# The Russo-Georgian War 2008:

## The Role of the cyber attacks in the conflict

May 24th 2012

Warfare has reached a new frontier. Over the past several years and even decades, it has been accumulating to this point where war is not only fought with bombs and guns anymore but also with bits and bytes. With the increasing implementation of the World Wide Web into our society and its increasing necessity in conducting our regular lives, it was only a matter of time that somebody would utilize cyberspace to their tactical and strategic advantage in combat. The U.S. government once classified cyberspace as a nervous system and therefore control system of the nation.[1] Even the U.S. Pentagon has formally acknowledged cyberspace as a new sphere in warfare that is equally important as operations conducted in land, sea, air and space.[2] Now we have reached a point in which cyber operations have become an essential part in warfare. Anybody who doesn't have a proper cyber warfare policy or even have the most rudimentary cyber capabilities will fall behind in any military struggle in the future. Even though the physical harm that cyber attacks could induce are still limited at the moment, the increasing interconnectedness of our electronic systems and essential life-lines to the world are becoming more vulnerable and at the same time, more attractive to control in combat. The world is beginning to see the worthwhile advantages that cyber operations can provide when used in combat. The impact of such cyber operations which was previously limited to industry insiders, specialized military units or intelligence services, was revealed in August 2008 when Russian forces invaded their neighbor Georgia with the help from initially invisible cyber warriors.

Hostilities between the Russian Federation and the Republic of Georgia weren't an extraordinary occurrence by itself since there have been violent conflicts in the past that range back decades. But this altercation between the Russians and Georgians was different. Their

[1] Department of Homeland Security, *The National Strategy to Secure Cyberspace*, February 2003, p. vii, Retrieved April 15th 2012 from web site: www.us-cert.gov/reading_room/cyberspace_strategy.pdf
[2] William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, Foreign Affairs, Issue Sept/Oct. 2010, pp. 97–108

conflict was heavily influenced by cyber elements. Up to this conflict, cyber warfare only referred to sole cyber attacks by one party on to another or solely between hackers without any other measures taken. But this conflict between Georgia and Russia was unprecedented in warfare because the offensive cyber attacks conducted, appeared to be part of a synchronized effort that accompanied strategic and tactical military operations on the ground. This case was one of the first overt acts of cyber warfare in recent history after the events in Estonia in 2007. This small regional quarrel showed several cyber warfare techniques, their limitations as well as their impact on the population. At the same time and because of the public nature of the conflict, this case has sparked global fears of the additional possibilities that cyber attacks can have in the future of warfare.

**History and reasons for war**

Russia and Georgia share a long history of differences that reach back to the beginning of the Soviet Union in the early 20th century. These differences have been brewing ever since and resulted in violent ethnic clashes that need to be considered to understand the motivations of the cyber hackers. Once the Soviet Union collapsed in the early 1990s, multiple leaders of ethnic regions in the successor states demanded instant autonomy from the new governments in the former satellite states.[3] Early demands by ethnic regions like South Ossetia and Abkhazia were seen as reasonable at first. But the demands for autonomy soon escalated and turned confrontational once they were pushing the limits the governments were willing to make. The resulting violent ethnic separatism between Georgia and the regions of Abkhazia and South Ossetia was constantly influenced by Russia. Russia stood on the side of the minorities and

[3] Julia A. George, *The Politics of Ethnic Separatism in Russia and Georgia* (New York: Palgrave Macmillian, 2009), p. 13

supported them. Russia's involvement resulted from a 1992 law that allowed former Soviet Union citizens to apply for Russian citizenship and many of the people in the neighboring regions took advantage of.[4] This made Russia a key player to any discourse between the parties because it oftentimes invoked the right to intervene for its citizens. To further ensure their constant involvement in any negotiations, the Russia aids the regions financially. They also left small military peacekeeping forces in both Abkhazia and South Ossetia after violence broke out in the early 1990s.[5] Ever since then, tensions were running high. These disagreements resulted in minor aggressions and the occasional posturing from time to time. All sides would exchange some fire or increase their militia and police presence to make their points while the politicians continue their course of flaring harsh rhetoric against each other.[6] But a Russian invasion into South Ossetia and Abkhazia like in August 2008 was unprecedented. Right before the Russian invasion though, there were several signs that pointed to a potential escalation and maybe even violent confrontation. The Georgian government under the leadership of Saakashvili pursued several policies that would lead to the complete destabilization of relations between Georgia and South Ossetia.[7] Saakashvili began to rapidly build up Georgian military capabilities. This build-up only increased the distrust among the regional factions. Furthermore, Georgia began targeting smuggling markets important to the economy of South Ossetia by implementing several anti-corruption reforms.[8] These reforms combined with heightened rhetoric by senior Georgian officials allowed relations to become more than tense and they were only amplified by Russia

[4] The Christian Science Monitor, *Russia-Georgia conflict: Why both sides have valid points*, August 19th 2008, Retrieved April 14th 2012 from web site: http://www.csmonitor.com/World/Europe/2008/0819/p12s01-woeu.html
[5] Ibid
[6] George, *The Politics of Ethnic Separatism in Russia and Georgia*, p.180
[7] Ibid, p. 181
[8] Ibid, p. 183

interests in blocking Georgian aspirations to join the ranks of NATO.[9] These and many more simmering long-time differences between the opposing parties accumulated and ultimately escalated in the crisis of August 2008. As relations between the parties were deteriorating, both Russia and Georgia seem to have taken preemptive measures in case of an escalation of the aggressions. Signs of approaching divergence caused Russia to hold military exercises (called "Kavkaz-2008") at several points of the border with Georgia.[10] From mid-July to August 2008, Russia had 8000 soldiers and heavy military hardware in the area that remained on high alert even after the exercises had ended.[11] One of the exercises even involved a hypothetical attack on Abkhazia and South Ossetia (probably from a country symbolizing Georgia) to which Russian forces practiced a counterattack to protect their interests (i.e. Russian citizens).[12] In this military exercise, Russian troops received a leaflet indicating exact Georgian troop compositions, strengths and weaknesses as well as a reminder to know the "probable enemy".[13] This would suggest that Moscow was determined to show force and even make use of it to keep their control in the region. Records even show that the coalition forces of Russia, Abkhazia and South Ossetia were prone to more and earlier violent actions than Georgian forces which might indicate preventive intensions.[14] On the other hand, Georgia already experienced violent exchanges with South Ossetian militias in previous months running up to the Georgian incursion.[15] And even

