SMALL WARS JOURNAL

smallwarsjournal.com

Cyberwar Case Study: Georgia 2008

by David Hollis

The Russian-Georgian War in August of 2008 represented a long history of geostrategic conflict between the two nations and was based on many complex factors: geopolitical, legal, cultural, and economic. The 1992 South Ossetia War and the 1993 Abkhazian War resulted in the loss of the regions from Georgia to internationally unrecognized, pro-Russian local governments. Tensions had been building in the region for several years prior-to the initiation of conflict in August 2008. The war officially started on 7 August 2008 after several weeks of growing arguments over the future of the South Ossetian territory. Georgian troops initiated a military attack against South Ossetia and began a massive shelling of the town of Tskhinvali in response to alleged Russian provocation. Russia deployed additional combat troops to South Ossetia and retaliated with bombing raids into Georgian territory. Russia deployed naval forces to formally blockade Georgia and landed naval infantry (marines) on Abkhaz coast (near Georgia). The decisive ground combat operation of the campaign resulted in mechanized Russian military and Ossetian militia forces defeating the more lightly armed Georgian military forces in the only large-scale major ground combat of the war (battle for the town of Tskhinvali). Georgian tactical military defeat at the battle of Tskhinvali, operational defeat via Russian uncontested invasion of the western part of Georgia, unchallenged naval blockade of Georgia, and Georgian difficulty getting their media message out to the world, led to Georgia's strategic defeat in the war. The conflict forced approximately 25,000 Georgian residents to flee from ground combat as refugees into internal displacement. The two countries signed a ceasefire agreement a week later but tensions remain high to this day. Russia has failed to implement some of the terms of the ceasefire agreement, resulting in further loss of Georgian territory to Russian occupation.[1]

As wars historically go, it wasn't very big, did not involve vast amounts of military forces, nor did it last long. One might argue that it was more of a typical battle or campaign framed in an on-going long term geopolitical cold war between the combatants, a cold war punctuated with occasional outbreaks of small to large scale violence. On the surface, it represents one of many cold wars (with periodic renewals of formal national-level military conflict) fought every day on the "near abroad" of the Russian periphery. A conflict which may not end for a very, very long time. But while much of that is true, a deeper analysis of the cyberspace domain operations conducted by both sides in this conflict indicate that image is

[1] Associated Press "Georgia Reports Attacks Continue as Russia's Medvedev Orders Troop Withdrawal" Fox News, (12 August 2008), found at: http://www.foxnews.com/story/0,2933,402043,00.html; Jon E. Chicky "The Russian-Georgian War: Political and Military Implications for U.S. Policy" Silk Road Studies Program policy paper (February 2009) found at: http://www.silkroadstudies.org/new/docs/Silkroadpapers/0902Chicky.pdf , and George Friedman "The Russo-Georgian War and the Balance of Power" STRATFOR (12 August 2008), found at: http://www.stratfor.com/weekly/russo_georgian_war_and_balance_power

illusory and incomplete.[2] The Russian-Georgian war was quite historic and precedent setting for several reasons.

This appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains (consisting of Land, Air, Sea, and Space). "…three weeks before the shooting war between Georgia and Russia began, online attackers started assaulting Georgia's websites. Since then, researchers have tried to find out who masterminded the network strikes - military electronic warriors, patriotic hackers, cyber-crooks - without finding anything definitive."[3] Nevertheless, "…Russia invaded Georgia on four fronts. Three of them were conventional - on the ground, through the air, and by sea. The fourth was new - their attacks via cyberspace ... It is, quite simply, implausible that the parallel attacks by land and by cyberspace were a coincidence - official denials by Moscow notwithstanding."[4] The (alleged) Russian attack upon the Georgia's military and government networks was highly successful. "It seems that 54 web sites in Georgia related to communications, finance, and the government were attacked by rogue elements within Russia ... So as tanks and troops were crossing the border and bombers were flying sorties, Georgian citizens could not access web sites for information and instructions."[5] Georgian authorities discovered their Internet access and communications networks to be exceptional vulnerable to (alleged) Russian interference.[6]

There was another historically unique and critical aspect to the fighting - the emergence of synchronized cyberspace domain actions as an intelligence indicator for strategic, operational, and tactical level military operations. Unlike the (alleged) Russian cyberattack upon Estonia in 2007, the (alleged) Russian cyberattack on Georgia was accompanied by physical domain combat between Russian and Georgian military forces. The (alleged) Russian network attack

