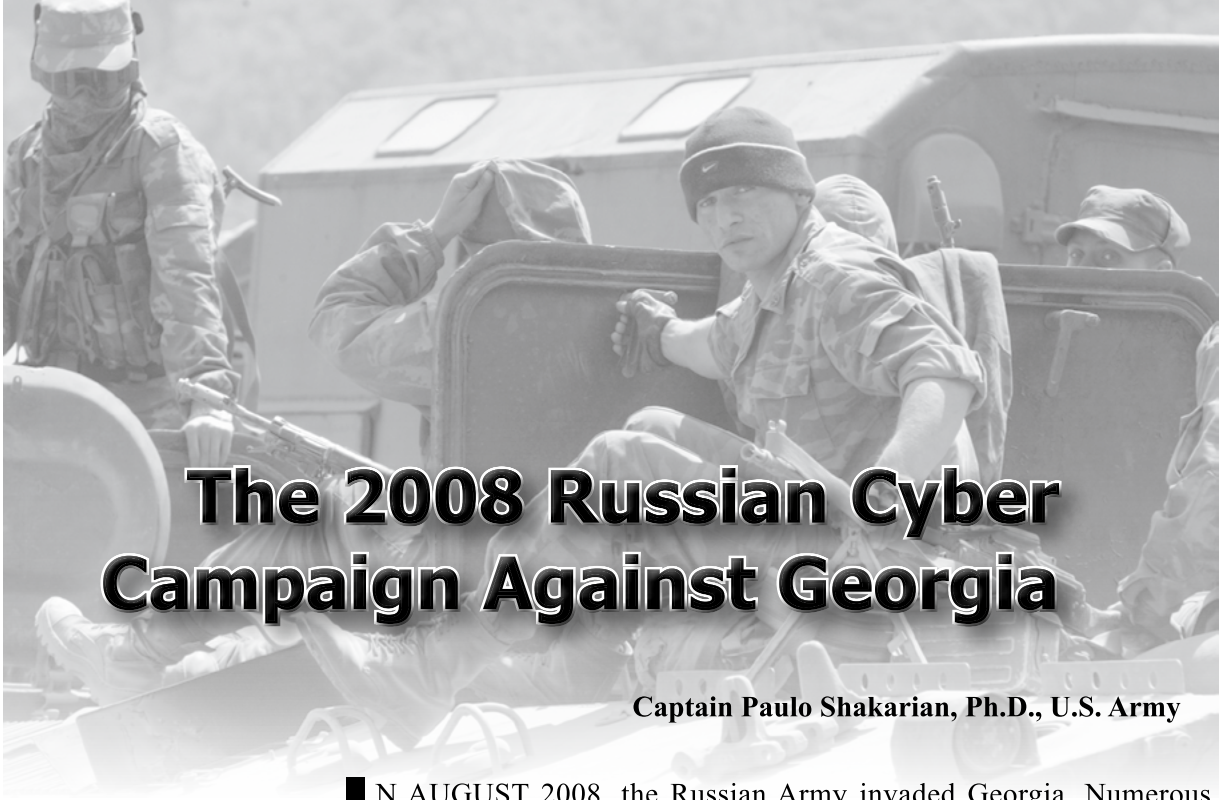


The 2008 Russian Cyber Campaign Against Georgia

Captain Paulo Shakarian, Ph.D., U.S. Army

IN AUGUST 2008, the Russian Army invaded Georgia. Numerous, coordinated cyber attacks accompanied the military campaign. This represents the first instance of a large-scale computer network attack (CNA) conducted in tandem with major ground combat operations. The attack had no direct connection to the Russian government, but had a significant informational and psychological impact on Georgia: it effectively isolated the Caucasus state from the outside world.

Security experts have identified two phases of the Russian cyber campaign against Georgia. The first phase commenced on the evening of 7 August when Russian hackers targeted Georgian news and government websites.[1] Russian Military Forecasting Center official Colonel Anatoly Tsyganok said these first actions were a response to Georgians hacking South Ossetian media sites earlier in the week.[2] The fact that the alleged counterattacks occurred only one day prior to the ground campaign has led many security experts to suggest that the hackers knew about the date of the invasion beforehand.

