Cyberwar – Russia the usual suspect

Sérgio Tenreiro de Magalhães

Faculty of Social Sciences
Portuguese Catholic University
Campus Camões,
4710-362 Braga, Portugal
E-mail: stmagalhaes@braga.ucp.pt

Henrique Santos

Department of Information Systems
University of Minho
Campus de Azurem,
4800-058 Guimarães, Portugal
E-mail: hsantos@dsi.uminho.pt

Leonel Duarte dos Santos

Department of Information Systems
University of Minho
Campus de Azurem,
4800-058 Guimarães, Portugal
E-mail: leonel@dsi.uminho.pt

Hamid Jahankhani

School of Computer and Technology
University of East London,
University Way,
London E16 2RD, UK
E-mail: hamid.jahankhani@uel.ac.uk

Abstract. The evolution of the technology and the changes in the organization and control of the critical infrastructures of nations are creating a new combat front. The cases studied in this paper relate to the attack to the information systems and services of Estonia, in May 2007, and Georgia, in August 2008, occurring at the same time as the conventional military operation executed by the Russian Federation's army in the South Ossetia. The Russian Federation has been repeatedly accused of this operations, but the data collected raises doubts and in the second case-study showed the existence of a poorly organized network, related to Russian criminal organizations, supporting the possibility of this being an instance of the Maoist concept of the “People’s war”. This paper will also show that, despite the unsophisticated resources used in most of the attacks and to promote them, the damages in the selected targets were considerable.

Keywords: cyberwar; information security; Information warfare, Russian Federation; people’s war; people’s cyberwar; Estonia; Georgia

Introduction

The evolution of the technology changed the way nations fight. The battle field has changed along time, reflecting the four basic ways of confrontation: the melee (face to face combat, without organization, where each men takes is own decisions on what and how to do); massing (massive attacks using rigid formations); manoeuvre (adoption of manoeuvre and combat tactics); swarming (disperse attacks characterized by a high level of autonomy, requiring a high organizational level that allows the maintenance of the strategic coherence) [1]. This evolution is gaining new perspectives, once the physical world is more and more vulnerable to attacks occurring in the digital world, cyberspace, once it is getting more and more dependent on information and information systems. In fact, the United States Department of Defence information system alone suffers something like 250.000 attacks every year [2].

Although the use of the cyberspace to conduct military operations, as another military front, can be classified as a type of irregular war, once there are not well defined combat front-lines or rears and because it occurs in an unlimited space [3], it may involve the preparation and execution of military operations conducted by the entities of one nation against one other, with identical objectives to those of a conventional war and sometimes aiming to weaken the conventional communication and control enemy defences, in order to weaken its conventional ability to response [4]. This can mean the interference, the control or the destruction of the information and of the civilian and military systems, of the critical infrastructures like the communication centres of the medical emergency, transportation, energy, water and other critical services. Also the civilian population’s computing systems can be affected in order to achieve the defined goals. Therefore, the consequences of a combat in the cyberspace can be as real as those of a conventional war and can even cause casualties [5].

In April 2007, Russia was accused by Estonia of attacking its digital structure, in an event that many consider to be the first conflict that can be named as a cyberwar [6]. Just over a year of being accused of those, Russia was again accused to perform a cyberattack to Georgia (one of the countries of the extinct Soviet Union) on August of 2008. This attack was made at same time as Russian’s armed forces attacked conventionally Georgia. Those attacks were related with South Ossetia, a region of

Georgia known to be pro-Russian and with separatist claims. Although the poor data, there were some appeals on the Internet to cybercombat that allows the evaluation of the intentions and some of the resources used. The appeals were made in several Russian language *fora* and on the websites www.stopgeorgia.ru and www.stopgeorgia.info, on an action with a very strong, if not exclusive, popular character.