---

[2] Bob Killebrew "Russia-Georgia: Early Take" Small Wars Journal blog, (15 August 2008), found at: http://smallwarsjournal.com/blog/2008/08/russiageorgia-the-impact-first/

[3] Noah Shachtman "Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It" Wired Magazine, (11 March 2009) found at: http://www.wired.com/dangerroom/2009/03/georgia-blames/

[4] Noah Shachtman "Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It" Wired Magazine, (11 March 2009) found at: http://www.wired.com/dangerroom/2009/03/georgia-blames/ As stated by Georgian National Security Council chief Eka Tkeshelashvili at the GovSec conference in Washington, D.C in March 2009: "But Georgian National Security Council chief Eka Tkeshelashvili says she knows exactly who's behind the network assault. "There's plenty of evidence that the attacks were directly organized by the government in Russia," she tells Danger Room. It's perhaps the boldest, most direct accusation of blame to come from a senior government official in the Russia-Georgia cyber war. But, in conversations with Danger Room, neither Tkeshelashvili nor her advisers offered any new evidence that conclusively linked Moscow to the attacks on Georgian cyberspace. "I'm not saying it's enough for a criminal court, to prove a case beyond a reasonable doubt," Tkeshelashvili conceded…. And she may not be wrong. But the maddening thing about network attacks is that it's all too easy to cloak identities, work through third-parties, and route attacks through far-flung servers. Which makes it next-to-impossible to definitively pin blame. Russian hackers have claimed key roles in the cyber war. Ordinary citizens were encouraged to pile on. One member of Russia's parliament recently said the whole thing was started out of his office."

[5] Jon Oltsik "Russian Cyber Attack on Georgia: Lessons Learned?" Network World, (17 August 2009), found at: http://www.networkworld.com/community/node/44448 "The bad guys weren't working for the Russian government or military but it is safe to say that there had to be some complicity here."

[6] Ben Arnoldy "Cyberspace: new frontier in conflicts, Internet attacks on Georgia expose a key flaw for more than 100 nations" Christian Science Monitor (13 August 2008), found at: http://www.csmonitor.com/USA/Military/2008/0813/p01s05-usmi.html "Georgia's Internet infrastructure has two big weaknesses. First, most of its external connections go through Russia. Second, there's a lack of internal connections called Internet exchange points. So when a Web surfer in Georgia calls up a Georgian Web page, that request routes through another country, which is similar to driving to Mexico to get across town in San Francisco, says Mr. Woodcock, whose organization helps countries build their own Internet exchange points."

operations in virtual cyberspace occurred prior to hostilities and later mirrored (apparently synchronized with) Russian combat operations in the land warfighting domain.[7] These attacks included various distributed denial of service (DDOS) attacks to deny/disrupt communications and information exfiltration activities conducted to accumulate military and political intelligence from Georgian networks. These attacks also included web site defacement for Russian propaganda purposes.[8] One of the first elements of Georgian society that were attacked was a popular hacker forum - by attempting to take out Georgian hackers, Russian-supported hacker militia preemptively tried to forestall or mitigate a counter-attack (or returning fire) from Georgian hackers.[9] What is not widely known is that pro-Georgian hackers made limited but successful network counter-attacks against Russian targets.[10] Hacker wars between (often quite talented) patriotic amateur hackers, cyber militias, and organized criminal gangs have become a widely accepted de facto form of nation-state conflict over the past twenty years (for example: Israeli vs Arab/Muslim (Sept 2000), India vs Pakistan, US vs China (April-May 2001), Russian vs Estonia (April-May 2007), etc…). These non-governmental national assets are generally used for the traditional purposes of imposing one nation's will and conditions upon another.