[9] Richard Weitz, *Global Security Watch: Russia* (Santa Barbara, Praeger Security International, 2010), p. 133
[10] John Berryman, "Russia, NATO Enlargement, and 'Regions of Privileged Interests'" in *Russian Foreign Policy in the 21st Century* edited by Roger E. Kanet (New York, Palgrave Macmillian, 2011), p. 234
[11] Ibid
[12] Jim Nichol, *Russia-Georgia Conflict in August 2008: Context and Implications for U.S. Interests*, Congressional Research Service, March 3rd 2009, p. 4, Retrieved April 15th 2012 from web site: www.fas.org/sgp/crs/row/RL34618.pdf
[13] Svante Cornell & Frederick Starr, *The Guns of August 2008: Russia's War in Georgia* (New York: Central Asia-Caucasus Institute, 2009), p. xi - xii
[14] Andrei Illarionov, "The Russian Leadership's Preparations for War, 199-2008" in *The Guns of August 2008: Russia's War in Georgia* edited by Svante Cornell & Frederick Starr (New York: Central Asia-Caucasus Institute, 2009), p. 77-82
[15] George, *The Politics of Ethnic Separatism in Russia and Georgia*, p.181

though there was a military exercise in Georgia with troops from the United States and other regional neighbors to increase the interoperability of NATO and coalitions forces in Iraq, most of these troops had already left once the fighting with the Russians began.[16] Finally, in the evening of August 7th 2008, the Georgian military entered the South Ossetian capital and several other villages because they claimed that they were responding to bombardments by South Ossetian soldiers that ignored a previously established cease-fire.[17] On August 8th 2008, Russia responded to the Georgian invasion of South Ossetia with superior military force because they saw Georgian actions as a threat. This was the first time that Moscow deployed its military forces outside of its borders since the war in Afghanistan in 1979.[18] Even though both Russia and Georgia are disputing the justifications for intervention of their respective adversary, they both went to war that ultimately ended in a show of Russian superiority and the degradation of the long-term effectiveness of the Georgian military.[19]

**Cyber attacks: The importance and the techniques**

But as already mentioned before, this altercation between Russia and Georgia was more unusual then the ones that came before. Prior to and throughout the conflict, Georgia experienced an intensive build up of cyber attacks against governmental and civilian online infrastructure. The increasing reliance on computer networks to pass information has left governments and the public vulnerable to influence from third parties. Computer Network Operations (CNO) usually inherits a support function in military operations. According to the United States Information Operations doctrine, computer network operations have several purposes that include the denial,

[16] Nichol, *Russia-Georgia Conflict in August 2008*, p. 4
[17] George, *The Politics of Ethnic Separatism in Russia and Georgia*, p. 182
[18] Charles E. Ziegler, "Russia, Central Asia, and the Caucasus after the Georgia Conflict" in Russian Foreign Policy in the 21st century edited by Roger E. Kanet (New York, Palgrave Macmillian, 2011), p. 155
[19] Weitz, *Global Security Watch: Russia*, p. 150

degradation or destruction of information resident in computer networks as well as the gathering of data from adversarial information systems.[20] The cyber attacks against Georgia showed similar functions. These attacks appear to have had many different objectives but the bulk of activities were specifically targeted to deny and disrupt communications and therefore affecting the overall information flow inside Georgia.[21] The unavailability of information in a conflict can have severe psychological effects that can demoralize or disorient the people and decision making. Also, several hackers infiltrated numerous Georgian web sites and defaced them for Russian propaganda purposes.[22] But these attacks were not only designed to control the flow of information or form the perception of the people, they were also part of information exfiltration activities that tried to steal and accumulate military and political intelligence from Georgian networks as well.[23] These activities included various waves and different techniques that ranged from distributed denial of service (DDOS) attacks to web site defacements.[24] Even though these attacks have utilized simple methods, they appear to have been executed in a very sophisticated manner that successfully achieved their desired objectives. Although, Georgia has a relatively low number of internet users and a low overall dependence on IT-based infrastructure, the cyber attacks supported the overall Russian invasion.[25]

---

[20] U.S. Department of Defense, *Joint Publication 3-13: Information Operations*, February 13th 2006, Retrieved April 15th 2012 from web site: http://www.fas.org/irp/doddir/dod/jp3_13.pdf

[21] David Hollis, *Cyberwar Case Study: Georgia 2008*, Small Wars Journal, January 6th 2011, p. 3, Retrieved April 15th 2012 from web site: smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

[22] Hollis, *Cyberwar Case Study: Georgia 2008*, p.3

[23] Joseph Menn, *Expert: Cyber-attacks on Georgia websites tied to mob, Russian government*, Los Angeles Times, August 13th 2008, Retrieved April 15th 2012 from web site: http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html

[24] U.S. Cyber Consequences Unit, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, August 2009, p. 4, Retrieved April 15th 2012 from web site: http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

[25] E. Tikk, K. Kaska, K. Rünnimeri, M. Kert, A. Talihärm & L. Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified*, Cooperative Cyber Defence Centre of Excellence, November 2008 , p. 5, Retrieved April 15th 2012 from web site: www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