In the first phase of the attack, the Russian hackers primarily launched distributed denial of service (DDoS) attacks. A denial of service attack is a cyber attack that attempts to prevent the legitimate use of a computing resource. When multiple computers achieve this goal, a distributed denial of service attack has occurred. One way to categorize DDoS attacks is to differentiate between *semantic* and *brute force* attacks. A semantic DDoS takes advantage of either a feature or bug in some software on the target system. A brute force (or "flooding") DDoS attack occurs when the target system receives more Internet traffic than it can handle, which exhausts the command and control resources of the server, rendering it unavailable.[3]

The DDoS attacks during this phase were primarily carried out by *botnets*.[4] A botnet is a group of computers on the Internet (termed "bots" or "zombies") that have been infected with a piece of software known as malware. The malware allows a computer "command and control" server to issue commands to these bots. Often, botnets launch spam email

Captain Paulo Shakarian is an assistant professor in the Department of Electrical Engineering and Computer Science at the U.S. Military Academy (USMA). He holds a B.S. from USMA and an M.S. and Ph.D. from the University of Maryland. He served two tours in Iraq in various military intelligence positions.

PHOTO: Russian soldiers are seen atop an armored vehicle in the breakaway Georgian Province of South Ossetia, 8 August 2008. (AP Photo/Musa Sadulayev) campaigns, but they can also be used to launch wide-scale DDoS attacks. The hijacking of the zombie computers typically occurs in the same manner as infections with other viruses (e.g., email scams, fake websites, infected documents). The communication from the command and control computer to the zombies can be conducted over seemingly innocuous channels on the network (such as a channel normally used for Internet chat) to prevent discovery.[5] Criminal organizations, such as the Russian Business Network (RBN), use and lease botnets for various purposes.[6] The botnets used in the onslaught against Georgian websites were affiliated with Russian criminal organizations, including the RBN.[7]

> ***… cyber activity shifted to the recruitment of "patriotic" Russian computer users—often referred to as "hacktivists."***

In this first phase, the attacks primarily targeted Georgian government and media websites. The Russian botnets relied on a brute force DDoS to attack these targets.[8] The Georgian networks, due to their fragile nature, were more susceptible to flooding than the Estonian networks Russian hackers attacked a year earlier.[9]

In the second phase, Georgian media and government websites continued to receive the attacks, but the Russian cyber operation sought to inflict damage upon an expanded target list including financial institutions, businesses, educational institutions, Western media (BBC and CNN), and a Georgian hacker website.[10] The assaults on these servers not only included DDoS, but defacements of the websites as well (e.g., pro-Russian graffiti on government sites such as a picture likening Georgian President Mikheil Saakashvili to Adolf Hitler). In addition, several Russian hackers utilized publically available email addresses of Georgian politicians to initiate a spam email campaign.[11]

To carry out website defacements, the Russian hackers resorted to another type of attack known as an *SQL injection,* which uses a text field on a webpage to directly communicate with the back end database (normally, a common SQL database—hence the name). A system susceptible to this type of vulnerability essentially gives the hacker total access to the database—including list user login IDs, financial transactions, or website content.[12]

During this phase of the operation, much of the cyber activity shifted to the recruitment of "patriotic" Russian computer users—often referred to as "hacktivists."[13] According to postings on some Russian hacker websites, many "hacktivists" were thought to be members of Russian youth movements.[14] The recruitment was primarily done through various websites, the most infamous of which was "StopGeorgia.ru," which went online 9 August 2008.[15] One hacktivist notes that the instructions provided were very accessible, even for a novice user.[16] For example, StopGeorgia.ru provided easy-to-use tools and instructions to launch DDoS from private machines. It even featured a user-friendly button called "FLOOD" which, when clicked, deployed multiple DDoS on Georgian targets. Although many of the hacktivist assaults relied on a different vulnerability than the botnet actions, they still aimed to overload Georgian servers by brute force.[17] The tools provided were also very versatile. For instance, some could assail up to 17 Georgian servers simultaneously. These hacktivist websites also featured target lists of Georgian systems—including specifications whether it was accessible from Russia or Lithuania and known vulnerabilities.[18] These included susceptibility to SQL injection.[19] It is also noteworthy that some security experts have linked StopGeorgia.ru to Russian organized crime.[20]

