Cryptology and Information Security Series
Volume 3, 2009
The Virtual Battlefield: Perspectives on Cyber Warfare
Edited by Christian Czosseck, Kenneth Geers
ISBN 978-1-60750-060-5

A Brief Examination of Media Coverage of Cyberattacks (2007 - Present)

Cyrus FARIVAR
Freelance Technology Journalist (NPR, PRI, CBC, The Economist)

Abstract. As cyberattacks become more frequent, they draw new attention in the media. Indeed, there has been a significant spike in journalistic coverage of cyberattacks and cybersecurity in the last year alone, making this particularly relevant now. The aim of this paper is to provide an overview of coverage and make suggestions for future journalists and policymakers to work better together to better understand this new threat.

Keywords. Media studies, media, journalism, cybersecurity, cyberattacks

Introduction

In the last decade, there have been countless cyberattacks against various political, military and economic targets in the United States, Europe and elsewhere. Some have been made public, and others remain classified. Many of these cyberattacks have been against various American military targets and some have have overlapped into cyber-espionage territory. (For the purposes of this paper, I will focus only on political-oriented direct cyberattacks, not cyber-espionage.)

Since 2007, the world has seen three major politically-oriented cyberattacks (denial of service attacks) against three former Soviet Union countries, Kyrgyzstan (January 2009), Georgia (August 2008), and Estonia (April-May 2007). All three likely originated from within Russia, and may have implicitly involved the Kremlin, despite official denials. As such, this increase in cyberattacks has resulted in a corresponding increase in the amount of coverage this issue receives in the English-language print media. In the case of the 2007 attacks against Estonia and the 2008 attacks against Georgia, both made the front page of *The New York Times*. However, while there has been more attention paid to this issue, some of it has been misleading at best and false at worst. Therefore, it is in the interests of the cybersecurity community and the media that cover them to better understand how the media has treated cyberattacks, and to improve public understanding of this phenomenon.

Cryptology and Information Security Series
Volume 3, 2009
The Virtual Battlefield: Perspectives on Cyber Warfare
Edited by Christian Czosseck, Kenneth Geers
ISBN 978-1-60750-060-5

1. Not all Cyberattacks Are Created Equal (Kyrgyzstan)

On January 28, 2009, The Wall Street Journal ran this headline: "Kyrgyzstan Knocked Offline."[1] However, the six-paragraph article, which relied on two sources, only one of which was named, described how a denial-of-service attack hit the country's two main ISPs, accounting for nearly 80 percent of the country's bandwidth. While such a tactic would seem like major news, it was treated as a minor, largely unimportant story. The Journal relegated it to page A10 of the newspaper, indicating that the news was only moderately important. The attack was also covered by a few industry publications, including Computerworld and The Register. The New York Times, ignored the story in print and only wrote about the event on its blog, The Lede.[2]

This lack of attention shows that when a minor, obscure country gets hit, it's difficult to develop much interest in such a story – particularly when it's a country that doesn't have an active online presence, nor that is accompanied by any kind of corresponding real-world action, nor is it an active member of a multi-national organization like the European Union or NATO. This is not to say that the attack against Kyrgyzstan should not have warranted more coverage. If any North American, E.U., or East Asian nation suddenly had 80 percent of its online capacity knocked out, it likely would have made international headlines, as it did in late 2008 when an undersea cable near Egypt was cut by accident, and not as a result of a cyberattack.[3] This is an unfortunate example of a double-standard in the media should be rectified the next time something like this happens.

2. When a Cyberattack Accompanies Real-World Events, People Take Notice (Georgia)

In August 2008, when Georgia suffered a cyberattack that accompanied its invasion by Russia, the world sat up and took notice. *The Wall Street Journal* reported: "Georgia States Hit By Cyberattack," while *The New York Times* noted: "Before the Gunfire, Cyberattacks."[4] Most media outlets sat up and took notice that a cyberattack element corresponded with actual physical attacks. Even though these attacks again took the form of "hacktivism," and denial-of-service attacks, these media outlets tended to analyze the online component in more straightforward and plain terms. The *Times* noted that the attacks simply "overload and effectively shut down Georgia servers."