The coordination for the cyber attacks appears to have been implemented weeks before the any shot was fired between both adversarial parties. Reports suggest that there have been streams of data directed against Georgian government sites and their internet assets as early as July 19th 2008.[26] Hackers targeted the website of the President of Georgia Mikhail Saakashvili and were able to overload the site with requests which made it unavailable and necessary to be taken down for 24 hours.[27] The technique used to render the website inoperable was a distributed denial of service (DDoS) attack. Distributed denial of service (DDoS) attacks is a well-known method used in cyberspace and by various hackers around the world. They allow a user to utilize several thousands of previously infected computers around the world to flood a specific site with equally abundant requests that effectively shuts down the service by cutting off new legitimate visitors.[28] The infected computers that are actually flooding the sites, often to the surprise of their owners, have a master/slave relationship. They can also be known as botnets or zombie computers because they can be directed by only a small amount of controllers. The first attack by itself did not raise any suspicions. After the initial cyber attack at the end of July, there hasn't been much activity running up to the conflict besides what in hindsight appears to have been preparations or reconnaissance for the major attacks.[29]

Right before the Russian invasion of Georgia, the cyberattacks have increased in numbers, in targeted websites and also in sophistication. Web sites affected this time by the attacks, besides the page of the Georgian president, included the pages of the parliament, the

[26] John Markoff, *Before the Gunfire, Cyberattacks*, New York Times, August 12th 2008, Retrieved April 15th 2012 from web site: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1
[27] Dancho Danchev, *Georgia President's web site under DDoS attack from Russian hackers*, ZD Net, July 22nd 2008, Retrieved April 15th 2012 from web site: http://www.zdnet.com/blog/security/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/1533
[28] Brian Krebs, *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks*, The Washington Post, October 16th 2008, Retrieved April 15th 2012 from web site: http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html
[29] Markoff, *Before the Gunfire, Cyberattacks*, 2008

foreign ministry, the interior ministry, several news agencies and even a few banks.[30] Also among the first targeted web sites were Georgian hacker forums.[31] These were not entirely successful but appear to have been designed as a pre-emptive strike against any possible retaliatory attacks from Georgian hackers.

In addition of using distributed denial of service attacks, the hackers utilized other methods like SQL injections and cross-site scripting (XSS) that generally achieve the same outcome and deny access to the targeted sites.[32] SQL injection is a more sophisticated method of denial of service attack that allows the user to achieve the same results but without the same amount of infected computers or 'zombies' at his disposal. This method allows the user to bypass the websites and directly inject the malicious queries into the web server and blocking the response time.[33] Using methods like these indicates that there was some level of planning, reconnaissance and technical knowledge involved that allowed such swift control and access to servers.[34]

Other than experiencing denial of service attacks, several Georgian websites experienced defacements as well. Website defacement is a technique that changes the appearance of the website. The online hackers utilized several picture collages that depicted and compared the Georgian president Mikhail Saakashvili with postures of Adolf Hitler, the leader of Nazi Germany.[35] Defacements of this type and other pro-Russian propaganda depictions were found

[30] Travis Wentworth, *You've Got Malice*, Newsweek: The Daily Beast, August 22nd 2008, Retrieved April 15th 2012 from web site: http://www.thedailybeast.com/newsweek/2008/08/22/you-ve-got-malice.html
[31] Gregg Keizer, *Russian hacker 'militia' mobilizes to attack Georgia*, Computerworld, August 13th 2008, Retrieved April 21st 2012 from web site: http://www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html
[32] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol: O'Reilley Media Inc., 2012), p. 3
[33] Krebs, *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks*, 2008
[34] Ibid
[35] Dancho Danchev, *Coordinated Russia vs Georgia cyber attack in progress*, ZD Net, August 11th 2008, Retrieved April 16th 2012 from web site: http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670

on political/governmental and financial sites of the Georgian president, the National Bank of Georgia as well as the Ministry of Foreign Affairs while afterwards being under denial of service attacks as well.[36] Such depictions can have a tremendous value and influence on the local Georgian and Russian population. Depicting the Georgian leader as a vicious WWII dictator is both demoralizing for the Georgians and also rallying for the Russians to attack the enemy. Such psychological operations (PSYOPS) usually are undertaken by military personnel because of their demoralizing effects. It therefore is questionable if such behavior wasn't previously planned ahead because such depictions like the comparison of Saakashvili to Hitler were well selected.

There were also unconfirmed reports that might suggest that several hackers targeted servers located in other countries like Turkey and the Ukraine.[37] Georgia is very dependent on other neighboring countries when it comes to internet connectivity by land. It has to rely on connections that run through countries like Turkey, Armenia and Russia.[38] So if these reports are accurate about targeted servers in neighboring countries that are responsible for guiding internet traffic to Georgia, then controlling these servers meant that cyber hackers were in full control of the complete internet transfer in Georgia and therefore in control of the flow of information in Georgian cyberspace. Such access would allow for tremendous tactical as well as strategic advantages for the Russian forces on the ground. Researchers have also found evidence that some Georgian internet traffic was apparently redirected through Russian telecommunications firms and that some of their servers had software programs responsible for some attacks.[39] This implicates Russian involvement that might go beyond random hackers due to its higher sophistication.

[36] Tikk, Kaska, Rünnimeri, Kert, Talihärm & Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified*, p. 7
[37] Ibid, p. 11
[38] Ibid, p. 6
[39] Markoff, *Before the Gunfire, Cyberattacks*, 2008

Besides the aforementioned attacks, online hackers also abused lists of public e-mail addresses and exploited government networks for potentially valuable information.[40] Because the cyber attacks gained access to government websites and servers, they were also aware to some of the information stored on them. This allowed them to use the information on Georgian politicians for spamming or other nefarious purposes. The cyber aggressors also tried to sway initial international public opinion of the conflict by trying to manipulate non-scientific quick votes online on sites like from CNN.[41] This allowed the Russian bloggers to influence initial perception and make Russia's actions appear to be justified as a peacekeeping intervention. Such efforts in connection with the unreliable communications in the conflict might generate initial support for the Russians side until the deception would be discovered. Such rather minor actions, even though not considerably harmful, created nuisances that diverted focus and necessary attention.