Another interesting aspect of the Russian hacker websites is their administrators' professionalism. Not only did they provide novice hacktivists with timely advice, they also policed their sites very well. During the conflict, administrators of Russian hacker site "XAKEP.ru" promptly responded to port-scans by the U.S.-based open-source security project called "Project Grey Goose" by temporarily blocking all U.S. Internet Protocol (IP) addresses. There was also evidence showing that they quickly cleaned up the server, in one instance removing a post containing the keyword "ARMY" in a matter of hours.[21] The precautions of the administrators were well founded. One security organization identified a fake tool uploaded to a Russian hacker website described to launch attacks against Georgian targets. However, this particular piece of software turned out to target Russian systems. The experts concluded that Georgian hackers uploaded the software in an effort to launch a cyber counterattack, although there was no evidence that this tool caused significant damage.[22]

The Georgian reaction to the Russian attacks first consisted of filtering Russian IP addresses, but the Russian hackers quickly adapted and used non-Russian servers or spoofed IP addresses. The Georgians then moved many of their websites to servers out of the country (mainly to the United States). Nevertheless, even these offshore servers were still susceptible to flooding exploitation owing to the extremely high volume of the Russian brute force assault.[23]

Analysis

The following analysis surveys the objectives of the attack. Kenneth Corbin wrote that the goals of the Russian cyber attacks were to "isolate and silence" the Georgians.[24] The assaults had the effect of silencing the Georgian media and isolating the country from the global community. The reports on the event and the target lists provided on the Russian hacker websites give credence to Corbin's hypothesis. Furthermore, the Georgian population experienced a significant informational and psychological defeat, as they were unable to communicate what was happening to the outside world.

While careful not to attribute the cyber attacks to the Russian government, the head of the Russian Military Forecasting Center, Colonel Anatoly Tsyganok, describes the Russian cyber campaign as part of a larger information battle with Georgian and Western media.[25] Russian journalist Maksim Zharov describes cyber warfare as only a small part in a larger information campaign that also included bloggers and media outlets.[26] At one point, Russian sympathizers even flooded a CNN/Gallup poll with over 300,000 responders stating that the Russian cause was justified.[27] Many analysts believe that the primary goal of the first phase of the Russian CNA was to prevent Georgian media from telling their side of the story.[28] This seems to align with the Russian emphasis on information warfare.[29]

Isolating Georgia from the outside world may also explain the attacks on Georgian banks that occurred during the second phase of cyber opera-

(AP Photo/Darko Bandic)

Russian soldiers man a checkpoint on the outskirts of Gori, northwest of the capital Tbilisi, Georgia, 15 August 2008.

tions. At this time, several banks were flooded with fraudulent transactions. International banks, wanting to mitigate the damage, stopped banking operations in Georgia during the conflict.[30] As a result, Georgia's banking system was down for ten days.[31] This led to a shutdown of cell-phone services in the country—further isolating Georgia from the rest of the world.[32] Russian hackers targeting Georgian business websites, also during the second phase, may have aimed to cause similar economic damage.

The objectives of "isolate and silence" were limited in scope. They avoided doing permanent damage to Georgian networks and to Supervisory Control and Data Acquisition (SCADA) targets.[33] SCADA systems are designed for real-time data collection, control, and monitoring of critical infrastructure, including power plants, oil and gas pipelines, refineries, and water systems.[34] Obviously, disruption to these systems would have serious implications for the Georgian infrastructure. Since the Russian hackers most likely had the capability to attack these targets, it is reasonable to assume they exercised some restraint to make sure they did not harm them. Further, Georgia's physical connection to the Internet remained largely unaffected. At the time of the attacks, Georgia connected to the Internet by landlines through Turkey, Armenia, Azerbaijan, and Russia. No evidence points to an attempt to sever these connections in either the physical or virtual world—including the connections running through Russia.[35] This could suggest that the Russian aggressors did not intend to inflict permanent damage on Georgia's Internet infrastructure, but rather target particular servers to meet their "isolate and silence" objectives.