As the second major cyberattack in recent memory, the Georgia attack was notable as the cyberattack was squarely set in the context of the events on the ground. Perhaps one of the reasons why the attack against Kyrgyzstan never captivated the attention of reporters and editors in the same way was because there was no clear narrative of why it happened – competing theories about obscure political disputes in far-off countries perhaps don't work. In Georgia, like in Estonia before it, there was a clear example of a former occupying power asserting its dominance, like a bully beating up a little kid. This attack was also notable as it was the first (and possibly only) cyberattack where a journalist became an active participant in the war – albeit in a very minor way. Evgeny Morozov, a Belorussian journalist now living the United States, in his *Slate* piece "How I became a soldier in the Georgia-Russia cyberwar," showed how easy it was for an average Russian-speaking Internet used to quickly acquire the tools necessary to throw an "e-Molotov Cocktail."[5] Morozov was likely the first journalist who quickly understood how such an attack could emerge so quickly. In essence, nationalist fervor

Cryptology and Information Security Series
Volume 3, 2009
The Virtual Battlefield: Perspectives on Cyber Warfare
Edited by Christian Czosseck, Kenneth Geers
ISBN 978-1-60750-060-5

plus an Internet connection could rapidly constitute a "cyberwar." He concluded his piece this way, noting:

In less than an hour, I had become an Internet soldier. I didn't receive any calls from Kremlin operatives; nor did I have to buy a Web server or modify my computer in any significant way. If what I was doing was cyberwarfare, I have some concerns about the number of child soldiers who may just find it too fun and accessible to resist.

My experiment also might shed some light on why the recent cyberwar has been so hard to pin down and why no group in particular has claimed responsibility. Paranoid that the Kremlin's hand is everywhere, we risk underestimating the great patriotic rage of many ordinary Russians, who, having been fed too much government propaganda in the last few days, are convinced that they need to crash Georgian Web sites. Many Russians undoubtedly went online to learn how to make mischief, as I did. Within an hour, they, too, could become cyberwarriors.

3. The First Cyberwar (Estonia)

2007 was the first time that *The New York Times* ever used the word "cyberwar." In its May 29, 2007 article, "Digital Fears Emerge After Data Siege in Estonia," the American newspaper of record followed the tone that had already been set for much of the worldwide English-language media coverage of the event.[6] The *BBC*, which was one of the first major news outlets to publish, declared on May 17, 2007: "Estonia hit by 'Moscow cyber war.'"[7] On the same day, the British newspaper *The Guardian* wrote: "Russia accused to unleashing cyberwar to disable Estonia."[8]

While the *BBC* had used the term before, this was the first time that it had been used to describe real-life state-to-state attacks. In addition to declaring the events a "war," there was a great deal of description about how "E-stonia" essentially functioned off of its Internet applications. While it is true that Estonia has a high level of connectivity, Internet banking, online voting and all the rest, the tone of many articles illustrated a scene of near-meltdown and destruction. The *Times* reported that the attacks "came close to shutting down the country's digital infrastructure." *The Washington Post* wrote that the attacks "disrupted government e-mail and led financial institutions to shut down online banking." Jaak Aaviksoo, Estonia's defense minister, told *Wired* that Estonia's national security was threatened. However, the attacks, while annoying, did not do any permanent damage, nor was the society in immediate peril.[9] While there was little technical difference between the attacks against Estonia and Georgia, the first political "cyberwar," Estonia's technological landscape made the rhetoric used that much more dramatic.