**Georgian cyber defenses**

The Georgian government's cyber defense capabilities were very limited and spread out thinly due to the scale of the conflict on the ground as well as the barrage of cyber activities on their systems. The Georgian's first response to the massive amounts of activity in their internet infrastructure was to establish filtering mechanisms that would lock out any Russian IP-address from accessing Georgian networks.[42] The bulk of attacks originated from servers located in Russia. This method was rather ineffective because the hackers expected such behavior and adapted quickly by circumventing these filters through accessing the Georgian systems over

[40] Tikk, Kaska, Rünnimeri, Kert, Talihärm & Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified*, p. 10
[41] Alexander Melikishvili, *The Cyber Dimension of Russia's Attack on Georgia*, The Jamestown Foundation, September 12th 2008, Retrieved April 21st 2012 from web site:
http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=33936
[42] U.S. Cyber Consequences Unit, *Overview by the US-CCU of the Cyber Campaign*, p. 7

servers in other countries apart from Russia. The Georgian government also immediately contacted Estonian officials in hopes of gaining access to their vast expertise after the 2007 cyber attacks in Estonia and also because there wasn't any international organization they could address for help otherwise.[43] The Estonians provided informal access to some of their own cyber security experts and even sent two of their information security experts to Georgia in order to assist locally with the defense.[44] But even with their cooperation, they were unable to mitigate any of the attacks effectively and mostly worked on damage control.

The only real effective defensive countermeasure the Georgians used in order to keep some of their information channels to the public open was the transfer of cyber assets and websites to servers in countries like the United States, Estonia and Poland.[45] These measures were often undertaken by third parties like private businesses rather than official host countries like the U.S. government. The Georgian President's website transferred to Google blog servers in California, the Ministry of Defense website to a private business in Atlanta, the Ministry of Foreign Affairs to servers in Estonia and the Office of the President of Poland allowed its website to disseminate information on behalf of the Georgian government.[46] The owner of Tulip Systems in Atlanta has offered his services to the Georgian government in order to protect Georgian internet interests but without any official approval by the U.S. government.[47] After the conclusion of the conflict, the company reported that it experienced cyber attacks against the

[43] Ibid
[44] Tikk, Kaska, Rünnimeri, Kert, Talihärm & Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified*, p. 15
[45] Ibid, p. 14
[46] Richard Clarke & Robert Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: Harper Collins Publisher, 2010), p. 19 and Tikk, Kaska, Rünnimeri, Kert, Talihärm & Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified*, p. 14
[47] Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, Parameters, U.S. Army War College, Volume XXXVIII, No. 4, p.66-67

website that was taking refuge on their servers.[48] Such involvement of other country's servers and cyberspace could have potentially escalated the situation if there had been any coherent and uniform cyber policy that would address sovereignty in cyberspace in case of attacks. Large scale attacks on a country's assets usually calls for the involvement of the government. This relocation of cyber assets could have involved the United States, Poland or Estonia in the Russo-Georgian conflict politically or militarily. Matters like taking down websites are often still considered cyber crimes. These classifications should be reconsidered since these attacks were applied as a tool of warfare and were not of criminal origin. Such evasion of cyber assets was a new precedent in strategic cyber operations and needs to be addressed in the future because of its potential to engross other actors into a confrontation and bypass their neutrality.

However, during the attacks on the Georgian internet infrastructure, the Georgians weren't only on the defensive. Once the ramifications and the impact on the Georgian cyber infrastructure were realized, more international support from unlikely places poured in as well. A few German hackers tried to redirect Georgian internet traffic through a German server and keep the websites up and running. They managed this only for a few hours in the initial stages of the conflict until their efforts were intercepted and rerouted through servers in Moscow.[49]After the initial attacks and their failure to completely take down local hacker forums, Georgian hackers began to mobilize as well. They retaliated with their own denial of service attacks. The Georgians targeted the web site of a Russian news service based in Moscow called RIA Novosti.[50] Another counterattack effort by Georgians was the distribution of an attack tool designed for Russian sympathizers that by its use would unknowingly attack Russian web sites

[48] Korns & Kastenberg, *Georgia's Cyber Left Hook,* p. 67
[49] Tom Espiner, *Georgia accuses Russia of coordinated cyberattack*, C-Net, August 11th 2008, Retrieved April 17th 2012 from web site: http://news.cnet.com/8301-1009_3-10014150-83.html
[50] Keizer, *Russian hacker 'militia' mobilizes to attack Georgia*, 2008

instead of Georgian sites.[51] Retaliations of this kind were very limited and rather ineffective due to the massive influx of attacks from Russian sources.

**Origin of the cyber attacks and their possible connections**

Overall, these cyber attacks on Georgian systems and networks spanned over several weeks that lasted from before the conflict had started to after it already had ended. However, the main bulk of the attacks were simultaneously coordinated with Russian forces on the ground during the five day Russian incursion that started August 8th and lasted until the ceasefire agreement on August 12th 2008. Such coordination with military forces and the military value of denying the adversary any means of communications would suggest that the Russian government and its military were behind the barrage of cyberattacks on Georgian systems. They would have been the greatest beneficiary of the situation. But even though the Georgian government was quick to accuse the Russians for the attacks and the Russians were equally as swift to deny any cyber involvement, there are several signs that might suggest the real perpetrators.[52] After the conflict, there were a lot of accusations identifying several different groups to be behind the attacks. These groups included the Russian military, their secret intelligence services (i.e. the FSB), Russian nationalists and even Russian organized crime syndicates. It appears that all of these groups could have had some (even if only limited or indirect) involvement with the cyber attacks.