---

[7] John Leyden, "Bear prints found on Georgian cyber-attacks: Shots by both sides," The Register, (14 August 2008), found at: http://www.theregister.co.uk/2008/08/14/russia georgia cyberwar latest/ "Meanwhile nationalist articles in Russian papers have even reportedly inspired the notorious RBN (Russian Business Network) to flood Georgian systems with junk traffic from compromised systems based in Turkey." Also see Dan Goodin "Georgian cyber attacks launched by Russian crime gangs with help from Twitter, Facebook and Microsoft" The Register, *(*18 August 2009), found at: http://www.theregister.co.uk/2009/08/l8/georgian cyber attacks/ "Last year's cyber attacks that brought internet traffic to a standstill in Georgia were carried out by civilians and Russian crime gangs, in some cases with the unwitting help of websites and software companies located in the US, according to researchers .... The first group involved used botnets, command and control channels, and other resources operated by Russian crime gangs ... " and Mark Rutherford, "Report: Russian mob aided cyberattacks on Georgia," CNET News (18 August 2009) found at http://news.cnet.com/8301-13639_3-10312708-42.html "Civilians recruited by Russian language social networking sites and using Russian Mafia-associated botnets perpetrated many of the cyberattacks on Georgian government Web sites during the five-day Russian-Georgian war in 2008, according to a recent report. However, while the cyberattackers appear to have had advance notice of the invasion and the benefit of some close cooperation from a state organ, there were no fingerprints directly linking the attacks to the Russian government or military, according to the U.S. Cyber Consequences Unit (US-CCU), an independent nonprofit research institute that produced the report," (see endnote #11).

[8] Joseph Menn, "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government" LA Times, (13 August 2008), found at: http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html and Associated Press "Russian Hackers Attack Georgia in Cyberspace" Fox News (13 August 2008), found at: http://www.foxnews.com/story/0,2933,402406,00.html "…hackers took over the Web site of Georgia's parliament and replaced it with an image that drew parallels between Georgian president Mikhail Saakashvili and Adolf Hitler…"

[9] Gregg Keizer, "Russian hacker 'militia' mobilizes to attack Georgia" Network World (13 August 2008), found at: http://www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html

[10] Gregg Keizer, "Russian hacker 'militia' mobilizes to attack Georgia" Network World (13 August 2008), found at: http://www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html "That coordination, said Danchev, was sophisticated enough to launch DDoS attacks against one of the most popular hacker forums in Georgia as a preemptive strike. But the attacks weren't entirely successful, since limited retaliations against Russian sites have succeeded. "Georgian hackers, or pro-Georgian hackers, [launched] distributed-denial-of-service [attacks against] RIA Novosti," he said via IM. RIA Novosti is a Moscow-based news service. The campaign against Georgia is just a sample of what the world should expect when there's armed conflict, said Zenz. "This is what happens," she said, "especially in Russia. Every time something happens, there are attacks. Name any crisis there in the past year, and I can point to a spike in attack traffic .... The future looks a bit grim, added iDefense's director of intelligence, Rick Howard. "Estonia was just the beginning," he said in a statement today. "Anyone picking a political fight with Russia today can now expect to deal with multiple forms and sources of electronic attack; not only from the Russian military, but also from the Russian government's unofficial civilian hacker assets."

At the strategic level the (alleged) Russian cyberspace reconnaissance and probing attacks began weeks prior to the actual inception of virtual and physical combat. Russian web sites, chat rooms, and networks also discussed the upcoming attacks for several weeks. "The attacks originally starting to take place several weeks before the actual "intervention" with the Georgia President's web site coming under DDoS attack from Russian hackers in July, followed by active discussions across the Russian web on whether or not DDoS attacks and web site defacements should in fact be taking place, which would inevitably come as a handy tool to be used against Russia from Western or Pro-Western journalists.[11] It appears that the (alleged) Russian attackers conducted a dress rehearsal for their synchronized cyberattack early in July 2008. "Weeks before bombs started falling on Georgia, a security researcher in suburban Massachusetts was watching an attack against the country in cyberspace. Jose Nazario of Arbor Networks in Lexington noticed a stream of data directed at Georgian government sites containing the message: "win+love+in+Rusia." Other Internet experts in the United States said the attacks against Georgia's Internet infrastructure began as early as July 20, with coordinated barrages of millions of requests - known as distributed denial of service, or D.D.O.S., attacks - that overloaded and effectively shut down Georgian servers.... As it turns out, the July attack may have been a dress rehearsal for an all-out cyberwar once the shooting started between Georgia and Russia. According to Internet technical experts it was the first time a known cyberattack had coincided with a shooting war."[12] These extensive preparatory actions imply a strategic planning process that began long before July 2008.