4. Lay Off the Hyperbole – It's the Worst Thing Ever

If there is anything to be learned from the first "cyberwar," or the first "Web War One," (as *Wired* called it) is that hyperbole is a great weapon that can be used effectively to draw the attention of the world. I'll admit that I myself fell for it – my *Slate* piece in the aftermath of the attacks on Estonia was dubbed by my editors as "Cyberwar I."[10] In retrospect, the term "cyberattack" would have been more

Cryptology and Information Security Series
Volume 3, 2009
The Virtual Battlefield: Perspectives on Cyber Warfare
Edited by Christian Czosseck, Kenneth Geers
ISBN 978-1-60750-060-5

descriptive, as a war implies a congruous, more or less armed conflict between two clear entities. In this case, the metaphor of "war" is not very accurate, as it was not possible for Estonia (or any other cyberattacked country) to retaliate even if it wanted to. In a cyberattack, the only strategy is defense – there is no way to counter-attack, or to take out the online firing turret. Furthermore, it's impossible to have a war against an enemy even more faceless and intangible than international terrorist organizations. If ordinary, un-technically sophisticated people like Morozov can become "cyberwarriors" within an hour, does that mean, then, that they are protected under the Geneva Conventions? Using the language of war quickly breaks down.

In addition to using the term "cyberwar," everyone has been easily seduced by the armageddon-style rhetoric that Estonian government officials and associated figures have used to describe what had happened. Ene Ergma, the speaker of the Estonian parliament, in an interview with *Wired* magazine, compared the cyberattacks to a nuclear explosion, calling them "the same thing."[11] Linnar Viik, the Estonian Internet guru, told *The Washington Post*: "These attacks were an attempt to take one country back to the cave, back to the Stone Age."[12] Not only are these statements ludicrous on their face, but they're blatantly untrue. If the Kremlin or the Russian "hacktivists" had wanted to pummel Estonia, then the attacks wouldn't have ceased two weeks after they had begun. The attacks clearly were meant as a message, not as a war. With all due respect, it was wrong of Ergma and Viik to make such hyperbolic statements, and it was equally wrong of anglophone journalists to lap it up as easily as they did. Journalists have a responsibility to not take such ridiculous statements at face value, particularly ones who have a history of reporting on technology.

Journalists and Estonians alike would do well do remember the example set by President Bill Clinton in February 2000. This was just after major American tech companies including Yahoo, Buy.com and CNN were hit with denial-of-service attacks. In a press conference, the president was asked if this attack was the "electronic Pearl Harbor." Clinton replied: "Well, I hope not. (Laughter.) I think it was an alarm. I don't think it was Pearl Harbor. We lost our Pacific fleet at Pearl Harbor – I don't think the analogous loss was that great."[13]

5. Cyberattacks and Civilians

As a technology journalist, or as a cybersecurity professional, it's easy to have tunnel vision. It's easy to see botnets on every network and miscreants in every Internet forum. This is not to say that these threats are not real. Rather, it is important to step back from our bandwidth-fueled lifestyle and begin to examine how cyberattacks do or don't affect people in the real world. It is a luxury to have high levels of Internet services, and it is equally a luxury to be able to worry about whether or not these sites are affected by online "warfare."

While trying to report on the cyberattacks against Georgia in August 2008, I was embarrassed when calling the Georgian Ministry of Foreign Affairs in Tbilisi, and a spokesperson rebuked me for wanting to know about cyberattacks, when in fact the Ministry was far more concerned with protecting territorial integrity and Georgian citizens, rather than where the ministry's web site was going to be hosted. While it may be of great concern and worry to many cybersecurity professionals who have warned for years of coming cyberattacks – these types of attacks, at least in their current form, take a back seat to actual, physical warfare. After all, it is worth repeating that no one

Cryptology and Information Security Series
Volume 3, 2009
The Virtual Battlefield: Perspectives on Cyber Warfare
Edited by Christian Czosseck, Kenneth Geers
ISBN 978-1-60750-060-5

has died as a result from a cyber attack. Further, while the Estonian Internet security community was going into overdrive during the cyberattacks of 2007, the Estonian public did not seem to be touched by the attacks. In a survey by the Estonian newspaper *Postimees*, nearly half (over 49 percent) of the 1,243 Estonian surveyed said that they were not affected by cyberattacks.