Because of the nature of the internet with its anonymity and the limited detection possibilities, the true origin of the cyberattacks is difficult to determine. Internet traffic can be redirected throughout the world and over several different servers that are located in countries

[51] U.S. Cyber Consequences Unit, *Overview by the US-CCU of the Cyber Campaign*, p. 7
[52] Markoff, *Before the Gunfire, Cyberattacks*, 2008

who might have had no involvement at all. Nevertheless, several cyber security analysts concluded that the bulk of the attacks originated from severs that were located in the Russian Federation.[53] Due to the origin of the servers, the minor sophistication and crude techniques used in the attacks, most security analysts are confident that regular Russian civilians were mostly responsible for initiating the chaos on Georgian web sites and networks.[54] Although over the course of the conflict, there were signs that an increasing amount of pro-Russian sympathizers from other countries, like from the Ukraine and Latvia, began participating in some form as well.[55] Over the past several years, there has been a major mobilization of a hacker underground movement in Russia and which oftentimes speaks out about political issues virtually or literally seeks out involvement in form of nationalistic articles in the Russian media.[56] Therefore, it is believed that a lot of these Russian nationalists tried to assist their government against the Georgians that in their eyes have been responsible for the ethnic tensions in the Caucasus area. This Russian 'cyber militia' is very active. The cyber attacks in Estonia in 2007 as well as the attacks in Lithuania in 2008 have been attributed to their exploits. Right before the increased volume of the cyber activities were registered, several Russian web forums and hacker sites became active against Georgia. Sites like "xaker.ru"(in English: hacker.ru), **"**stopgeorgia.ru" or "stopgeorgia.info" began rallying for the Russian cause and encouraged would-be cyber militia members by using propaganda, distributing a static list of targets as well as providing cyber tools and their instructions.[57] Security analysts found out that many of these sites catered to a specific demographic and nationality because the access from U.S.-based addresses and computers was

[53] Espiner, *Georgia accuses Russia of coordinated cyberattack*, 2008
[54] U.S. Cyber Consequences Unit, *Overview by the US-CCU of the Cyber Campaign,* p. 2
[55] Ibid, p. 3
[56] Danchev, *Georgia President's web site under DDoS attack from Russian hackers*, 2008
[57] Danchev, *Coordinated Russia vs Georgia cyber attack in progress*, 2008

quickly banned or restricted.[58] At these sites, there was a whole cadre of knowledgeable hackers that assisted beginners with their hacking techniques. This top-down hierarchy was also the supplier of the instructions and tools that allowed beginners to evade security firewalls and disguise their tracks to circumvent any Georgian countermeasures.[59] Such specialized knowledge and sophistication again suggests some sort of support from the Russian government or military and some elements could have easily been inside that hierarchy. A former Russian defector admitted once that Russian hackers convicted of cyber crimes are oftentimes given a choice to work for the intelligence services instead of going to prison.[60] Such hackers under the control of the government could easily direct and give instructions to beginners while completely disguised under a random username in a forum. Through such an ad hoc approach of teaching novice hackers, a few experienced could control a sizable operation by distributing seemingly random orders. Afterwards, it would be impossible to determine who was behind the main users that instigated others to join. Once the targets, tools and instructions were provided and online for everybody to obtain, the Russian cyber militia began to mobilize themselves like a chain reaction. Many of the hackers even began collaborating over well-known social media portals like Twitter and Facebook.[61] Such a form of cyber militia comprised of enthusiastic nationalists and hackers can be very devastating but also very beneficial for a government. Because there is no 'visible' connection between the government and the 'voluntary' hackers, deniability is ensured. On the other hand, the actions of the militia cannot be directly controlled unless they are preplanned. Indications for such organization can be found in the specific distribution of targets, tools and instructions. Therefore, it is still unclear if the cyber militia acted alone or was

[58] Krebs, *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks*, 2008
[59] Ibid
[60] Ibid
[61] Siobhan Gorman, *Hackers Stole IDs for Attacks*, The Wall Street Journal, August 17th 2009, Retrieved April 21st 2012 from web site: http://online.wsj.com/article/SB125046431841935299.html

instigated by others. The information on the main perpetrators in the cyber campaign against Georgia that organized the whole operation is still limited. But there are indications or potential connections that might implicate the Russian government over another third party.

There has been an accumulating amount of evidence that points to a St. Petersburg-based criminal cyber gang known as the Russian Business Network or RBN.[62] Many of the attackers against Georgia have apparently used tools, attack commands and servers that have been attributed with the Russian organized crime outfit. This organization has been connected to several criminal specialties over the past. Their expertise has been proven to include crimes in identity theft, child pornography, and extortion as well as other nefarious crimes conducted over the internet.[63] Several thousand internet pages are linked to the Russian Business Network but still the company seems to have no legal identity. It is possible though that this Russian cyber mafia has very loose connections to the Russian government. The RBN has been known to contract its services to third parties and since there hasn't been any major attempt by the Russian government to shut down this organization, the absence of action could suggest that it is being endured if not even employed for its services.[64] Stopgeorgia.ru was another site involved in the cyber attacks that had ties to criminal activities involving fraudulent passports and credit card scams to which the Russian authorities were rather inactive in investigating.[65] There is also evidence that the Russian Business Network has been focusing their efforts on non-Russian companies or citizens which implies a possible nationalistic character.[66] Targeting non-Russian entities, having no legal identity, no 'official' point of contact or its law-enforcement adverse

[62] Markoff, *Before the Gunfire, Cyberattacks*, 2008
[63] Brian Krebs, *Shadowy Russian Firm Seen as Conduit for Cybercrime*, The Washington Post, October 13th 2007, Retrieved April 17th 2012 from web site: http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html
[64] Wentworth, *You've Got Malice*, 2008
[65] Tikk, Kaska, Rünnimeri, Kert, Talihärm & Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified*, p. 13
[66] Krebs, *Shadowy Russian Firm Seen as Conduit for Cybercrime*, 2007

behavior could all indicate that this 'company' and its function is a cover or a front company for something else that might be indirectly connected to the Russian government, one of its intelligence services or the Russian Mafia. Ever since the fall of the Soviet Union and the restructuring of the main intelligence service KGB, there have been allegations that there are likely ties between the Russian government and organized crime syndicates. Several allegations even suggest that the Russian government or parts of the ultra-nationalist Liberal Democratic Party of Russia (LDPR) use criminal organizations or mafias as an extension of political power and utilize them in cases where the government cannot 'officially' act.[67] The involvement of the suspicious Russian Business Network can only suggest that this wave of cyber attacks against Georgia wasn't an unplanned and spontaneous occurrence after all. It rather suggests that there is a strong sense of coordination behind the operation even though hard evidence and ties to the Russian government are still elusive.