People's war

The digital attack to Georgia was coordinated from the domain www.stopgeorgia.info (based in German and quickly closed by the owner of the web server) and www.stopgeorgia.ru. This last site was based on the United Kingdom, created on 9 August of 2008, and kept in operation until 13 August, when it was suspended, returning to work after twenty four hours, without the software section and with a inoperative forum.
In the manifest presented on Website it can be read:

> *We, the representatives of Russian's hacking underworld, can't tolerate Georgian's provoking, in all their manifestations. We want to live in a free world and free of aggressions and lies in web space. We don't need the orientation of authorities or other people's orientations, but to act in accord with convictions based on patriotism, of conscience and in believing on justice force. You can call us cyber-criminals and terrorists, triggering a war and killing people. But we will fight and it's unacceptable the aggression against Russian Federation on internet.*
> *We demand the end of attacks in what regards to field of information and means, and call to all media and journalists to cover the events objectively. Until situation changes, we will stop the divulgation of false information from occidental governments and from Georgian's government and media. We appeal to all that aren't indifferent to the lies of websites political Georgian's to contribute, all, who are able to inhibit the propagation of black information. (Translated from www.stopgeorgia.ru).*

On the software section it was possible to download a tool to perform flood attacks with intent to perform an attack by DDoS (Distributed Denial of Service), an anonymization tool, a tool of saturation of telephone lines using a voice over IP software and a tool of mobile phone's saturation using the transmission of SMS (Short Message Service). This website appealed to an attack to a list of targets and called the Internet users to a special effort on the 13th of August, declared day of mourning for the victims of South Ossetia's invasion. The list of targets made available in the Website as well as their availability through the 13th to the 25th of August 2008 is displayed in table 1. Some of the websites changed their server's location to avoid the break of service, like television channel Rustavi2 (with frequent online transmissions), or to avoid the change of contents (defacement), like the website www.civil.ge, that was changed to include images that compared the Georgian's President to Adolf Hitler. It is important to refer that some of the websites were able, during the pick of attacks, to be temporarily available, whereby the table aims to provide the comparative state of the combat effects during the monitored days. Figure 1 shows the evolution of the intensity of the effects, some will take long to be solved once Georgia its a country that does not depend on the internet and, once the country has other priorities, many of the websites stays to rebuild although they had reassumed their control.

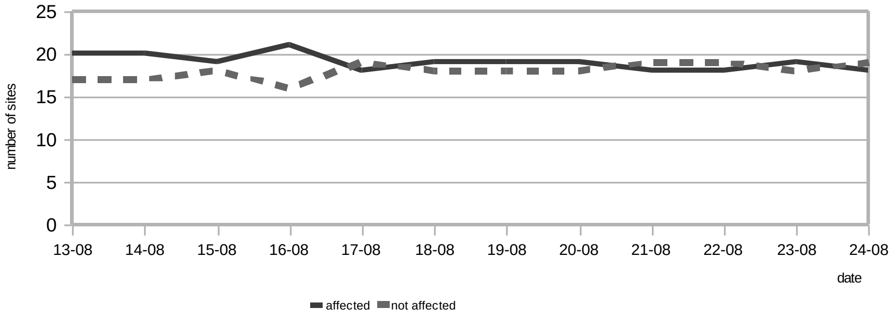


Fig. 1. Evolution of the attacks from 13/08/2008 to 24/08/2008

Some rumours say that Russian Business Networks (RBN), a criminal organization detected some years ago, are involved on those attacks diverting the traffic directed to Georgia through Russia. Once the access from Portugal to Georgia is usually made through Turkey, the dates on Table 1 do not reflect the eventual penalizations of performance that result from this type of attacks. Although, it was possible to verify, in some situations, that the access to websites on Georgia was made by Azerbaijan, via Russia, with no difficult. This study also used, for several times, a website of Russian's traceroute and there weren't significant differences, with respect to servers responses, on results obtained on accesses by Russian Federation when compared with those obtained from Portugal.

