in advance. Many of the actions the attackers carried out, such as registering new domain names and putting up new websites, were accomplished so quickly that all of the steps had to have been prepared earlier. Given the speed of action, the signal to go ahead also had to have been sent before the news media and general public were aware of what was happening militarily.

- Social networks operating over the internet were the main tool used to recruit those carrying out the attacks.

  From the nature and effects on the online postings, it is clear that the cyber attackers were not just communicating over the internet; they were being recruited over the internet. This is a relatively new development, made possible by the recent expansion of “Web 2.0” websites and by the increase in the total number of computer users in Russia with access to them. The forums used to recruit and arm the cyber attackers were not, for the most part, hacker forums, but social networking forums devoted to dating, hobbies, politics, and other shared interests. All but one of the main forums used to organize the attacks were in Russian. The one non-Russian forum was in English, hosted out of San Francisco.

- The civilian cyber attackers were aided and supported in their efforts by Russian organized crime.

  Some of the webservers and addresses used to control and coordinate the attacks were ones that had previously been used by Russian criminal organizations. Several servers used in the attacks were simultaneously hosting software ready to be used for other cyber crime activities. In addition, the specific botnets employed in the cyber campaign were ones closely associated with Russian organized crime. Occasionally, during the cyber campaign, some of the zombie computers being used to attack Georgia were also used temporarily for criminal attacks on e-commerce websites. It appears that Russian criminal organizations made no effort to conceal their involvement in the cyber campaign against Georgia, because they wanted to claim credit for it.

- The total number of individual civilian cyber attackers involved in the campaign against Georgia was much greater than in the campaign against Estonia, although the total number of computers involved was much smaller.

  The greater number of civilian attackers active against Georgia was evident in much greater quantity of activity visible in online forums. The total volume of attacks needed to shutdown the Georgian targets, however, was considerably less than the volume needed to shut down the Estonian targets, because of the much higher volume of domestic and international internet traffic that Estonian websites are designed to handle.

Methods Used to Carry Out the Cyber Campaign

- The first wave of cyber attacks was carried out by botnets and command and control systems that that were ready before the Russian invasion.

  These were the botnets and the command and control systems associated with Russian organized crime. They were the only botnets known to be utilized in the cyber campaign. The botnets themselves had already been used for criminal activities, but several of the command and control systems were utilized for the first time to control the attacks on Georgia. They continued to be used to attack the same websites throughout the conflict. After the initial wave of attacks, the target lists of these botnets were extended to include a few more websites, but the focus of these botnets still remained fairly narrow, never expanding beyond a total of eleven targets.

- After the first wave of attacks, the chief method used to maintain and expand the cyber campaign was a series of postings on websites. These postings contained both the cyber-attack tools and the lists of suggested targets for attack.

  The web postings were sufficiently complete, so that individuals could contribute to the cyber attack effort who had very limited computer skills. A variety of different websites were used for the postings, including some that were created specifically for the cyber campaign. Some of the websites that were used to organize the attacks were hosted in the United States. The website postings were so productive, that a further forty-three targeted websites were effectively shut down or defaced, in addition to the eleven targeted by the botnets associated with organized crime.

- The types of cyber attacks used against Georgia were limited to denials of service and website defacements, but these relatively unsophisticated types of attacks were carried out in a very sophisticated manner.

  Most of the cyber-attack tools used in the campaign appear to have been written or customized to some degree specifically for the campaign against Georgia. The tools employed for denials of service included three different software applications designed for “stress tests,” in which webservers are flooded with HTTP packets to see how much of this traffic they can handle. A fourth piece of software was originally designed for adding functions to websites, but was adapted by the attackers so that it would request random, non-existent web pages. These HTTP-based attack tools were tested by the US-CCU in a laboratory environment and proved far more effective than the ICMP-based attacks that the Russians had used on Estonia. The attack tool that requested non-existent web pages was especially efficient, because the servers attacked by this tool rapidly exhausted their computing capacity searching for the pages that weren’t there. This tool, as posted, simultaneously targeted seventeen different Georgian websites. Together, these features made this attack tool particularly devastating. Some of the website defacements were carried out using SQL injections, which were also discussed in the online attacker forums. This is an unusually sophisticated technique for such a purpose.