Even though there are a few pieces missing that would establish a 'visible' connection with the Russian government and military, the 'coincidence' of a coordinated attack from the Russian ground forces and the invisible cyber forces still seems far from being a random event. Besides the possible connections to a main supplier or organizer (the RBN), the patterns of the cyber attacks also suggest that there must have been some communication with the Russian military. Besides the rapid mobilization of Russian forces on the border to Georgia and the reconnaissance work in Georgian networks by hackers, the first wave of cyber attacks coincided almost simultaneously with the first Russian aerial bombing runs.[68] Such tactical and operational assistance in cyberspace can be beneficial when it seamlessly coincided with the location and

[67] Luka Harding, *WikiLeaks cables: Russian government 'using mafia for its dirty work'*, The Guardian, December 1st 2010, Retrieved April 22nd 2012 from web site: http://www.guardian.co.uk/world/2010/dec/01/wikileaks-cable-spain-russian-mafia

[68] Dan Goodin, *Georgian cyber attacks launched by Russian crime gangs*, The Register, August 18th 2009, Retrieved April 22nd 2012 from web site: http://www.theregister.co.uk/2009/08/18/georgian_cyber_attacks/

destination of the Russian military. The main bulk of the cyber activities followed the military like a homing beacon. The logical course of action for independent Russian hackers with no ties to the Russian military would have been to solely target the main hubs of Georgian power and communications systems in the capital of Tbilisi. But instead, the cyber attacks initially focused on local news sites as well as official sites of the town of Gori because it was the first target of the Russian military.[69] Such denial and disruption of information is important in order to undermine an adversary's command and control structure. The resulting confusion can be exploited. Also, another sign of military involvement in the cyber attacks can be found in the modus operandi of the cyber intruders. Not only did they specifically target main internet lines of communications but they also targeted specific Georgian "cyber defenses" in form of Hacker forums. This kind of preemptive strike resembles military behavior that would focus on taking out potential threats first. After already having an upper hand, the Russian assault followed the military concept of 'shock and awe' and rapidly overwhelmed the enemy. 'Shock and awe' or rapid dominance is designed to anticipate and counter all opposing moves as well as control the battlespace and deprive the enemy of all its senses.[70] Elements in cyberspace would be essential to such a strategy in the 21st century. These similarities with military behavior might suggest some consultation with each other.

**Outcome and lessons for the future**

Even though it was a very short quarrel, the Russo-Georgian conflict has achieved strategic repercussions for the Russians. The Russian government is one of the main suppliers of energy to the European continent. Besides the constant ethnic tensions in the Caucasus region,

[69] Menn, *Expert: Cyber-attacks on Georgia websites tied to mob, Russian government*, 2008
[70] Harlan K. Ullman & James P. Wade, *Shock and Awe: Achieving Rapid Dominance* (National Defense University, 1996), p. xxvii, xxix

the actors in the region are strong competitors in the energy market. Ever since Georgia became a major distribution center for energy in the region, Russia experienced major losses in market share and in its political bargaining power with Europe. Once the Russians invaded Georgia, a major bulk of their military operations focused on the security of energy distribution centers like ports or pipelines.[71] This turmoil triggered energy producers and consumers to look for more secure sources. Russian supply became more attractive again even though it might be more costly. Even after the conflict has ended, the uncertainty of new potential conflicts still creates doubt within energy consumers.[72]

Besides the energy benefits for Russia that resulted from the conflict, the use of the 'unofficial' Russian cyber militias has proven to the world the potential such an instrument can have on a conflict. Not only did these rather crude cyber efforts disrupt vital lines of communications to the people in the crisis as well as to the international community, they also had a significant psychological element that intensified the fears and mismanagement of the public. Such actions can create panic and confusion which can delay valuable defensive measures. Should such measures increase in sophistication in the future and be applied to a fully developed communications network, then they could have an even more amplified effect compared to the situation in Georgia. The international community and especially the United States often underestimate the value of such cyber militia groups while countries like Russia and China have been encouraging them. These cyber attacks on Georgia have proven to Russia once again that the use of a cyber militia can have a tremendous impact on economics or psychology

[71] U.S. Cyber Consequences Unit, *Overview by the US-CCU of the Cyber Campaign*, p. 7
[72] Jeffrey White, *Georgia-Russia conflict shows EU's energy vulnerability*, The Christian Science Monitor, August 15th 2008, Retrieved April 23rd 2012 from web site: http://www.csmonitor.com/World/Europe/2008/0815/p01s03-woeu.html

without causing a severe international response.[73] The usage of this tool has already gradually increased over time and the Russian government has been benefiting a lot from the actions of its hackers through their campaigns against Estonia (2007), Lithuania (2008) and Kyrgyzstan (2009). The Russian government has been benefiting from the situation while always keeping their deniability intact. Tools like these might become a norm for Russian political interaction in the future since it has been proven useful both in peacetime and in tandem with military operations. Especially since such a cyber campaign is very cost effective and can have more local and international impact than some military hardware by itself.[74] Therefore to fully understand the motivations that potentially can rally such a cyber militia, it is important to understand the historical and cultural backgrounds of the nation that utilizes them. Because the main bulk of the cyber attackers were regular citizens acting out of patriotism that were most likely instigated by Russian provocateurs, there needs to be further understanding what could trigger their behavior. History, Culture and ethnic differences need to be further analyzed to gather more potential indications and warnings (I&W) mechanisms. Through the rising technological advancements and easy to use tools, regular citizens can have a significant impact in the cyber realm. A single individual with a computer can become an influential and impactful asset in military operations in the future because he could cause disruption and confusion on a wider scale at his home computer than what a single individual could have achieved alone a few decades ago.

