Georgia 2008: Why We Need National and NATO Cyber Defense Policies

- The 2008 Russian cyber attack on Georgia, an improved version of Moscow’s 2007 cyber-assault on Estonia, along with the recent (thus far unattributed) appearance of the Stuxnet worm and several other instances, was a clear signal that cyber-war is here and here to stay.
- What distinguishes the 2008 Russia-Georgia war, however, is that the cyber campaign was fully integrated with a full-scale kinetic war waged on land, sea and in the air.
- This is not to say that all cyber attacks will henceforth be associated with kinetic ones—there are and there will be many variants.
- However, the reverse is likely true: all but the simplest brush wars—which are, admittedly, a lot—will have a cyber dimension.
- The 2008 Russia-Georgia war was the first instance of a cyber campaign integrated into a kinetic war, but it will not be the last.
- To review, these were the basic elements of Russia’s 2008 cyber attack on Georgia:
  - Early (July) defacements of Georgian Government websites, particularly www.president.gov.ge
  - Widespread distributed denial of service (DDoS) attacks
  - Internet blockade
  - Well organized “hacktivism”
  - Fake BBC and CNN reports…
    - …incorporating the “name.aci.exe” trojan
  - A final (September 27) DDoS attack
- Likely objectives were to
  - Prepare the battlefield
  - Blind the target government
  - Prevent broadcast of accurate information
  - Delay international response
  - Disrupt the economy and create uncertainty
  - Disorient the population and damage morale
  - Blunt any efforts to mount a coherent defense
Without going blow-by-blow through either the cyber or the kinetic war, I shall draw from them a few general observations.

FIRST—make no mistake—the campaign just outlined was part of a long and well prepared war. This war did not begin in early August! Consider these Russian actions:

- May—heavily armed “peacekeepers” deployed in Georgian territories
- May—Railroad Troops deployed to repair the Sukhumi-Ochamchire, Abkhazia line upon which the Russian western front would depend
- May—improvements at the Gudauta, Abkhazia air base
- June-July—military exercises scripted to prepare for invasion of Georgia and to cover marshalling of forces
- July—overt airspace violations
- July-August—troop deployments and pre-positioned supplies
- July-August—cyber attacks. In the cyber dimension, the following had already been accomplished at that time:
  - Reconnaissance
  - Mapping
  - Attack scripts
  - New domain registrations
  - New websites construction
- Preparation—cyber and kinetic—had to have started long before the spring of 2008.
  - The bottom line: the Russian attack on Georgia, including its cyber dimension, was long and well prepared from about the time of the Kosovan declaration of independence in February, 2008.

SECOND, the cyber attacks on Georgia in 2008 represented improvements over the 2007 attacks on Estonia.

- In an August 2009 report, the US Cyber Consequences Unit (US-CCU), an independent research institute, writes, “These HTTP-based attack tools were tested by the US-CCU in a laboratory environment and proved far more effective than the ICMP-based attacks that the Russians had used on Estonia.”

THIRD, the Russian Government and Russian organized crime, particularly the Russian Business Network (RBN) worked in close coordination.

- US-CCU writes:
  - “The cyber attacks against Georgian targets were carried out by civilians with little or no direct involvement on the part of the Russian government or military.”
  - “The attackers displayed a convincing amount of disorder without being at all random.”
  - “The organizers of the cyber attacks had advance notice of Russian military intentions…”
  - “The civilian cyber attackers were aided and supported in their efforts by Russian organized crime.”
  - “It appears that Russian criminal organizations made no effort to conceal their involvement in the cyber campaign against Georgia because they wanted to claim credit for it.”

This is a common sense, historical attribution.

- Given all the circumstances of Russia’s attack on Georgia, and results of considerable investigation after the fact, the conclusion that the Russian Government, using Russian organized crime and “hacktivists,” directed a cyber campaign against Georgia is unexceptionable
- That said, this does not solve the near-real-time, actionable attribution problem characteristic of cyber attacks.
There are some further interesting observations about cyber-criminals, particularly about RBN:

- The servers and botnets used in the attacks on Georgia are associated with Russian criminal organizations; indeed, some even participated in criminal attacks on E-commerce sites during the campaign.
- RBN faded from view soon after the war to the point that some commentators criticized Georgian officials for harping upon an apparently defunct organization.
  - Yes, criminal organizations, by nature, fade, morph and reappear, but the greedy, unscrupulous people behind them remain.
    - Some of the people behind RBN are also behind Canadian Pharmacy, rated the number one worst spammer in the world by Spamhaus, an international non-profit organization that tracks Internet spamming operations. (See [http://www.spamhaus.org/statistics/spammers.lasso](http://www.spamhaus.org/statistics/spammers.lasso), accessed November 13, 2010).
    - By the way, RBN seems recently to have reappeared!

- FOURTH, in the Russia-Georgia war, Russian cyber attacks not only complemented the kinetic war, some cyber-actions actually substituted for kinetic war.
  - I am indebted for this point to Khatuna Mshvidobadze whose presentation, *New Threats: Energy Security, Cyber Defense, Critical Infrastructure Protection* is now part of the official bibliography for NATO’s new *Strategic Concept*.
  - Some types of cyber-attack performed new or different missions.
  - However, some cyber attacks were just new ways of good, old-fashioned warfare that in earlier times would have been assigned to
    - Artillery
    - Air interdiction
    - Spetsnaz or special forces
  - US-CCU writes, “The news media and communications facilities, which would ordinarily have been attacked by missiles or bombs during the first phase of an invasion, were spared physical destruction, presumably because they were being effectively shut down by cyber-attacks.”
  - In this sense, cyber attacks are indeed armed attacks.