- At least one of the website defacements used in the Georgian campaign was prepared specifically for use against Georgia more then two years before the attacks.

    In fact, the US-CCU's technical analysis showed that the graphic art used in this website defacement was created on March 10, 2006, when relations between Georgia and Russia had previously been in crisis. This graphic art was not deployed anywhere, however, but was simply stored until it was used in the cyber campaign of August 2008. The fact that this website defacement was saved, along with the many other signs of advance preparation and planning, suggests that cyber attacks against Georgia had been on the Russian agenda for some time.

- The cyber attackers refrained from carrying out the sorts of attacks that would have done lasting physical damage to the Georgian critical infrastructure, even though some of those involved in planning the cyber campaign may have had some idea of how to carry out such attacks.

    Investigations by the US-CCU suggested that a number of Georgian critical infrastructures were accessible over the internet at the time Russia invaded Georgia. There is reason to believe that at least some of these infrastructures would have been vulnerable to cyber attacks causing physical damage. Meanwhile, at least some of the Russian cyber attackers showed signs of considerable technical expertise. If the Russian military had chosen to get directly involved, such attacks would have been well within their capabilities. The fact that physically destructive cyber attacks were *not* carried out against Georgian critical infrastructure industries suggests that someone on the Russian side was exercising considerable restraint.

The Targets and Effects of the Cyber Campaign

- The first targets for cyber attacks were government and news media websites.

    These cyber attacks were clearly designed to make it harder for the Georgians to determine what was happening. The inability of the Georgia to keep these websites up and running was instantly damaging to national morale. These attacks also served to delay any international response.

- After the Russian troops had established positions in Georgia, the attack list was expanded to include many more government websites, Georgian financial institutions, business associations, educational institutions, more news media websites, and a Georgian hacking forum.

    These cyber attacks were designed to make it difficult to organize an effective response to the Russian presence. Many of them were intended to interrupt normal business operations. Others were intended to make Georgian population uncertain about what to expect and what they should do. Nearly all of the more important government websites were successfully attacked, including the presidency, ministries, courts, and parliament. Apart from the two big banks, the business-related targets were primarily organizations that could have been used to communicate and coordinate responses among different businesses. The educational institutions attacked included those devoted to science, technology, and medicine. The BBC and CNN were among the many news media attacked, probably because they were providing useful information about the conflict, rather than for ideological reasons. Five of the Georgian government websites, along with the national bank, were defaced with political propaganda, but this material seems to have been designed for more for emotional disruption than political persuasion.

- The primary objective of the cyber campaign was to support the Russian invasion of Georgia, and the cyber attacks fit neatly into the invasion plan.

  The cyber attacks began on a large scale within a few hours of when the Russian military operations began, and they ended just after the Russian military operations ended. The targets for attack were nearly all ones that would produce benefits for the Russian military. The one target for cyber attack that was somewhat unusual from a military standpoint was a website for renting diesel-powered electric generators, but even this target was presumably chosen to reinforce the effects of physical strikes on the Georgian power grid. More strikingly still, the news media and communications facilities, which would ordinarily have been attacked by missiles or bombs during the first phase of an invasion were spared physical destruction, presumably because they were being effectively shut down by cyber attacks.

- The cyber attacks significantly impeded the ability of the Georgian government to deal with the Russian invasion by interfering with communications between the government and the public, stopping many payments and financial transactions, and causing confusion about what was happening.