Every time such cyber attacks occur, they test the international community. Their willingness to react, their cyber defenses, their detection capabilities as well as other potential third party involvements (like German hackers trying to help Georgian internet traffic to stay

[73] U.S. Cyber Consequences Unit, *Overview by the US-CCU of the Cyber Campaign*, p. 8
[74] Markoff, *Before the Gunfire, Cyberattacks*, 2008

online) are always exposed for analysis in the aftermath. These cyber warfare campaigns can often be seen as real-life simulations with real-life consequences. Such gathered data from these events can be very beneficial for defensive measures. Security analysts can oftentimes gain valuable insights from the attacker's pattern of movement in cyberspace or from their targeting methods. This allows experts and intelligence analysts to generate indication and warning (I&W) procedures that specify certain aspects that might direct to an oncoming cyber assault. Such intelligence information is very valuable to government and militaries because it allows them to plan ahead and be on alert if such signatures amass. Elements from the Georgian cyber conflicts might prove useful in the future if analyzed intensively. Preemptively targeting a nation's patriotic hacker community to eliminate retaliatory capabilities is an intelligence indicator example that has not been seen in any other cyber campaign from the past. A nation's civilian hacker community has not been considered to be a significant threat in the past but the Russian cyber militia has proven that even civilian hackers might be able to strike effectively and could retaliate. Other indicators might involve an increased amount of internet traffic on strategically important lines of communications (local news services, governmental sites, servers, etc.) or regional locations. Because of the modus operandi of the Russian cyber militia that attacked Georgian networks, many countries can potentially build countermeasures against them or allow their intelligence services to be alerted in time to effectively respond otherwise. Accumulating indications and warnings (I&W) would allow analysts to counter any potential attacks. But public dissemination and analysis of such cyber attacks needs to be considered carefully and potentially controlled. Even though private businesses are always in search of new cyber defenses, it could occur that by publishing their analysis, cyber offenders might have access to the information as well. Having such information allows perpetrators to adapt their techniques

and signatures for potential future operations. Public dissemination of such cyber attacks needs to be more contained or limited so that perpetrators cannot adapt their array of techniques to become more effective in the future.

Another issue that the events in Georgia have exposed is that the international community and the United States are still unprepared concerning a lot of subjects in cyberspace. There is still a need for more international consensus and clarification when it comes to cyberspace and cyber attacks with military potential. The lines between cyber crime and cyber warfare are still not clearly defined should another situation arise. Current international law and United States law concerning the rules of engagement in cyberspace are still very ambiguous. The July 2008 cyber attacks prior to the conflict would have been classified as cyber crimes even though they were essential in the reconnaissance of Georgian systems and ultimately in the execution of the attacks in August.[75] Also, the U.S.-based businesses that assisted Georgian websites to stay online could have been seen by the adversarial cyber hackers as legitimate targets because they offered their servers as protection. This could have threatened United States neutrality in the conflict and could have potentially involved them further even though they did not authorize any of the transfers.

The Russo-Georgian conflict has also shown that there is an increasing need for synchronized cyberspace and military operation exercises that could effectively simulate potential future conflict scenarios. The cyber element has become an essential part of effective full spectrum operations and needs to be further explored in order to understand all the essential aspects. The Russian cyber militia might represent a variable which is not fully explored in the planning of war scenarios by the intelligence and military services. Because of the Russian

[75] *Computer Fraud and Abuse Act (18 U.S.C. 1030)*, as amended, Retrieved April 24th 2012 from web site: http://www4.law.cornell.edu/uscode/18/1030.html

government's deniability with the activities of their civilian cyber force, the militia could be utilized for an array of intelligence functions. Not only can they be called upon in conflict situations, they could prove useful in intelligence gathering or even denial & deception (D&D) operations because their activities in peacetime are still seen as mediocre crimes instead of threats to national security.

As one can see, such cyber assaults have almost become part of standard Russian political and military discourse. Every time there were unfavorable Russian sentiments being displayed in former Soviet Union satellite countries like Estonia, Lithuania, Georgia or Kyrgyzstan, Russian-originated cyber attacks took place to cause trouble and show force. There isn't much effort to suppress such activity by the Russian government and their inaction only provides more tacit affirmation to the Russians responsible. The Russo-Georgian war in 2008 wasn't the fullest display of cyber warfare capabilities to date and their level of sophistication was limited because they didn't utilize military cyber capabilities (that are publically known). But this case allows a glimpse at the potential such unsophisticated techniques can have when civilians target and disrupt strategic communications mechanisms. Cyber warfare has become a necessary element in the modern conduct of war. Here, cyber capabilities showed their potential on an only limited connected country while leaving the potential effects of a military operation with cyber elements on an IT-developed country still open to imagination.