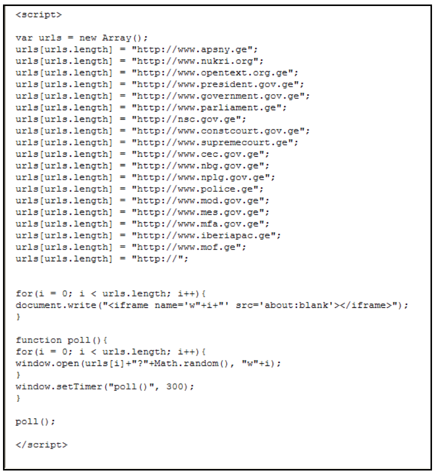
		State of the Website (checked between 17:30 ands 18:30, GMT)								
Domain	Location	13/08	14/08	15/08	16/08	17/08	18/08 to 20/08	21/08 and 22/08	23/08	24/08
parliament.ge	Georgia	Inactive						Not Affected		
assistancegeorgia.org.ge	Georgia	Very slow	Inactive	Very slow						

<table>
<tr><th colspan="2"></th><th colspan="9"><b><i>State of the Website (checked between 17:30 ands 18:30, GMT)</i></b></th></tr>
<tr><th><b>Domain</b></th><th>Location</th><th>13/08</th><th>14/08</th><th>15/08</th><th>16/08</th><th>17/08</th><th>18/08 to 20/08</th><th>21/08 and 22/08</th><th>23/08</th><th>24/08</th></tr>
<tr><td rowspan="2">cec.gov.ge</td><td>Georgia</td><td>Not Affected</td><td colspan="8">X</td></tr>
<tr><td>Holland</td><td>X</td><td colspan="8">Not Affected</td></tr>
<tr><td rowspan="2">mdf.org.ge</td><td>Holland</td><td>X</td><td colspan="2">Not Affected</td><td colspan="6">X</td></tr>
<tr><td>Georgia</td><td>Not Affected</td><td colspan="2">X</td><td>Inactive</td><td colspan="5">Not Affected</td></tr>
<tr><td>mfa.gov.ge</td><td>Estonia</td><td>Very slow</td><td colspan="8">Not Affected</td></tr>
<tr><td>corruption.ge</td><td>n/d</td><td colspan="9">Inactive</td></tr>
<tr><td>constcourt.gov.ge</td><td>Georgia</td><td colspan="3">Not Affected</td><td>Inactive</td><td colspan="5">Not Affected</td></tr>
<tr><td>insurance.caucasus.net</td><td>Georgia</td><td colspan="3">Not Affected</td><td>Inactive</td><td colspan="5">Not Affected</td></tr>
<tr><td>mc.gov.ge</td><td>n/d</td><td colspan="9">Inactive</td></tr>
<tr><td>nsc.gov.ge</td><td>Georgia</td><td colspan="9">“under construction”</td></tr>
<tr><td>supremecourt.ge</td><td>Georgia</td><td colspan="9">Not Affected</td></tr>
<tr><td>iberiapac.ge</td><td>Georgia</td><td colspan="9">Not Affected</td></tr>
<tr><td>court.gov.ge</td><td>Georgia</td><td colspan="9">“under reconstruction”</td></tr>
<tr><td>civil.ge</td><td>Estonia</td><td colspan="9">Not Affected</td></tr>
<tr><td>georgia.usembassy.gov</td><td>USA</td><td colspan="9">Not Affected</td></tr>
<tr><td>ukingeorgia.fco.gov.uk</td><td>United Kingdom</td><td colspan="9">Not Affected</td></tr>
<tr><td>all.ge</td><td>Georgia</td><td colspan="7">“under construction”</td><td colspan="2">Inactive</td></tr>
<tr><td>geres.ge</td><td>Georgia</td><td colspan="9">Not Affected</td></tr>
<tr><td>rustavi2.com.ge</td><td>USA</td><td colspan="3">Inactive</td><td colspan="5">Not Affected</td><td>Slow</td></tr>
<tr><td>opentext.org.ge</td><td>Germany</td><td colspan="9">Not Affected</td></tr>
</table>

