

## State-sponsored Cyber Terrorism: Georgia's Experience

Khatuna Mshvidobadze

Presentation to the Georgian Foundation for Strategic and International Studies

Tbilisi, Georgia

September 29, 2011

### WHAT IS CYBER TERRORISM?

- To a large degree, classification of cyber acts depends on the circumstance and the intent of the perpetrator.
  - This is especially so when, as in the case of Russian attacks on Georgia, the same people, computers and techniques are used for multiple purposes.
  - Some things are pretty easy to define:
    - Cyber hooliganism—making an image of the devil appear on your screen or erasing documents stored in your computer.
    - Petty cyber-crime—I'm stuck in London; please send \$2,000.
    - Even greater cyber-crimes—stealing credentials to clean out bank accounts.
    - Or cyber espionage—exploiting a vulnerability to steal information.
      - The definition is clear even when the precise objective and attribution are not—for example, the recent hacking of Lockheed Martin, L-3 and possibly other US defense contractors; or the 2003 Titan Rain attacks on US military systems.
        - Pictured here is a drawing of the new US Department of Homeland Security Headquarters—some believe that the recent intrusions at Lockheed and others were in search of plans for this building.
        - But even if we don't know who did it or precisely what they were after, we know that someone exploited a vulnerability to steal information.



- Definitions get harder with more sophisticated schemes run by criminal syndicates such as Russian Business Network (RBN).
  - RBN, now evaporated, or at least invisible, was a Russian cyber criminal group known to have been a key player in the 2008 attacks on Georgia.
  - A particular botnet could be used to spam pharmacy fraud one day and to debilitate the critical infrastructure of a neighboring country on the next day.

Copyright © 2011, Khatuna Mshvidobadze

- Pictured below are the Gardabani gas-fired power plant, not far from Tbilisi and a screen-grab from one of RX-Promotion’s many online pharmacy scams.
- Criminal systems could be used to sell bogus Viagra to a gentleman in Topeka on one day and to black out Georgia’s capital city for geopolitical purposes on the next day.
- By the way, Pavel Vrublevsky, the principle in RX-Promotions, was recently arrested in Russia—NOT, of course, for his pharmacy scams, but because he ran afoul of more powerful Russian vested interests.
- So I think that the best definition of cyber terrorism is, “cyber acts designed to foment terror or demoralization among a target population for some purpose of the perpetrator.”
  - Most likely this will be some kind of attack on critical infrastructure.
    - To use a conventional analogy, a terrorist bomb could explode on a deserted road or next to a security wall, by accident or just to make a point. It is more likely, however, to be directed at something or someone. GRU, Russian military intelligence, has carried out both kinds of explosions on Georgian territory.
    - Similarly, cyber-terrorism could involve sterile website defacements, but more likely—or what we should worry about, at least—are attacks on critical infrastructure.
  - Here I want to add three qualifiers to that definition.
    - First, some attacks could have dual effects: debilitating a country’s financial system, government communications, air traffic control or critical supervisory control and data acquisition (SCADA) systems may spread terror AND also do concrete damage.
    - Second, acyber attack does not need to go BOOM to be cyber terrorism, sabotage or even war.
      - Of course, there is a natural human reliance on the visual—a gaping hole in a nuclear containment facility grabs the senses more than a stopped commuter train.
      - And for us in Georgia, these pictures of Russian attacks on civilian apartments in Gori will remain imprinted on our minds forever—the image of a frozen bankomati machine simply cannot compare.





- Or consider the differing human reactions to an image of a mother trying to protect her baby daughter to one of clear blue sky—a sky without airplanes because air traffic control and air navigation systems are shut down.
- But we are too reliant on pre-cyber notions of war and terror—a non-kinetic attack could emerge to be more harmful than a kinetic one.
- Third, I think we must apply to the cyber realm a distinction made in the terrorism realm—there could be non-state and state-sponsored cyber terrorism.
- I do not mean to suggest that this is the only concern, but here in Georgia, our primary cyber terrorist concern is state-sponsored attacks that can spread terror AND do concrete damage, that may or may not go BOOM, for the purpose of undermining our independence.
  - In Georgia, we have experienced a lot of this already.
  - We have seen plain acts of state-sponsored terrorism—the bombing of a Gori police station in 2005 and exploded gas and electricity lines, most recently in 2006.