Another important strategic consideration is how the Russian hacker militia efforts closely coordinated their attacks with the overall strategic objectives of the Russian government:

"For example, they didn't attempt to cripple sites that could have caused chaos or injury, such as those linked to power stations or oil-delivery facilities, but merely those that could trigger comparative "inconvenience." "There was a political decision not to attack those critical infrastructures directly. They made the point that they could launch these attacks. They showed they have the capability to do more," Bumgarner said. This mirrors Russian action against Georgia's paramount strategic installation -- the Baku-Ceyhan oil pipeline, by far the biggest reason why the U.S. and the West as a whole are interested in Georgia. We've discussed here how Russia bombed all around the pipeline without actually hitting it -- a clear message that it could do so if it wished, but would refrain for the moment. Indeed the cyber attack fit into an overall Russian strategy centered on Georgia's oil infrastructure, Bumgarner concludes.[13]

---

[11] Dancho Danchev, "Coordinated Russia vs Georgia cyber attack in progress" ZDNet, (11 August 2008), found at: http://blogs.zdnet.com/security/?p=1670 "The peak of DDoS attack and the actual *defacements* started taking place as of Friday: "Several Georgian state computer servers have been under external control since shortly before Russia's armed intervention into the state commenced on Friday, leaving its online presence in disarray."

[12] John Markoff, "Before the Gunfire, Cyberattacks" New York Times (12 August 2008) found at: http://www.nytimes.com/2008/08/13/technology/13cyber.html

[13] US Cyber Consequences Unit, "The US-CCU Report on the Georgian Cyber Campaign," (August 2008) found at http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf A great summary of the cyber attack on Georgia, John Bumgarner and Scott Borg provide an interesting analysis of how Russia has combined physical attack (conventional combat in Georgia and irregular warfare/terrorism in other places) with its cyber campaigns to influence world-wide energy policy and various sovereign countries on their borders. Also see related Steve Levin "Cyber-Attack Strategy: Part of Russian Attack on Georgian Pipelines, Report Finds," (20 August 2009), found at http://www.oilandglory.com/2009/08/cyber-attack-strategy-part-of-russian_20.html "Yet, the cyber attackers did not go in for the kill, Bumgarner told me -- they didn't attempt to cripple sites that could have caused chaos or injury, such as those linked to

At the tactical and operational levels, specific geographic localities were virtually targeted in cyberspace prior to combat operations in the physical realm. "Many of the most serious attacks began just as the tanks began to roll, although the networks had been set up beforehand. And the choice of targets is especially telling. Official sites in Gori, along with local news sites, were shut down by denial-of-service attacks before the Russian planes got there. "How did they know that they were going to drop bombs on Gori and not the capital?" Jackson asked. "I would say that from what I've seen firsthand, there was at some level actual coordination and/or direction [by the Russian government], especially in regard to the timing and the targets of some of the attacks.""[14] It appears that the Russians selected the Georgian government as the center of gravity to focus its primary attacks upon. Cyberspace domain operations conducted by the Russian cyber militia supported that effort by denying and degrading the Georgian government's ability to communicate, both internally and with the outside world. Through this effort and combined with other physical domain efforts (for example: uncontested ground invasion in the west, naval blockade, and bombing of areas around the oil pipeline), the Russians were able to demonstrate that the Georgian government was unable to defend its sovereign territory in both the physical and cyberspace domains. This degraded the Georgian government's legitimacy and demonstrated to the world an unhindered ability to shut down the critical Baku-Ceyhan pipeline at a time and place of Russian convenience. Russian tactical and operational level actions (in all domains) during this war fit seamlessly into a larger geopolitical strategy of energy dominance by threatening alternate (competing) sources of energy in the physical and cyberspace environments, and destabilizing the national governments representing those alternate and competing energy sources.

What are some of the operational and intelligence lessons that can be drawn from these conclusions? First, for Russia or China to employ their people's patriotic 'hacker militia' to conduct a network attack against a target nation-state, they must engage them first - to motivate and 'sell' them on the concept; steer them toward appropriate targets; synchronize those cyberspace operations with combat activity in the physical realm; and discuss the most effective cyberspace tactics, techniques and procedures (TTPs) to be used. The patriotic hackers and cyber militias need to be focused by the aggressor government against the opponent's center of gravity and their activities to be synchronized with attacks against that center of gravity from the other domains. These hackers and cyber militias need to understand the opponent's center of gravity in order to develop cyberspace domain approaches and techniques to effectively attack it. These preliminary cyberspace activities often create an identifiable signature that can be tracked and monitored in advance of combat operations. Nations need to monitor hacker chat rooms and communications of potential aggressor nations in order to intercept and understand this activity.