## Bibliography

Berryman, John. "Russia, NATO Enlargement, and 'Regions of Privileged Interests'" in *Russian Foreign Policy in the 21st Century* edited by Roger E. Kanet (New York, Palgrave Macmillian, 2011)

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol: O'Reilley Media Inc., 2012)

The Christian Science Monitor. *Russia-Georgia conflict: Why both sides have valid points.* August 19th 2008. Retrieved April 14th 2012 from web site: http://www.csmonitor.com/World/Europe/2008/0819/p12s01-woeu.html

Clarke, Richard & Robert Knake. *Cyber War: The Next Threat to National Security and What To Do About It* (New York: Harper Collins Publisher, 2010)

*Computer Fraud and Abuse Act (18 U.S.C. 1030)*, as amended, Retrieved April 24th 2012 from web site: http://www4.law.cornell.edu/uscode/18/1030.html

Cornell, Svante & Frederick Starr. *The Guns of August 2008: Russia's War in Georgia* (New York: Central Asia-Caucasus Institute, 2009)

Danchev, Dancho. *Coordinated Russia vs Georgia cyber attack in progress*. ZD Net. August 11th 2008. Retrieved April 16th 2012 from web site: http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670

Danchev, Dancho. *Georgia President's web site under DDoS attack from Russian hackers*. ZD Net. July 22nd 2008. Retrieved April 15th 2012 from web site: http://www.zdnet.com/blog/security/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/1533

Department of Homeland Security. *The National Strategy to Secure Cyberspace.* February 2003. Retrieved April 15th 2012 from web site: www.us-cert.gov/reading_room/cyberspace_strategy.pdf

Espiner, Tom. *Georgia accuses Russia of coordinated cyberattack.* C-Net. August 11th 2008. Retrieved April 17th 2012 from web site: http://news.cnet.com/8301-1009_3-10014150-83.html

George, Julia A. *The Politics of Ethnic Separatism in Russia and Georgia* (New York: Palgrave Macmillian, 2009)

Goodin, Dan. *Georgian cyber attacks launched by Russian crime gangs*. The Register. August 18th 2009. Retrieved April 22nd 2012 from web site: http://www.theregister.co.uk/2009/08/18/georgian_cyber_attacks/

Gorman, Siobhan. *Hackers Stole IDs for Attacks.* The Wall Street Journal. August 17th 2009. Retrieved April 21st 2012 from web site: http://online.wsj.com/article/SB125046431841935299.html

Harding, Luka. *WikiLeaks cables: Russian government 'using mafia for its dirty work'.* The Guardian. December 1st 2010. Retrieved April 22nd 2012 from web site: http://www.guardian.co.uk/world/2010/dec/01/wikileaks-cable-spain-russian-mafia

Hollis, David. *Cyberwar Case Study: Georgia 2008.* Small Wars Journal. January 6th 2011. Retrieved April 15th 2012 from web site: smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Illarionov, Andrei. "The Russian Leadership's Preparations for War, 199-2008" in *The Guns of August 2008: Russia's War in Georgia* edited by Svante Cornell & Frederick Starr (New York: Central Asia-Caucasus Institute, 2009)

Keizer, Gregg. *Russian hacker 'militia' mobilizes to attack Georgia.* Computerworld. August 13th 2008. Retrieved April 21st 2012 from web site: http://www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html

Korns, Stephen W. & Joshua E. Kastenberg. *Georgia's Cyber Left Hook.* Parameters. U.S. Army War College Volume XXXVIII. No. 4. p. 60-76

Krebs, Brian. *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks.* The Washington Post. October 16th 2008. Retrieved April 15th 2012 from web site: http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html

Krebs, Brian. *Shadowy Russian Firm Seen as Conduit for Cybercrime*. The Washington Post. October 13th 2007. Retrieved April 17th 2012 from web site: http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html

Lynn III, William J. *Defending a New Domain: The Pentagon's Cyberstrategy*. Foreign Affairs. Issue Sept/Oct. 2010. pp. 97–108

Markoff, John. *Before the Gunfire, Cyberattacks*. New York Times. August 12th 2008. Retrieved April 15th 2012 from web site: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1

Melikishvili, Alexander. *The Cyber Dimension of Russia's Attack on Georgia.* The Jamestown Foundation. September 12th 2008. Retrieved April 21st 2012 from web site: http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=33936

Menn, Joseph. *Expert: Cyber-attacks on Georgia websites tied to mob Russian government*. Los Angeles Times. August 13th 2008. Retrieved April 15th 2012 from web site: http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html

Nichol, Jim. *Russia-Georgia Conflict in August 2008: Context and Implications for U.S. Interests.* Congressional Research Service. March 3rd 2009. Retrieved April 15th 2012 from web site: www.fas.org/sgp/crs/row/RL34618.pdf

Tikk, E., K. Kaska, K. Rünnimeri, M. Kert, A. Talihärm & L. Vihul. *Cyber Attacks Against Georgia: Legal Lessons Identified.* Cooperative Cyber Defence Centre of Excellence. November 2008. p. 5. Retrieved April 15th 2012 from web site: www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

Ullman, Harlan K. & James P. Wade. *Shock and Awe: Achieving Rapid Dominance* (National Defense University, 1996)

U.S. Cyber Consequences Unit. *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008.* August 2009. p. 4. Retrieved April 15th 2012 from web site: http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

U.S. Department of Defense. *Joint Publication 3-13: Information Operations.* February 13th 2006. Retrieved April 15th 2012 from web site: http://www.fas.org/irp/doddir/dod/jp3_13.pdf

Weitz, Richard. *Global Security Watch: Russia* (Santa Barbara, Praeger Security International, 2010)

Wentworth, Travis. *You've Got Malice*. Newsweek: The Daily Beast. August 22nd 2008. Retrieved April 15th 2012 from web site: http://www.thedailybeast.com/newsweek/2008/08/22/you-ve-got-malice.html

White, Jeffrey. *Georgia-Russia conflict shows EU's energy vulnerability.* The Christian Science Monitor. August 15th 2008. Retrieved April 23rd 2012 from web site: http://www.csmonitor.com/World/Europe/2008/0815/p01s03-woeu.html

Ziegler, Charles E. "Russia, Central Asia, and the Caucasus after the Georgia Conflict" in Russian Foreign Policy in the 21st century edited by Roger E. Kanet (New York, Palgrave Macmillian, 2011)