6. Difficulty of Catching the Cyberattackers

If there's one point that should be made to journalists and policymakers alike, it's that after nearly a decade of major denial of service attacks, that there is neither a perfect way to secure against them, nor is there a good way to track the perpetrators. After the attacks against CNN back in 2000, Richard Power, an official of the Computer Security Institute, told the news network at the time that such attacks "will be one of the most difficult things to address."[14] Indeed, it seems that while the attacks may have gotten more sophisticated and larger, that the basic procedure and execution of such an attack has not changed hardly at all since an attack that unleashed an estimated 800 megabits per second of data on web servers. Estonia was only able to defend against the attack by severing, temporarily, its international data connection to the outside world. Smaller countries with a limited number of international pipes can employ this tactic, whereas a much larger online presence like the United States, are unable to.

Further, it should be underscored that it's very difficult to catch anyone who engages in a cyberattack. Even the attacks against Estonia, which were publicized and had a high-level of international involvement, have only resulted in the arrest and successful prosecution of one Estonian citizen, Dmitri Galushkevich.

The 19-year-old quickly confessed to attacking government computer networks, which is punishable – according to the Estonian Penal Code Section 206, subsection 2 – up to three years in prison.[15] But Galushkevich said that he acted alone, based on instructions that he read online, which were probably not unlike the ones that Morozov discovered. He didn't have any knowledge about who the masterminds or perpetrators in other countries might be.

It is important to remember that in the immediate months after the 2007 cyberattacks, the Estonian government attempted to request further information from Russian authorities. Officials had a list of IP addresses that appeared to originate from within Russia, and needed the help of their neighbor to conduct further investigations, and perhaps find new suspects. But the Russian Embassy in Tallinn and the Kremlin gave their Estonian counterparts the run-around, arguing that technicalities of the treaty between the two countries prevented Russia from providing this information. Further, the Russian constitution forbids the extradition of its own citizens, so there was no way for Estonian authorities to question or even depose any Russians. Partly because of the evidence that he's seen, and Moscow's reluctance to be cooperative leads made Estonian Chief Prosecutor Margus Kurm say that he is confident that the leaders of the attacks are in Russia, despite saying: "We have no evidence and no information that this was the Russian government."

Still, Kurm is pretty hopeless of ever gaining any further information that could be legally useful for prosecuting anyone for cybercrimes against the Republic of Estonia. In an interview in July 2007, he admitted to me: "The status is that we haven't got any information from Russia and I'm quite sure that we will not get any information."[16]

Cryptology and Information Security Series
Volume 3, 2009
The Virtual Battlefield: Perspectives on Cyber Warfare
Edited by Christian Czosseck, Kenneth Geers
ISBN 978-1-60750-060-5

On January 25, 2008, Dmitri Galushkevich pled guilty to attacking Estonian websites. He had to pay a fine of 17,500 Estonian kroons, or around $1,700 and received only probation – no jail time. The case was closed, and no further legal action was taken against anyone, largely because, in the words of Kurm, "Russia refused to co-operate."[17]

What this means, is that for the foreseeable future, cyberattacks will remain an effective tactic countries between nations that are not exactly always friendly with one another, as is the case with Russia and many of its former Soviet satellites.

7. Suggestions for Researchers and Policymakers to Improve Media Coverage

In summation, there are three main points that I would like researchers, policymakers and journalists to come away with.