<table>
<tr><th colspan="2"></th><th colspan="9"><b><i>State of the Website (checked between 17:30 ands 18:30, GMT)</i></b></th></tr>
<tr><th><b>Domain</b></th><th>Location</th><th>13/08</th><th>14/08</th><th>15/08</th><th>16/08</th><th>17/08</th><th>18/08 to 20/08</th><th>21/08 and 22/08</th><th>23/08</th><th>24/08</th></tr>
<tr><td>svobodnaya-gruzia.com</td><td>Georgia</td><td>Not Affected</td><td>Inactive</td><td>Not Affected</td><td>Inactive</td><td colspan="5">Not Affected</td></tr>
<tr><td>sanet.ge/gtze</td><td>Georgia</td><td colspan="9">Inactive</td></tr>
<tr><td>messenger.com.ge</td><td>Georgia</td><td colspan="9">Not Affected</td></tr>
<tr><td>primenewsonline.com</td><td>USA</td><td colspan="8">Inactive</td><td>Not Affected</td></tr>
<tr><td>presidpress.gov.ge</td><td>Georgia</td><td colspan="9">White page</td></tr>
<tr><td>sakinform.ge</td><td>n/a</td><td colspan="9">Inactive</td></tr>
<tr><td>sakartvelo.ru</td><td>n/a</td><td colspan="9">Inactive</td></tr>
<tr><td>internews.ge</td><td>Georgia</td><td colspan="9">Inactive</td></tr>
<tr><td>internews.org.ge</td><td>Georgia</td><td colspan="9">Inactive</td></tr>
<tr><td>interpressnews.ge</td><td>Georgia</td><td>Slow</td><td colspan="2">Very slow</td><td>Not Affected</td><td colspan="5">Slow</td></tr>
<tr><td>internet.ge</td><td>Georgia</td><td colspan="9">Not Affected</td></tr>
<tr><td rowspan="2">stream.ge</td><td>Georgia</td><td colspan="3">Not Affected</td><td colspan="6">X</td></tr>
<tr><td>Holland</td><td colspan="3">X</td><td colspan="4">Not Affected</td><td colspan="2">Inactive</td></tr>
<tr><td>presa.ge</td><td>Georgia</td><td colspan="9">Not Affected</td></tr>
<tr><td>medianews.ge</td><td>Georgia</td><td colspan="5">Not Affected</td><td colspan="3">Slow</td><td>Not Affected</td></tr>
</table>

Table 1. Situation, along the conflict, of the websites listed as preferential targets

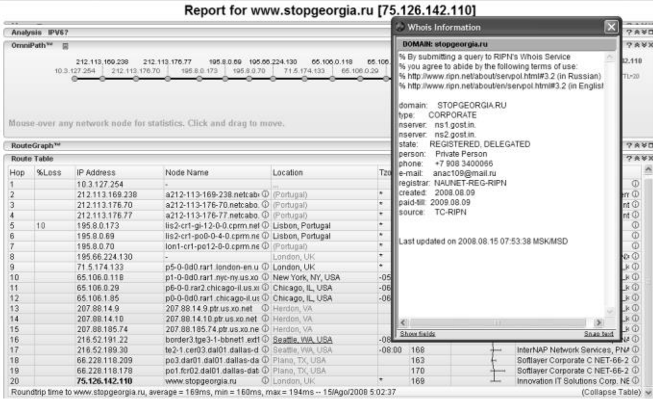
Also in some Russian language *fora* an appeal to combat was made. The majority limited the actions to the dissemination of links to www.stopgeorgia.ru, but some made other attack resources available. That is the case of http://clubs.ya.ru that proposes the creation of a batch to automatically send ping requests to the targets defined in stopgeorgia.ru; and of http://aeterna.ru that made available a link to an html file (Figure 2) that accesses the targets and, through an automatic update of the page, possible in some browsers, floods the targeted servers.



```
<script>

var urls = new Array();
urls[urls.length] = "http://www.apsny.ge";
urls[urls.length] = "http://www.nukri.org";
urls[urls.length] = "http://www.opentext.org.ge";
urls[urls.length] = "http://www.president.gov.ge";
urls[urls.length] = "http://www.government.gov.ge";
urls[urls.length] = "http://www.parliament.ge";
urls[urls.length] = "http://nsc.gov.ge";
urls[urls.length] = "http://www.constcourt.gov.ge";
urls[urls.length] = "http://www.supremecourt.ge";
urls[urls.length] = "http://www.cec.gov.ge";
urls[urls.length] = "http://www.nbg.gov.ge";
urls[urls.length] = "http://www.nplg.gov.ge";
urls[urls.length] = "http://www.police.ge";
urls[urls.length] = "http://www.mod.gov.ge";
urls[urls.length] = "http://www.mes.gov.ge";
urls[urls.length] = "http://www.mfa.gov.ge";
urls[urls.length] = "http://www.iberiapac.ge";
urls[urls.length] = "http://www.mof.ge";
urls[urls.length] = "http://";


for(i = 0; i < urls.length; i++){
document.write("<iframe name='w"+i+"' src='about:blank'></iframe>");
}

function poll(){
for(i = 0; i < urls.length; i++){
window.open(urls[i]+"?"+Math.random(), "w"+i);
}
window.setTimer("poll()", 300);
}

poll();

</script>
```