Coordination with Conventional Forces

The coordination of CNA with conventional forces was very limited. While many experts assert that the Russian hackers at least knew when the ground operations would commence, beyond the timing of the cyber attacks, there is little evidence of coordination. Two possible reasons exist for this: The Russian government wanted to be able to disassociate itself totally from the CNA operations (and there is still no hard proof for their involvement). Second, the Russian military had not embraced "jointness" at the time of the conflict—causing cyber operations to be stovepiped.[36] However, some security experts saw some coordination between cyber and ground forces. For example, media and communication facilities were not attacked by kinetic means—this may have been due to the success of the Russian CNA. Additionally, Russian hackers also attacked a website for renting diesel-powered electric generators in support of conventional strikes against the Georgian electrical infrastructure.[37]

Reconnaissance and Preparation

Many security experts believe that the Russian hackers had prepared their operation prior to the initial cyber strikes of 7 August 2008.[38] This is due to the speed of the botnet attacks in phase one and the availability of target lists and hacking tools—that included known SQL injection vulnerabilities—in phase two. Simply put, the effectiveness of the CNA initiated by the Russian hackers leads us to infer that reconnaissance took place well in advance.

There were other indicators of preparation as well. In July 2008, Georgian servers (including the presidential website) were flooded with the message "win+love+in+Russia."[39] These attacks originated from a botnet known as *Machbot Network*, which is known to be used by various Russian criminal organizations.[40] Some analysts suspect that this early strike may have been a "dress rehearsal" for the August attacks.[41] Analysis of the graffiti images used to deface the Georgian websites led security experts to believe that some of these images were created as early as 2006, which could mean that the cyber attacks may have functioned as a contingency operation well before 2008.[42]

Attribution

Many bloggers and news reporters have pondered the level of involvement of the Russian government in the attacks. Here, I will touch on a few of these theories and illustrate how they stack up to the evidence.

- *The Russian cyber operations originated spontaneously from patriotic "hacktivists" primarily in response to attacks on South Ossetian websites.* While this theory may seem plausible, it also poses some problems. First, there was apparently a great amount of reconnaissance planned and executed in preparation. This most likely occurred well before the attacks on South Ossetian media sites on 5 August. Second, the majority of CNA during the first phase of the operations launched from botnets. These assaults were significant and occurred several days before many sites recruiting and supporting the hacktivists went online. The use of botnets suggests the involvement of Russian organized crime–either launching DDoS against Georgia or leasing their botnets to other individuals doing so.

● *The cyber attacks originated solely from Russian organized crime.* The use of botnets and the fact that many hacktivist websites (such as StopGeorgia.ru) have been linked to Russian organized crime makes this hypothesis more credible than the previous one. However, the obvious question is what did the criminal organizations gain from these operations? If the Russian government did not fund or otherwise support them, one theory suggests that the hackers were using the cyber attacks to infiltrate certain Georgian systems for later use (such as the financial institutions attacked in phase two).

● *The cyber attacks originated from Russian organized crime at the request of the Kremlin.* This theory has been put forth by several writers who claim that organizations such as the RBN have links to Vladimir Putin and the Kremlin.[43] The coordination with conventional military operations addressed earlier and a linkage between StopGeorgia.ru and the Russian GRU are also supporting arguments.[44] However, even these findings are circumstantial (at the time of this writing, there is no hard proof of the Kremlin's involvement).

Preparing for a Cyber-Capable Adversary

Whether or not the Kremlin was involved, the cyber attacks yielded a benefit to the overall Russian operation. As such, perhaps we should regard cyber capabilities as a battlefield operating system similar to maneuver, artillery, air defense, etc. Fully understanding the enemy's cyber capabilities is an important piece of analysis. We note that the enemy hacker can take various forms—including individuals at government-sponsored labs, uniformed members of cyber units, members of criminal organizations, and hacktivists. Distinguishing different players in cyberspace is often difficult or impossible. However, understanding which of these cyber soldiers are in a combatant's order of battle can provide insight into their actions. With the order of battle established, we can then apply cyber "doctrinal templates." An example based on the Georgia conflict would include Russian criminal organizations in the order of battle, even though we do not know their precise relationship to conventional forces. Based on their presence in the order of battle, we can then look at a doctrinal template associated with the criminals. This may indicate the use of botnets and hacktivists with the mission to isolate and silence the enemy, but not permanently affect the cyber infrastructure or SCADA.