First, tone down the rhetoric, hyperbole, and watch your language. If you talk about "cyberwar," – the use of the word war has a very specific meaning and very specific consequences. A war usually implies two, more-or-less equal sides, with a clear objective. Cyberattacks generally are not always necessarily couched in the applications of political conflict – in fact, many attacks have more to do with organized crime or online mischief than they do actual warfare. As such, journalists should be wary of sources that compare cyberattacks to nuclear warfare and make similarly absurd comparisons. Further, researchers and policymakers need to be aware of the words that they use themselves.

Second, researchers and policymakers need to be more open (as much as possible) with the information that they do have. Journalists need to be able to verify data, and understand the data that they're looking at. When everything is construed as a "cyberwar," it's tough to determine how various "cyberwars" compare to one another. Was Estonia's attack the same as the one against Georgia? What about the 2009 attack against the United States and South Korea?

Third, and most importantly, policymakers and researchers need to understand how they can work together. Whether they like it or not, media can have a significant influence on public policy. It is the job of the media to inform the public and act as a watchdog on government's activities. The more information that public officials, corporations and researchers can provide to journalists, the better the journalists can do in presenting the case. However, one of the problems is that there simply aren't very many journalists that fully understand neither how cyberattacks work nor what they are. It would be helpful for journalists to participate in a workshop on cyberwarfare from their local governments, or perhaps from the CCDCOE to better understand how these attacks work from a technical standpoint.

References

[1] Rhoads, Christopher, "Kyrgyzstan Knocked Offline," *The Wall Street* Journal. , January 28 2009. http://online.wsj.com/article/SB123310906904622741.html?pagewanted=print
[2] Mackey, Robert, "Are 'Cyber-Militas Attacking Kyrgyzstan?', *The New York Times*
[3] *Led* Blog, February 5 2009. http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/?pagewanted=print
[4] "Severed cable disrupts net access," *BBC* News, December 19, 2008 http://news.bbc.co.uk/2/hi/technology/7792688.stm

Cryptology and Information Security Series
Volume 3, 2009
The Virtual Battlefield: Perspectives on Cyber Warfare
Edited by Christian Czosseck, Kenneth Geers
ISBN 978-1-60750-060-5

[5] "Georgia States Computers Hit By Cyberattack," *The Wall Street* Journal, August 12, 2008. http://online.wsj.com/article/SB121850756472932159.html
[6] Morozov, Evgeny, "An Army of Ones and Zeroes," *Slate*, August 14, 2008. http://www.slate.com/id/2197514/pagenum/all/#p2
[7] Landler, Mark, and Markoff, John. "Digital Fears Emerge After Data Siege in Estonia," *The New York Times,* May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=print
[8] "Estonia hit by 'Moscow cyber war,' *BBC* News, May 17, 2007. http://news.bbc.co.uk/2/hi/europe/6665145.stm
[9] Traynor, Ian, "Russia accused of unleashing cyberwar to disable Estonia," *The* Guardian, May 17, 2007. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia
[10] Davis, Joshua, "Hackers Take Down the Most Wired Country in Europe," *Wired,* August 21, 2007. http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all
[11] Farivar, Cyrus, "Cyberwar I," Slate, May 22, 2007. http://www.slate.com/id/2166749/fr/flyout
[12] Davis, Joshua, "Hackers Take Down the Most Wired Country in Europe," *Wired,* August 21, 2007. http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all
[13] Finn, Peter, "Cyber Assaults on Estonia Typify a New Battle Tactic," *The Washington* Post, May 19, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html
[14] "Remarks by the President in Photo Opportunity with Leaders of High-Tech Industry and Experts on Computer Security," *The White House Office of the Press* Secretary, February 15, 2000. http://www.fas.org/irp/news/2000/02/000215-secure-wh1.htm
[15] "Cyber-attacks batter Web heavyweights," CNN, February 9, 2000. http://archives.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/index.html
[16] "Tulemused – Teksid," http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30068K7&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistusseadustik
[17] Margus Kurm, in discussion with the author, July 19 2007. Email from Margus Kurm to the author, January 29 2008.