  The cyber attacks disrupted the Georgian government's efforts to disseminate information about the invasion and deprived the government of many information sources. They made it difficult to keep the outside world informed about what was happening, reducing the chances of outside help. Although the portion of the total population using the internet in Georgia is relatively low, the portion of business executives, community leaders, journalists, and government officials using the internet is much higher. Communication among these groups was greatly impeded during the cyber campaign, not only when it involved the targeted websites, but also more widely, because the high volume of cyber attack traffic jammed many general communications links. The channels of communication that were seriously disrupted during parts of the cyber campaign included e-mails, land-line phone calls, and cell phones. The National Bank of Georgia was forced to severe its internet connection for ten days, stopping most of the financial transactions dependent on that institution. The economic disruptions and other uncertainties may have slowed activities where the Georgian government was dependent on private sector businesses. In a crisis situation, all of these mechanisms and effects became very important.

- There could also be delayed effects of the cyber attacks if criminals or other groups used the denial of service attacks and the website defacements as a cover for inserting spyware or other malware into the targeted systems.

  The defenders were so preoccupied with responding to the overt cyber attacks, that they gave little or no attention to the possibility of simultaneous covert attacks. However, since Russian criminal organizations were helping with the attacks, and since many of the targets were financial institutions, it would be surprising if some of the professional criminals involved didn't also try to exploit the situation for future financial gains.

Georgia's Response to the Cyber Campaign

- One of Georgia's first responses to the cyber attacks was to contact Estonian officials, who had already had experience with a campaign of cyber attacks. These officials put the Georgians in touch with an informal network of international cyber-security experts who were able to offer help and advice.

  The Georgian efforts to deal with the cyber campaign were organized on this informal, ad hoc basis, rather than by the intervention of any international organization. Although the amount of talent the Georgians were able to involve informally was impressive, it is noteworthy that there was no international organization they could contact for help.

- Georgia's initial technical response to the cyber attacks was to install filters that would block Russian IP addresses and certain protocols used by the attackers, but the attackers circumvented these counter-measures by using foreign servers to mask their actual IP addresses, by employing attack software that spoofs IP addresses, and by changing protocols.

- Georgia's more effective technical response to the cyber attacks was to shift the hosting of their websites to other countries, where the attack traffic could be more easily filtered out and where the available bandwidth was greater.

  Some of the websites for the Georgian government were moved to servers in Estonia and the United States. Even these foreign hosting companies, despite their greater available bandwidth, had great difficulty in keeping the Georgian websites accessible, because of the larger volume of traffic that the attackers were generating by that point.

- There was at least one significant Georgian cyber counter-attack against Russian targets, but the damage it did was very limited.

  This counter-attack took the form of an attack tool that was posted on Russian websites with instructions for Russian sympathizers to use it against Georgia. The US-CCU obtained this attack tool, analyzed it, and found that the attack script was designed to attack only Russian websites, with nineteen of them on the pre-loaded target list. Any Russian sympathizers who used the tool would therefore have been unknowingly attacking Russian websites. No evidence of damage caused by this attack script came to the US-CCU's attention, which suggests that any harm it caused was not extensive.

Strategic Consequences of the Cyber Campaign

- If the conflict is viewed from a broader perspective, encompassing economic and cyber action, the real strategic focus seems to have been the Georgian oil and gas pipelines.

  When the Baku-Tbilisi-Ceyhan pipeline became operational in 2005, Georgia became a major transshipment hub for oil and natural gas being pumped from the landlocked Caspian Sea. This caused Russia to lose large amounts of revenue and reduced its economic and political bargaining power in Europe. Georgia's Baku-Supsa oil pipeline, its Baku-Tbilisi-Erzurum gas pipeline, and its tanker car railroads, are also very important to the international energy markets.