Fig. 2. Source code of the webpage distributed to perform the attacks.

The website also provides a list of proxy servers (including some only available to computers located on the Russian Federation) and a list of Georgia's websites vulnerable to attacks by SQL injection, explaining for each case the way to proceed to obtain the desired results. We can conclude that part of the attacks was organized with few resources although, as we can see on Table 1, the effects are significant. Once Georgia's government accused the Russia Federation of being responsible by those actions [7] it is important to try to understand who is the responsible for these websites. This is a difficult job to do but, in this case, it's facilitated by the existence of a website dedicated to this cyberwar. A traceroute and a consult to a whois server, indicates that it is a domain located in the United Kingdom under claimed responsibility of someone with the e-mail address anac109@mail.ru, with a contact telephone number from Irkutsk, on Siberia (Figure 3). Some researches in a few search engines provided the information that this e-mail address was used to register other domains: dokim.ru and rakar.ru (Figure 4), both based in the United States of America. This information allowed us to find out some more data related to the owner of the domain, like his alleged name: Andrej V. Uglovatyj that, of course, it's probably false, mainly if we consider the subject of the domain dokim.ru: sell false passports! In fact, this website sells passports from Russia Federation (supposedly lawfully issued) and from some European countries namely Lithuania, Leetonia, United Kingdom and Germany. The price of one passport from European Union varies between 3000€ and 3500€. The domain rakar.ru has illicit objectives too: to sell plastic cards with magnetic stripe with the data of legitimate credit cards and respective PIN codes. Those data are obtained illegally and sold, according with the quantity bought, by unit value between US$70 and US$450.