The Cyber Aspect of the Area of Interest

Perhaps another lesson to infer from the Georgian case is that commanders should not only consider security issues for military networks, but civilian networks as well. While generally not focused on military targets, the Russian cyber attacks in Georgia had significant informational and psychological effects. Further, some cyber attacks, such as the July attacks on Georgian government websites, may forebode not only larger-scale cyber attacks, but ground operations as well. As a result, a commander may want to develop priority information requirements that are cyber in nature. To help protect the local populace, it may become imperative to ensure the survival of civilian computer networks.

Cyber Reconnaissance and Surveillance

As described above, smaller cyber attacks may be indicators for larger-scale CNA as well as kinetic operations. Additionally, there are other signs of impending CNA, the reporting of which may fall on a variety of individuals. For example, the communications officer may report suspicious traffic on a computer network, or a liaison with a

Whether or not the Kremlin was involved, the cyber attacks yielded a benefit to the overall Russian operation.

host nation government may report suspicious traffic on a civilian network. Bloggers or other posts to hacker websites may also hint at an imminent cyber offensive. Personnel tasked with conducting open-source intelligence analysis could monitor them. We should also train and then task traditional signals and human intelligence personnel to identify indicators of cyber attacks specific to their domain.

The Russian cyber campaign on Georgia in August 2008 represents the first large-scale CNA occurring simultaneously with major conventional military operations. These CNA operations had a significant informational and psychological impact on Georgia, as they reduced the capability of not only the media and government, but also the public to communicate with the outside world. Although we cannot directly link the attacks to the Russian government, the government benefited enough from their effects to warrant consideration in future conflicts. Processes such as priority information requirements development and cyber reconnaissance and surveillance planning should be adjusted to account for a cyber capable enemy. ***MR***

NOTES

1. John Bumgarner and Scott Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008.* U.S. Cyber Consequence Unit Special Report, August 2009, 2.

2. Anatoly Tsyganok, "Informational Warfare—A Geopolitical Reality," Strategic Culture Foundation online magazine, 5 November 2008, <http://rbth.ru/articles/2008/11/05/051108_strategic.html> (16 October 2010). Note that this is an English version of the article provided by the website. "South Ossetian News Sites Hacked," Civil.ge Daily News Online, 5 August 2008, <http://www.civil.ge/eng/article.php?id=18896> (16 October 2010).

3. Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communication Review* 34, no. 2, April 2004, 39-53.

4. Jose Nazario, "Georgia DDoS Attacks—A Quick Summary of Observations," Arbor SERT (Security Engineering and Response Team), 12 August 2008, <http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/> (16 October 2010).

5. We also note that more recent botnets use a far more advanced communication systems—the description of this is beyond the scope of this paper. See Evan Cooke, Farnam Jahanian, and Danny McPherson, "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets," *SRUTI* (Steps to Reducing Unwanted Traffic on the Internet Workshop), 2005, 39-44.

6. Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA, O'Reilly Media, Inc., 2010), 121-30.

7. Kenneth Corbin, "Lessons from the Russia-Georgia Cyberwar," *internetnews.com: Real time IT News,* 12 March 2009, <http://www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm> (16 October 2010).

8. The Russian botnets in this phase particularly focused on vulnerability with the protocol known as a TCP SYN exploit. See Nazario for details.

9. Bumgarner and Borg, 4.

10. Ibid, 5.

11. Dancho Danchev, "Coordinated Russia vs. Georgia Cyber Attack in Progress," *ZDNet*, 11 August 2008, <http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670> (16 October 2010).

12. Johannes B. Ullricha and Jason Lamb, "Defacing websites via SQL injection," *Network Security,* vol. 2008, issue 1, January 2008, 9-10.