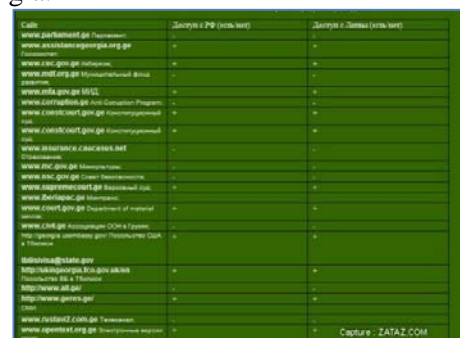
**2008: THE FIRST EVER COMBINED CYBER AND KINETIC WAR**

- AND we were attacked in the first ever combined cyber and kinetic war.
- Although I cannot now go through a full account, here is a summary of the cyber attacks against Georgia in 2008:
  - Early (began July 20) defacements of Georgian Government websites.
  - Distributed Denial of Service (DDoS) attacks.
  - Internet blockade.
  - Well organized hacktivism.
  - Fake BBC and CNN reports.
    - “name.avi.exe” Trojan.
  - August 27 DDoS attack—NOTE that this was two weeks after the so-called ceasefire.
- Here are some illustrations:



- In the first, you see one of the defacements of the President’s web site—a slide show depicting our president, Mikheil Saakashvili, as Hitler.
- Next is a screen grab from StopGeorgia.ru with a list of Georgian targets by type. This went online on August 8, just as Russian tanks rolled into Georgia.

- Other pages contained instructions for people with average computer skills.
- Targets for organized hacktivists included:
  - Government.
  - NGOs.
  - Insurance company.
  - News.
  - US Embassy.
  - UK Embassy.

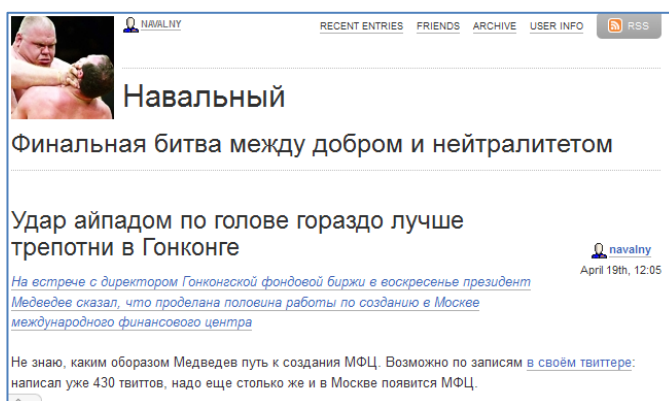


- StopGeorgia.ru was registered by Naunet, a registrar known to register sites for all kinds of criminal activity. It was involved with Innovation IT Solutions and Softlayer Technologies, both connected with Russian organized crime.
  - I mention this not to get into many details, but to point out that cyber forensics work, and we do know who did this.
  - Finally, is a scareware screen that popped up in fake BBC News reports offering disinformation about President Mikheil Saakashvili.
    - If you clicked on it, it dumped the “name.avi.exe” trojan into your computer.
- Internet traffic to and from Georgia was blocked or severely limited.
  - The 5 autonomous systems involved were associated with criminal syndicate Russian Business Network (RBN). (Autonomous systems are linked to blocks of Internet Protocol addresses.)
    - AS8342, RTCOMM.
    - AS28753, ROSTELCOM.
    - AS9121, TTNET..
    - AS8359, COMSTAR
    - AS18631, Moscow Internet Exchange.
- Again, I mention this, not complicate things, but to show that we do have a good idea about who attacked us.
- Moreover, you have to consider the context and timing of a cyber attack—in our case, the cyber attacks were coordinated with a very visible kinetic war.
- Considering all this, we can say beyond a reasonable doubt that Russia directed the cyber-attacks on Georgia, operating through Russian organized crime and well organized hacktivists.
- By the way, at the time, most Georgian Internet traffic went directly through Russia.
  - Since 2008, the Poti – Varna “Caucasus” fiber-optic cable handles about 90% of Georgia’s Internet traffic.
  - Pictured here is the laying of the Caucasus cable.



## **FROM EXTERNAL AGGRESSION TO INTERNAL REPRESSION**

- More recently, Russian domestic opposition has been targeted for cyber-attacks.
- The fingerprints of Russian organized crime are also all over the recent DDoS attacks on LiveJournal and Novaya Gazeta.
- LiveJournalblogsite is popular with critics of the regime such as Alexey Navalny.
  - Pictured here is Navalny’s blog alleging corruption in Transneft.
  - Boris Nemtsov, People’s Freedom Party leader, had planned to publish new report “Putin. Corruption” on LiveJournal.
- NovayaGazeta is newspaper that covers political & social affairs of Russia.
  - It is best known for its journalist Anna Politkovskaya, murdered in 2006.
  - Its most recent project is “ Online Parliament of Runet.”