---

power stations or oil-delivery facilities, but merely those that could trigger comparative "inconvenience." "There was a political decision not to attack those critical infrastructures directly. They made the point that they could launch these attacks. They showed they have the capability to do more," Bumgarner said. This mirrors Russian action against Georgia's paramount strategic installation -- the Baku-Ceyhan oil pipeline, by far the biggest reason why the U.S. and the West as a whole are interested in Georgia. We've discussed here how Russia bombed all around the pipeline without actually hitting it - a clear message that it could do so if it wished, but would refrain for the moment. Indeed the cyber attack fit into an overall Russian strategy centered on Georgia's oil infrastructure, Bumgarner concludes. It succeeded, in Bumgarner's view. "Unstable ground conditions, augmented by cyber attacks, soon made all of the Georgian pipelines seem unreliable," he writes. Certainly that was the impact for the first weeks and months -- Russia demonstrated that the pipeline was vulnerable, not to mention dispelling the illusion that Georgia enjoyed special Western protection. To a large degree, that remains the fact on the ground -- Georgia and the other former Soviet states of the Caucasus and Central Asia are far more deferential toward Russian wishes. Yet the oil and gas continues to flow."

[14] Joseph Menn, "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government" LA Times, (13 August 2008), found at: http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html

Second lesson, targets in cyberspace need to be identified and accesses developed prior to any actual military operation. The actual planned attacks and activities need to be practiced at a low level to assess their effectiveness. In future cyber combat, nations will need to conduct these preparatory operations, reconnaissance activities, and probing attacks well in advance of any network attack conducted in support of traditional military operation. There will be an attempt to disguise these activities but it is possible that they can be detected by the target nation networks. An alert and capable national cyber defense organization (with effective cyber-intelligence capabilities) conducting cyberspace counter-reconnaissance in combination/collaboration with an intelligence community conducting effective counter-intelligence in the cyberspace domain can effectively monitor and potentially degrade aggressor nation and hacker militia cyberspace preparatory activities. The aggressor nation performing reconnaissance/probing attack efforts will attempt to conduct a 'low and slow' method of patiently building targeting and response information from the target nation. This activity typically operates across a long time line with limited incremental activity that slowly but methodically builds toward a total aggregated situational awareness. However, this approach may not be optimal for rapid mobilization of patriotic 'hacker militia' in the private sector and in organized crime. Generally (not always), only Nation-state cyberspace operators may have the patience and resources to conduct long-time line operations while hacker militias historically have less resources, shorter timelines, and often have a strong psychological need for immediate gratification/feedback. Identifying and then monitoring the health of national critical infrastructure or "key terrain" in cyberspace (ex: government networks; critical communications nodes; national-level power, financial, and health networks; selected media outlets; and vital enclave networks) are critical to providing advanced warning of aggression.

Third lesson to be gleaned from this conflict is that the Russian-oriented hackers/militia took out news and local government web sites specifically in the areas that the Russian military intended to attack in the ground and air domains. The Federal and local Georgian governments, military, and local news agencies were unable to communicate with Georgian citizens that were directly affected by the fighting. This provided an intelligence indicator of the ground and air attack locations. It created panic and confusion in the local populace, further hindering Georgian military response. This effect also provides a future aggressor nation with an opportunity to conduct military deception operations via feints and ruses to mislead the target nation population, government, and military. A sudden ‘blackout' of cyberspace activities in a specific region may provide an indicator of a tactical or operational level conventional attack. Or it could be used as a sophisticated cyberspace operation as part of a larger deception plan, creating a feint in the cyberspace domain to lure opposing forces into believing an attack is imminent in another warfighting domain. Use of patriotic hackers and cyberspace militia themselves might be a deception effort to attract the target nation’s attention away from the aggressor nation’s top-quality military and intelligence community cyberspace operators that quietly conduct the main effort in the overall cyberspace domain operation.