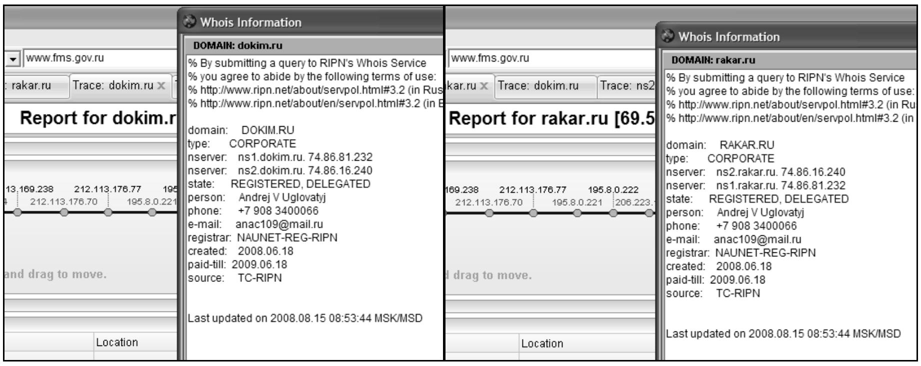
Hop	%Loss	IP Address	Node Name	Location	Tz		
1		10.3.127.254	-	...			
2		212.113.169.238	a212-113-169-238.netcab	(Portugal)	*		
3		212.113.176.70	a212-113-176-70.netcabo.	(Portugal)	*		
4		212.113.176.77	a212-113-176-77.netcabo.	(Portugal)	*		
5	10	195.8.0.173	lis2-cr1-gi-12-0-0.cprm.net	Lisbon, Portugal	*		
6		195.8.0.69	lis2-cr1-po0-0-4-0.cprm.ne	Lisbon, Portugal	*		
7		195.8.0.70	lon1-cr1-po12-0-0.cprm.ne	(Portugal)	*		
8		195.66.224.130	-	London, UK	*		
9		71.5.174.133	p5-0-0d0.rar1.london-en.u	London, UK	*		
10		65.106.0.118	p1-0-0d0.rar1.nyc-ny.us.xo	New York, NY, USA	-05		
11		65.106.0.29	p6-0-0.rar2.chicago-il.us.x	Chicago, IL, USA	-06		
12		65.106.1.85	p0-0-0d0.rar1.chicago-il.us	Chicago, IL, USA	-06		
13		207.88.14.9	207.88.14.9.ptr.us.xo.net	Herdon, VA			
14		207.88.14.10	207.88.14.10.ptr.us.xo.net	Herdon, VA			
15		207.88.185.74	207.88.185.74.ptr.us.xo.ne	Herdon, VA			
16		216.52.191.22	border3.tge3-1-bbnet1.ext1	Seattle, WA, USA	-08		
17		216.52.189.30	te2-1.cer03.dal01.dallas-d	Seattle, WA, USA	-08:00	168	InterNAP Network Services, PN
18		66.228.118.209	po3.dar01.dal01.dallas-da	Plano, TX, USA		163	Softlayer Corporate C NET-66-2
19		66.228.118.178	po1.fcr02.dal01.dallas-dat	Plano, TX, USA		170	Softlayer Corporate C NET-66-2
20		**75.126.142.110**	www.stopgeorgia.ru	London, UK	*	169	Innovation IT Solutions Corp. NE

Roundtrip time to www.stopgeorgia.ru, average = 169ms, min = 160ms, max = 194ms -- 15/Ago/2008 5:02:37

DOMAIN: stopgeorgia.ru

```
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in Englist

domain:    STOPGEORGIA.RU
type:      CORPORATE
nserver:   ns1.gost.in.
nserver:   ns2.gost.in.
state:     REGISTERED, DELEGATED
person:    Private Person
phone:     +7 908 3400066
e-mail:    anac109@mail.ru
registrar: NAUNET-REG-RIPN
created:   2008.08.09
paid-till: 2009.08.09
source:    TC-RIPN


Last updated on 2008.08.15 07:53:38 MSK/MSD
```

Fig. 3. stopgeorgia.ru domain’s owner and location



DOMAIN: dokim.ru

```
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Rus
% http://www.ripn.net/about/en/servpol.html#3.2 (in E

domain:    DOKIM.RU
type:      CORPORATE
nserver:   ns1.dokim.ru. 74.86.81.232
nserver:   ns2.dokim.ru. 74.86.16.240
state:     REGISTERED, DELEGATED
person:    Andrej V Uglovatyj
phone:     +7 908 3400066
e-mail:    anac109@mail.ru
registrar: NAUNET-REG-RIPN
created:   2008.06.18
paid-till: 2009.06.18
source:    TC-RIPN


Last updated on 2008.08.15 08:53:44 MSK/MSD
```