- So, considering the Russia-Georgia war, we can see that
  - Cyber war has become an integral part of war; it is simply a new dimension, just as sea, air and outer space were in earlier times.
  - At least some aspects of cyber-warfare, at least under some circumstances, are equivalent to armed attacks.
  - When cyber-warfare is part of kinetic war, cyber-activity may provide indications of war to come.
  - We must act now.

- This is not a startling revelation, but cyber-technology—offense and defense—is out ahead of cyber-policy.

- Policy is needed to guide us in
  - What to do
  - Particularly on what to spend limited resources
  - For what to look
  - What to do when we see it
  - Equally important, what we shall not do when we see it
  - Formulating declaratory policy, which is an important aspect of our response to this new challenge.
For example, a major step forward would be a firm declaration from major countries and/or NATO that we would regard the emplacement of logic bombs or trapdoors in security-related and critical infrastructure computer networks as a hostile act.

- Of course, this would not resolve the technical challenges of finding hidden logic bombs and trap doors and attributing them to a particular state or group.
- It would, however, marshal the efforts of democratic countries to find and attribute malware in their critical networks.
- And it would put cyber malefactors on notice that there could be consequences—better left unspecified—to their actions.
- Such a NATO declaration would be particularly potent if coupled with a statement that a cyber attack upon a NATO member could be considered an Article 5 attack under the North Atlantic Treaty.

Another idea for useful declaratory policy would be to say that with regard to attacks on our security-related and critical infrastructure computer networks, we hold any state responsible for what happens inside its borders, even if it is not the author of the attack. This would not guarantee success but it would establish the presumption that each state must

- Establish the means—legal and practical—to police the bits of cyberspace under its jurisdiction
- Cooperate reasonably with any legitimate request for investigation or assistance

Without cogent, coherent policy, we risk

- Mistaking our objectives
- Squandering resources
- Losing (or not gaining) political support and funding
- Chaos

While details must remain secret, most of the policy debate must, by definition, be a public debate.

- Although circumstances and details vary, there is precedent in the debate about nuclear weapons policy—the broad aspects of policy were developed publicly. In this sense, frankly, the cyber community must grow up.

We must develop policies national and international.

I shall sidestep national discussions except to say that there have been positive steps, but much remains to be done.

- In Georgia, the Government is beginning to formulate policy and has taken a concrete step with the creation of the Data Exchange Agency.
- The US is farther ahead, but there is far more to do. Recent steps include formation of US Cyber Command and publication of parts of the Comprehensive National Cybersecurity Initiative.

Instead, I shall concentrate on the need for international cyber-defense policy, particularly in NATO.

The cyber challenge is

- Transnational
- Big
- Common to all democratic countries

For western countries, NATO has six decades of experience in international security cooperation and interoperability. Therefore—of course, in cooperation with other organizations—it is the right organization to take the lead internationally.
• But, of course, NATO, too, has been on a learning curve that reflects growth in the cyber challenge.
  o The 1999 Strategic Concept mentioned
    ▪ Vulnerability of NATO IT systems
    ▪ Information superiority for military operations
  o The 2006 Comprehensive Political Guidance mentioned
    ▪ Need to protect IT systems against cyber attack (a step forward from 1999)
    ▪ Information superiority for military operations
  o The 2010 NATO 2020: Assured Security; Dynamic Engagement (Albright Group Recommendations) leans far more forward:
    ▪ “The next significant attack on the alliance may well come down a fiber-optic cable.”
    ▪ Ranks cyber with ballistic missiles and terrorism as one of top 3 threats
    ▪ Implies that a cyber attack could be an Article 5 event
    ▪ Says NATO mission could be broadened
    ▪ Recommends NATO consider pre-delegation of authority to the Secretary General or senior military commanders in case of a cyber-attack
    ▪ Recommends inclusion of both passive and active defenses in NATO strategy
• Looking toward the November 19-20 NATO Lisbon Summit that will approve the new Strategic Concept, it is doubtful that the alliance will reach consensus on
  o Pre-delegation
  o Active defense
    ▪ a debate on exactly what that means is already raging in the US
• Debate can continue on at least these two aspects. However, the Strategic Concept can be judged a cyber-success if it
  o Expands NATO’s mission to include cyber-defense
  o Contains robust language describing cyber threats and the need for cogent and coherent NATO responses
  o Recognizes that a cyber attack on a member state could be an Article 5 event
    ▪ Note the word “could.” In any case, the North Atlantic Council would have to decide unanimously to invoke Article 5.
  o There has been so much misinformation about this that it is worth presenting the entire first paragraph of Article 5:

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

  o Note that even in the case of an armed attack, the decision of what to do rests with each member state to take only “such action as it deems necessary.”
    ▪ Despite what some so-called experts have been saying, invoking Article 5 does not require a kinetic response; indeed, it does not require any response at all.
    ▪ Collective cyber defense—passive or active—is altogether consistent with Article 5.
  • Dispatching a NATO cyber rapid reaction team or re-hosting websites on different servers—roughly what was done on the fly for Georgia by Estonia and others—would be entirely consistent with Article 5.
- By the way, a kinetic response, if that is what the NAC unanimously decides, would not be precluded.
  - The new Strategic Concept or the summit declaration should also include a ringing endorsement of NATO’s Cooperative Cyber Defense Center of Excellence in Tallinn and a call for universal alliance support and participation.
- NATO’s objective should be to build the most resilient cyber posture possible.
  - Note that when I say NATO, I very much mean including key partner and aspirant states such as Georgia, which are vulnerable, but which can also add considerably to the alliance effort.
- So, there it is—we shall see the new NATO Strategic Concept on November 20.

###