  When the Russians invaded Georgia, a large portion of their military operations focused, not on securing the areas inhabited by ethnic Russians, but on the Georgian ports and facilities for handling oil and gas. Unstable ground conditions, augmented by cyber attacks, soon made all of the Georgian pipelines seem unreliable. Meanwhile, two days after the invasion began, the Turkish section of the Baku-Tbilisi-Ceyhan pipeline was attacked by local militants, supposedly on their own initiative. One result of these developments was to cause BP Azerbaijan to shift its oil transport to the Russian Baku-Novorossiisk pipeline, even though the costs were double those of the Georgian pipelines. When the Georgian railways were also attacked, oil and gas production in the Caspian fields had to be severely reduced. The longer-term effect of these disruptions has been to cause oil producers to look for alternative routes. This increases the value and importance of the Russian routes.

- The cyber campaign against Georgia must also be seen as part of longer term effort by Russia and other countries to test the uses of cyber attacks and the international responses to them.

  From the cyber campaign against Estonia in April and May of 2007, Russians had already learned that a cyber campaign mounted by civilians could cause serious economic and psychological disruptions in a country without provoking any serious international response. This lesson was reinforced by their experiences with the cyber campaigns against Lithuania at the end of June 2008 and against Kazakhstan in January 2009, where major local disruptions produced remarkably little international press coverage.

  The campaign against Georgia took place under different conditions, because Russia was engaged in overt military action against the country, but the cyber component was still carried out by civilians, and there were no international reprisals. Given this history, it would be very surprising if most future disputes and conflicts involving Russia and its former possessions or satellites weren't accompanied by cyber campaigns.

Practical Lessons from the Cyber Campaign

- There is urgent need for an international organization that would provide risk advisories to member countries a) when political, economic, and military circumstances make a wave of cyber attacks likely, and b) when warning signs of actual preparations for a cyber campaign are detected.

  A number of international experts, including those at the US-CCU should, in principle, have been able to warn Georgia that there was a high probability it would suffer cyber attacks coinciding with the escalating tensions between Georgia and Russia. Given the attitudes being expressed over the internet, all that was needed was a triggering incident, such at the invasion itself, to set off attacks. If Georgia had been monitoring the appropriate channels with international help, there is a good chance it would have observed signs of preparation for the attacks. The Georgian president's website had already been attacked three weeks before the Russian invasion. Other preparatory activities would probably have been apparent if someone had been looking for them. Once the attacks were getting underway, these advance warnings would have made it possible for Georgia to deal with each successive wave of attack activity as it was being mounted, rather than waiting until the Georgian targets had been shut down.

- There is urgent need for an international cyber response force that could provide quick reactionary assistance to member countries, advising them on what to do and setting up the operations to do it.

  This cyber response force would need to have well-established working relationships with each nation's computer emergency response team (CERT). It would also need to have contracts and other agreements ready to be activated that would allow the appropriate private sector hosting companies and other services to be brought in as soon as it was evident they were needed. If Georgia had been able to call on this sort of apparatus, the interruptions in its online activities would probably have only lasted a few hours or even a few minutes, rather than several days. In addition, a well-prepared international team could have collected forensic evidence, making it possible to answer the questions about the cyber campaign that still remain open. One of these important unanswered questions is what spyware and other malicious code the attackers may have left behind.

- There is an urgent need for cyber response exercises in every country, involving active participation by all of the relevant government officials and departments, the private sector companies that would be called upon to support them, and the international organizations whose help would be needed.

  Without such exercises, the relevant officials will waste precious time trying to figure out whom they should be contacting and what they should be doing. Even with a complete international support apparatus in place, there would be no way to utilize it efficiently without advance practice. The cyber security exercises that are required would not necessarily have to be international in scope, but they would need to have at least a few international participants. Even cyber campaigns directed only against targets in one country require an international response if they are going to be handled effectively.

John Bumgarner
Research Director for Security Technology (CTO)
U.S. Cyber Consequences Unit
john.bumgarner@usccu.us

Scott Borg
Director and Chief Economist (CEO)
U.S. Cyber Consequences Unit
scott.borg@usccu.us