- This is how the attack proceeded:
  - March 24: Navalniy's LiveJournal blog site was attacked.
  - March 26: Rospil.info, a Navalniy website was attacked.
  - April 4: LiveJournal was broadly attacked.
  - April 7-8: Novaya Gazeta was attacked.
- Boris Nemtsov said, "Hardly anyone could have done this other than the security services"
- Kaspersky Labs wrote that at least 2 botnets associated with Russian organized crime were involved, in particular, "Darkness."
- Many in Moscow point to some part of government linked to organized crime through the Kremlin's youth group *Nashi*.
- Sub-contracting cyber attacks to criminal syndicates and youth groups is super cost-effective.
  - The state does not have to buy equipment or recruit, train, pay and retain personnel—people and equipment are engaged in profitable activities when not needed by the state.
  - And it further confuses attribution.
    - Although with common sense and analysis one can eventually make attribution, relevant-time attribution is still a challenge.
    - Using criminals and kids adds another layer of analysis and another note of doubt about who the ultimate organizers were.
- By the way, just 2 weeks ago, a new youth group, apparently organized by *Nashi* leaders, was launched as "the nation's conscience on the Internet."
- On the same day, Russian Prosecutor General Yury Chaika told his CIS counterparts, "You saw what happened in London... In my opinion, the problem is evident and we need to bring social networks under reasonable control – simply to protect citizens' freedoms."
- Last February, Russian President Dmitry Medvedev made this statement to a security gathering in Southern Russia.
  - "Look at the situation that has unfolded in the Middle East and the Arab world. It is extremely bad. There are major difficulties ahead... We need to look the truth in the eyes. This is the kind of scenario that they were preparing for us, and now they will be trying even harder to bring it about."
- Moscow is concerned about:
  - Arab Spring.
  - London riots.
  - North Caucasus unrest.
  - Upcoming Duma and presidential elections.
- Internationally, Russia pushes restrictions on broadcast of information, including Internet communications, that could undermine state sovereignty.
  - They have used the Shanghai Cooperation Organization (SCO) to craft agreements to monitor and restrict information.
  - They have submitted draft UN resolutions to similar effect each year since 1999.
  - This year, Russia joined with China, Tajikistan and Uzbekistan to propose an international Internet code of conduct.
- We cannot predict the future, of course, but we can see that Russia is:
  - Very concerned about information warfare and is working the problems up to the highest levels.
  - Actively considering information warfare, including cyber warfare, at home and abroad.
  - Improving its capabilities and organization.

## LOOKING FORWARD

- Of course, we are wary of another combined attack.
- And, by the way, we must not discount the possibility of advances in cyber technology leading to the possibility of all-out cyber-only war.
- But we must also not dismiss the possibility of a state-sponsored cyber terrorism campaign waged to undermine our country and designed to thwart relevant-time attribution.
  - Its objectives could be to:
    - Discourage the population.
    - Aid Russian-supported internal opposition.
    - Discredit the elected government.
    - Discourage investment in Georgia.
    - And generally to create the image of Georgia as a mess that no one would want to touch.
- We must assume that such a campaign would feature improved techniques—both technical and sociological—based upon lessons learned in 2008 and from around the world since then.
  - For example, since Israeli Operation Cast Lead in Gaza in 2008 – 2009 and subsequent events in the Middle East, we must assume that there will be significant use of social network sites by multiple sides.
- We must further assume that Russia will refine its use of cyber criminal syndicates and youth groups such as *Nashi*.
  - Although Nashi has apparently recently lost some funding and overt political support, its fingerprints were on the March-April attacks on Russian domestic political opposition. So, for now, it is reasonable to assume that the *Nashi* cyber connection remains.
- Externally, Moscow has not lashed out at its neighbors—with kinetic or cyber attacks—for over two years. However, it would be naïve to believe that it has given up the will or the means to carry out such attacks. It is reasonable to assume that Russia’s offensive cyber capabilities stand improved, willing and able.
- By the way, war without tanks—or at least minimizing tanks—has been a Russian objective since the early cyber era.
  - For example, here is a 1996 statement of General-Colonel Viktor Nikolaevich Samsonov, then Acting Chief of General Staff, which roughly presaged what happened in 2008:
    - “The high effectiveness of ‘Information Warfare’ systems in combination with highly accurate weapons and ‘non-military means of influence’ makes it possible to disorganize the system of state administration, hit strategically important installations and groupings of forces, and affect the mentality and moral spirit of the population. In other words, the effect of using these means is comparable with the damage resulting from weapons of mass destruction.”
  - And here is what the 2010 Russian Military Doctrine says:
    - “Prior implementation of measures of informational warfare in order to achieve political objectives without the utilization of military forces.”



## **WHAT TO DO?**

- So what is a small country like Georgia to do?
- After the 2008 attack, our new National Security Concept, threat assessment, etc. have all been revised.
- The Georgian Government created the Data Exchange Agency, which is creating a Georgian CERT.
- And we are engaged in cooperation with like-minded countries.
  - With regard to international cooperation, we must not be beguiled by notions of universal norms or a “cyber Geneva Convention.” These will not work so long as certain major countries, like Russia, prefer to use cyber criminals rather than to prosecute them. Instead, we should stick to solid fundamentals such as the European Convention on Cyber Crime and combining with like-minded countries to build resilience to attack.
    - By the way, Georgia has signed the Convention, but not ratified it yet—it should proceed to ratify this important treaty.
- In Georgia, we are:
  - Defining critical infrastructure.
  - Crafting new legislation.
  - Forging unprecedented cooperation between government and industry.
  - Increasing cyber awareness.
  - Taking advantage of educational programs.
  - Cooperating with like-minded countries.

## **CONCLUSION**

- The bottom line is that Georgia did fend off the 2008 attacks. It is working to defend itself now. And, particularly if like-minded countries work together, much more is possible.