Fourth lesson is that the target nation's patriot hackers/cyber militia will probably be targeted first (or at least early in combat) by an aggressor nation in order to preemptively remove retaliatory capability. There have been a whole series of patriot cyber-militia hacker wars with various levels of government support for their local patriotic hackers over the past 20 years. These individual hackers and cyber-militias target each other and often know each other (at least by reputation). It can be reasonably assumed that government and government-sponsored (closely controlled militia) cyberspace domain operations will follow a similar strategy of

preemptive strike. It is clearly in the interests of any government to watch the status of their internal hacker community - an attack upon this community may very well be an intelligence indicator of potential foreign nation-state hostilities in other Domains. It is also in the interests of 3rd party neutral governments to watch their internal hacker and cyberspace communities in case of war between two other nations. This situational awareness may prevent the neutral nation from being inadvertently drawn into the conflict via unauthorized and unapproved civilian support in the cyber domain for one side (or both sides) of the conflict.[15] We live in a world where a few top-quality hackers, even when only equipped with off-the-shelf technology, can accomplish a considerable amount of damage at the national and strategic level.

These lessons illustrate the requirement for nations that intend to successfully operate in the cyberspace domain to develop air-gapped cyberspace ranges where various scenarios of attack/defend combinations can be practiced and played out in free-play force-on-force combat within a variety of network topology and technology terrain environments. This exercise environment must be integrated with physical domain exercise scenarios in order to better understand the interplay between cyberspace and the physical domains. It also needs to provide a training ground for cyberspace operators to understand and practice the nuances of both offensive and defensive operations (often two separate communities) and how to synchronize cyberspace operations with full spectrum Information Operations (IO) and political/military objectives in the other domains.

Three developing trends that extend across the levels of warfare from strategic to tactical are: 1) the increasing ability of network intelligence operatives at all levels to exfiltrate critical information from potential opponents and neutral players that is valuable for military, economic, diplomatic, and social/cultural purposes; 2) the increasing value of controlling and degrading/denying an opponent's media and publicity message (Information Operations) through denial/disruption/degrading and subversion of targeted information conduits such as web sites, voice over IP (VOIP), chat rooms, social networking sites (Twitter, FaceBook, etc ..), and other

---

[15] Stephen Korns and Joshua Kastenberg, "Georgia's Cyber Left Hook," (2009), Army War College, found at: http://www.carlisle.army.mil/usawc/Parameters/08winter/korns.pdf This source provides an excellent analysis of "cyber neutrality" and many of the policy and legal issues surrounding cyber policy. An example of unapproved civilian cyber activity is the US private sector support provided to Georgia during the cyberspace conflict that accompanied the Russian attack in August 2008: "The underlying implications of the overall issue should be of great concern to US policymakers and strategists. Even if the United States is not a belligerent in a cyber conflict, incursions against the US Internet infrastructure are likely. Private industry owns and operates the majority of the Internet system. During a cyber conflict, the unregulated actions of third-party actors have the potential of unintentionally impacting US cyber policy, including cyber neutrality. There is little, if any, modern legal precedent. The fact that American IT companies provided assistance to Georgia, a cyber belligerent, apparently without the knowledge or approval of the US government, illustrates what is likely to become a significant policy issue. Although nations still bear ultimate responsibility for the acts of their citizens, applying that dictum to the modern realities of cyber conflict is a complex challenge. Georgia's unconventional response to the August 2008 DDoS attacks, supported by US private industry, adds a new element of complication for cyber strategists." For a continuation of this debate, see Rain Ottis, "Georgia 2008 and Cyber Neutrality" blog (31 March 2010), found at: http://conflictsincyberspace.blogspot.com/2010/03/georgia-2008-and-cyber-neutrality.html "Were Georgian websites under attack? Yes, no doubt. Was this a part of the Russian war campaign? Maybe, but at least officially the Russians deny their involvement. Well, if neither belligerent takes responsibility for the attacks, then we can't really refer to Georgia as a "cyber belligerent" (what does this mean, anyway?). We are left with attacks that do not amount to war, but crime or political hactivism, and I am unaware of any international prohibition on cooperating against criminals or hactivists - even on the business level…. Since US is one of the leading nations harboring ISPs with questionable practices, and is also home to a large number of malware infected computers (bots in a botnet), then any time you have a large DDoS attack, US is likely to be on the "attack source" list [to be fair, the authors have also covered this aspect]. I consider it quite likely that at least some US-based computers were used against the Georgian sites during the war. If the Russian Federation was behind the attacks, does this mean that US lost its neutrality and became a belligerent? Again, I would say no. It would be great if US could clean up its part of the Internet, though.