13. Danchev.

14. Carr, 84.

15. Ibid, 15.

16. Evgeny Morozov, "Army of Ones and Zeros: How I became a soldier in the Georgia-Russia Cyberwar," *Slate,* 14 August 2008, <http://www.slate.com/id/2197514> (16 October 2010).

17. The DDoS attack conducted using such tools differed somewhat from the DDoS attacks by the botnets. Where the botnets used TCP SYN attacks, which exploit the underlying network protocol, many of the tools employed by the "hacktivists" relied on flooding servers with HTTP requests. This attack worked by requesting a given website more times than the webserver can handle. See Bumgarner and Borg, 4 for details.

18. Morozov.

19. Danchev.

20. Carr, 105-15.

21. Ibid, 16.

22. Bumgarner and Borg, 7.

23. Ibid.

24. Corbin.

25. Tsyganok.

26. A synopsis of Maksim Zharov's articles at the time of the conflict can be found in Timothy Thomas, "The Bear Went Through the Mountain: Russia Appraises Its Five-Day War in South Ossetia," *Journal of Slavic Military Studies* 22, (2009): 31-67.

27. See <http://www.theaustralian.com.au/news/attacks-on-cyberspace-preceded-russian-tanks/story-e6frg6to-1111117197354> (16 October 2010).

28. Corbin.

29. Timothy Thomas, "Russian Information-Psychological Actions: Implications for U.S. PSYOP," *Special Warfare* 10, no. 1, Winter 1997, 12-19.

30. Corbin.

31. Bumgarner and Borg, 6.

32. Corbin.

33. Bumgarner and Borg, 5.

34. John D. Fernandez and Andres E. Fernandez, "SCADA systems: vulnerabilities and remediation," *Journal of Computing Sciences in Colleges* 20, no. 4 (April 2005): 160-68.

35. Earl Zmijewski, "Georgia Clings to the Net," *Reneysys: The Internet Intelligence Authority,* 10 August 2008, <http://www.renesys.com/blog/2008/08/georgia_clings_to_the_net.shtml> (16 October 2010).

36. Tor Bikkvol, "Russia's Military Performance in Georgia," *Military Review (*November-December 2009): 57-62.

37. Bumgarner and Borg, 6.

38. See Carr, 183, and Bumgarner and Borg, 6.

39. Timothy Thomas, "The Bear Went Through the Mountain: Russia Appraises Its Five-Day War in South Ossetia," *Journal of Slavic Military Studies* 22 (2009): 56.

40. Stephen Korns and Joshua Eastenberg, "Georgia's Cyber Left Hook," *Parameters* (Winter 2008-2009): 60-76.

41. Thomas, "The Bear Went Through the Mountain, 56.

42. Bumgarner and Borg, 5.

43. Corbin.

44. This circumstantial linkage is based on WHOIS registration for servers associated with StopGeorgia.ru. One registration address is located next to the Russian GRU headquarters in Moscow. Security experts and Project Grey Goose performed this analysis. See Carr, 105-15.

The Destruction of Sennacherib

by George Gordon, Lord Byron (1788-1824)

The Assyrian came down like the wolf on the fold,
And his cohorts were gleaming in purple and gold;
And the sheen of their spears was like stars on the sea,
When the blue wave rolls nightly on deep Galilee.