DOMAIN: rakar.ru

```
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Ru
% http://www.ripn.net/about/en/servpol.html#3.2 (in

domain:    RAKAR.RU
type:      CORPORATE
nserver:   ns2.rakar.ru. 74.86.16.240
nserver:   ns1.rakar.ru. 74.86.81.232
state:     REGISTERED, DELEGATED
person:    Andrej V Uglovatyj
phone:     +7 908 3400066
e-mail:    anac109@mail.ru
registrar: NAUNET-REG-RIPN
created:   2008.06.18
paid-till: 2009.06.18
source:    TC-RIPN


Last updated on 2008.08.15 08:53:44 MSK/MSD
```

Fig. 4. dokim.ru and rakar.ru domain’s owner and location

Analysing those facts, it is very provable that who ever as coordinated the cyberattack is not related with any official entity of Moscow. This indicates that there are other identities capable to mobilize the necessary means to successfully attack governmental websites, using attacks by DDoS or exploring vulnerabilities, such as SQL injections. As a matter of fact, in a message in the forum of website www.stopgeorgia.ru it could be read: “DDoS attacks have limited effects. We should find vulnerabilities and use it. DDoS just as a last resource”. Another possibility, raised by some analysts in the period of the attack to Estonia [8] is the use by the Russian Federation of the oriental strategy called “people’s war”, where the government’s role is to protect their citizens that, on their own, decide to get involved in a combat while, simultaneously stimulating nationalist feelings [9][10].

Conclusions

The case of the cyberattack to Georgia shows, that the attacks to the information systems of a government can be used by other states or nationalist groups from rival countries to paralyze the public services or, at least, stop the general citizen from accessing the Internet, for instance to provide information that can reach the international community. The studied case seems to be the first to simultaneously use a cyberwar aiming the civilian infrastructure and a military conventional intervention. This concept of cyberwar is a mix of the Maoist concept of "people's war" and the Trotsky's combat strategy, where specialized groups attack critical targets (power stations, communication infrastructures, etc.) expecting that the general public will then support the military action, instead of expecting their help to perform the actual action.

Countries that are changing their processes in a way that make them more and more dependent on the informational infrastructures, need to consider the cyberspace as another frontier that requires security measures that can guarantee their national interests.

References

1. Arquilla, J., & Ronfeldt, D.; Cyberwar is Coming! In J. Arquilla & D. Ronfeldt (Eds.), *Athena's Camps: Preparing for Conflit in the Information Age* (pp. 23-60). Santa Monica, California: RAND Corporation (1997).
2. DSCINT; Cyber Operations and Cyber Terrorism, DCSINT, (Vol. 1). Fort Leavenworth, Kansas: DCSINT (2005).
3. Oliveira, F. N. S. C.. Ações Maliciosas Sobre Redes e Sistemas de Informações, I Conferência Internacional de Perícias em Crimes Cibernéticos. Brasília: Federal Police Department (2004).
4. Bezerra, E. K., Nakamura, E. T., Lima, M. B., & Ribeiro, S. L.; O Espaço Cibernético e Seu Emprego Como Agente de Instabilidade de Uma Nação: Uma Visão Sobre Guerra Cibernética, I Conferência Internacional de Perícias em Crimes Cibernéticos. Brasília: Departamento de Polícia Federal (2004).
5. Shimeall, T., Williams, P., & Dunlevy, C.; Countering cyber war. Nato review, 16-18. (2002).
6. European Parliament.. Session of the European Parliament of 9th of May 2007, Retrieved 2007, from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20070509+ITEM-012+DOC+XML+V0//PT (2007)
7. "Georgia accuses Russia of waging cyberwar" (2008, 12th of August of 2008). CBC News. (2008).
8. Ottis, R.. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, 7th European Conference on Information Warfare and Security. Plymouth, UK. (2008).
9. Wu, C.; An Overview of the Research and Development of Information Warfare in China. In Edward Halpin *et al* (eds.) Cyberwar, Netwar and the Revolution in Military Affairs. Palgrave MacMillan, Hampshire, pp 173-195. (2006).
10. Jincheng, W.; "Information War: A New Form Of People's War." In Michael Pillsbury (eds) (1997) Chinese Views Of Future Warfare. National Defense University Press, Washington, pp 409 – 412. (1997).