cyberspace technology-based communications mediums; and 3) the time-sensitive nature of cyberspace warfare – a nation cannot engage in cyberspace warfare from a cold start, it must have well-developed tactical, operational, and strategic capabilities developed well in advance of any conflict. These capabilities are represented by trained human capital supported by doctrine, organization, command and control (C2), and technology that has been developed, tested, and refined in strenuous cyberspace combat exercises. Cyberspace intelligence capabilities and situational awareness also need to be developed long before any potential conflict involving the cyberspace domain. The culmination of these trends resulted in a situation that prevented government agencies in Georgia from communicating, both locally with their population and strategically with the rest of the world. Russia was able to successfully attack the Georgian center of gravity across several warfighting domains, to include the cyberspace domain through propaganda operations, and denial, disruption, and degradation of Georgian communications. This allowed the Russians to dominate the strategic communications environment during the several-week build-up to, and the conduct of military operations in the physical domain environments. Doctrinal concepts such as center of gravity and effects based targeting; and military principals such as mass, economy of force, C2, surprise, and unity of effort apply equally to military operations in the cyberspace domain as to operations in the other domains. Attacking and defeating the enemy's center of gravity and breaking the will of the enemy to continue the conflict are traditional objectives of warfare and they are as applicable to the cyberspace domain as any other warfighting domain.

At the operational and tactical levels of warfare, (alleged) Russian cyberspace operations were closely synchronized to achieve effects with their land, air, and sea domain military operations. It appears that networks and web sites within specific geographic locations were targeted for denial and disruption operations in order to cause panic and uncertainty (disruption) in the Georgian civilian population, hindering an effective military response. Georgian hacker forums were targeted early-in the process to preempt, disrupt, and degrade retaliatory operations. At the strategic level, these cyberspace actions supported attacks upon the Georgian center of gravity via propaganda attacks and by impeding official government web sites, obstructing the flow of military and intergovernmental information, and degrading/denying communications (internal and external). The intelligence lessons learned from these cyberspace operations represent tactical and operational level attack sensing and warning (AS&W) indicators as well as strategic-level indicators of potential national conflict. Any one of these individual indicators is probably happening in cyberspace every day so it is difficult to sort through the potential avalanche of Internet, wireless, and electronic spectrum intelligence data. But correlating and fusing cyberspace intelligence from all of these levels and sources in a central fusion center (or, better yet, a well-networked set of collaborative centers….) can help provide a more comprehensive intelligence/situational picture. All-source intelligence collection and analysis within the cyberspace domain is critical, as is combining cyberintelligence with other forms of traditional intelligence (HUMINT, SIGINT, etc…) to gain a complete fusion of all-source intelligence.

Lack of dominance in cyberspace operations also hindered Georgia's ability to conduct national-level strategic communications. They were temporarily prevented from effectively communicating their story to the rest of the world - a key component of an aggressor's strategy to rapidly and aggressive conduct traditional military operations. The Georgians were unable to recover their cyberspace and informational capabilities during the critical period during a very small window of combat operations, i.e., the Russians could only temporarily impose their will

in cyberspace but their successful timing implied close coordination between the military planners and the patriot hacker militia. In future combat, aggressor nation patriotic hacker militia can be called upon to conduct cyberspace fire & maneuver operations performed directly in support of forces in other domains, They could also be extensively utilized to conduct deception efforts in cyberspace in support of operations in the other domains or to act as a distraction for other cyberspace operations conducted by government professionals against target nation high value targets (HVT). The cyberspace operations discussed in this article were preceded by extensive preparatory and reconnaissance efforts in the cyberspace domain that could have provided some AS&W indicators, allowing Georgia to modify its strategy and policies toward its Russian neighbor. Or at least have been more prepared for the inevitability and direction of the war that was to come.

David M. Hollis is a Senior Policy Analyst with the Office of the Undersecretary of Defense for Intelligence (OUSD(I)). He has spent a total of four years on the OSD staff with three as Cyberspace Security Division Chief for the ASD NII/DoD CIO's office prior to working at OUSD(I). He is also a drilling USAR officer with US Cyberspace Command (USCYBERCOM); currently the senior USAR officer responsible for 25 USAR personnel supporting a wide range of USCYBERCOM J-codes and projects, and was previously a Joint Plans Officer with the USCYBERCOM J5. He was with the Army's 1st Information Operations Command from 2000 to 2006 as Red Team Chief, S2/Director of the Army's CyberIntelligence Center, and Senior Operations Planner. He has previously published cyberwarfare articles in the Joint Forces Quarterly and Armed Forces Journal magazines.