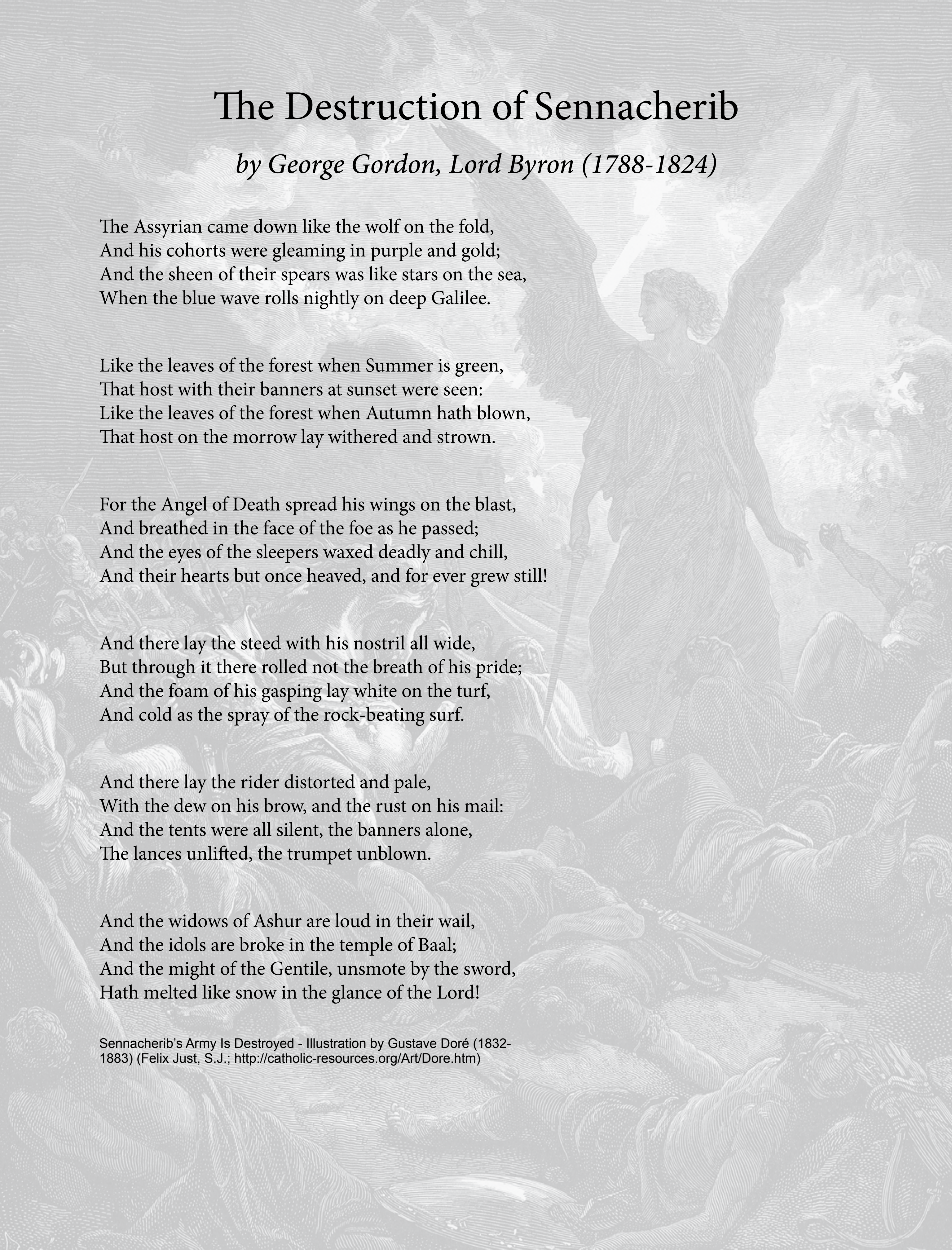
Like the leaves of the forest when Summer is green,
That host with their banners at sunset were seen:
Like the leaves of the forest when Autumn hath blown,
That host on the morrow lay withered and strown.

For the Angel of Death spread his wings on the blast,
And breathed in the face of the foe as he passed;
And the eyes of the sleepers waxed deadly and chill,
And their hearts but once heaved, and for ever grew still!

And there lay the steed with his nostril all wide,
But through it there rolled not the breath of his pride;
And the foam of his gasping lay white on the turf,
And cold as the spray of the rock-beating surf.

And there lay the rider distorted and pale,
With the dew on his brow, and the rust on his mail:
And the tents were all silent, the banners alone,
The lances unlifted, the trumpet unblown.

And the widows of Ashur are loud in their wail,
And the idols are broke in the temple of Baal;
And the might of the Gentile, unsmote by the sword,
Hath melted like snow in the glance of the Lord!



Sennacherib's Army Is Destroyed - Illustration by Gustave Doré (1832-1883) (Felix Just, S.J.; http://catholic-resources.org/Art/Dore.htm)