digital icons
Studies in Russian, Eurasian and Central European New Media

Blame It on the Russians: Tracking the Portrayal of Russian Hackers during Cyber Conflict Incidents

ATHINA KARATGOZIANNI
University of Hull, UK

Abstract: This article analyses various cyber conflicts and cyber crime incidents attributed to Russian hackers, such as the Estonian and Georgian cyber conflicts and the 'Climategate hack'. The article argues that Russian hackers were blamed by dozens of outlets for the Climategate hack, because that was consistent with global media coverage of cyber crime incidents which portrayed Russians as highly powerful hackers responsible for many hacking incidents. This narrative also was congruent with the new Cold War rhetoric that consistently takes issue with Russia acting on its geopolitical interests. These interests are seen to manifest themselves in Russia's objection to countries, formerly under its influence, participating in the NATO alliance and its seemingly obstructive stance at the Copenhagen summit on climate change.

Keywords: Russians, cyber crime, Climategate hack, cyber war, hacking, media bias

This article tracks the portrayal of Russian hackers in relation to various cyber conflicts and cyber crime incidents. It employs cyber conflict theory (Karatzogianni 2006; 2009a; 2009b; 2010) to engage with various aspects of cyber conflicts implicating Russian hackers, such as the cyber conflicts involving Estonia and Georgia. Further, its purpose is to identify and analyze the continuities in the coverage of Russian hackers, and links made in the global media between intelligence, cyber espionage, cyber crime and patriotic hacking, which eventually and inevitably also implicated Russian hackers and Russia in the Climategate hack.

The article is not written in defence of Russians or the Russian government. The intention here is to simply demonstrate that although Russians *are* involved in cyber crime and cyber conflict incidents – as are other nationals by participating in cyber crime gangs, ad hoc patriotic assemblages, or even hacking dissident media organisations to reinforce the government line – they are also portrayed by the majority of the global media as *the* perpetrators of everything under the sun (unless the crimes are attributed to China or Chinese hackers).The paper

demonstrates that the Russians were accused relentlessly of the Climategate hack under a new Cold War rhetoric spurred on by Russia's energy interests and motivations. In contrast to the overwhelming blame that Russian hackers are made to bear, there are other possible competing explanations: involvement of oppositional bloggers and scientists invested in the Climategate debate, or computer security failure at East Anglia University's network.

The first element of my analysis in this article is mapping the real events and the environment of cyber conflict. The Estonian and Georgian cyber conflicts are of the ethnonational type, revealing also cultural struggles, due to Russia's alleged continuing intervention in the political life of these countries. The hacker groups involved in these conflicts and their systems of belief and organisation aspire to hierarchical apparatuses (nation, ethnicity, identification with parties and leaders). The Climategate hack case, on the other hand, has sociopolitical and economic aspects, as it is an issue that is global in nature in terms of content. However, the Climategate case also points to ethnic and national issues in the coverage, as geopolitical narratives involved the main protagonists in the Climategate debate and the actual groups blamed for the hack. In mapping the environment of cyber conflict, the relationships between military and security, politicians and media, and geopolitical dimensions need to be addressed.[1]

In the process of building my argument, I surveyed approximately 130 articles collected between 2007 and 2010. The articles were sampled by using the keyword 'Russian hackers', while also snowballing to include other items that followed the initial searches. The articles discussed here include sources from mainstream media (online versions of newspapers, magazines and TV outlets, such as *The Guardian, New York Times, Wall Street Journal, The New Scientist, The Independent, Le Monde, BBC, AFP, Reuters*); country- and incident-specific media and blogs (such as the *Georgian Times, Russia Today* and climate sceptic blogs); and IT business, security, and military sites and blogs commenting on cyber security and on technical aspects of the cyber conflicts discussed (such as *National Defence Magazine, Wired Magazine, Asian Computers, PC World,* Villeneuve's blog). An effort was made to include an equal number of articles out of these three types of sources.

My analysis is also based on my previous research, where I integrated elements of social movement, conflict and media theories into a single analytical framework of 'cyber conflict', in order to explain the empirical evidence of various cyber conflicts. Elements of social movement theory were adopted to discuss sociopolitical cyber conflicts; conflict theory was used to address ethnoreligious cyber conflicts; and media theory was deployed as a component for both, deriving a single integrated analytical framework for understanding cyber conflicts. This framework has been applied when analysing ethnoreligious and ethnonational cyber conflicts (i.e. Israeli-Palestinian, pro-Islamic-anti-Islamic conflicts related to the Iraq war, Indian-Pakistani and American-Chinese) and sociopolitical cyber conflicts (such as anti-globalisation, anti-war movements, dissidents in authoritarian regimes and Internet censorship in different countries (Karatzogianni 2006).[2] Lastly, I have used framework analysis of

[1] For another example of similar types of analysis, see Greg Simons's work on the reporting of modern warfare and the Russian war on terrorism (Simons 2010).

[2] In sociopolitical cyber conflicts, I have looked at the impact of ICTs on mobilising structures; framing processes; structures of political opportunity, and hacktivism. In ethno-religious cyber conflicts I have focused on ethnic/religious affiliations, discourses of inclusion and exclusion, information warfare, and conflict resolu-

content, similar to Juyan Zhang and Shahira Fahmy's (2010) approach in their comparative analysis of American and Russian press coverage of political movements in Ukraine, Belarus and Uzbekistan. The authors chose the sourcing, causality and moral judgment frames to apply to their empirical evidence. This type of frame analysis is taken into account when looking at discourses and analysing the Internet as a medium.

The first section of this article is an overview of cyber attacks; the second discusses the global media coverage of Russian cyber crime; the third explains the connection of cyber crime and politically-motivated cyber attacks in the post-Soviet cyber space; the fourth section looks at cyber security and geopolitics discussions; the last section dwells on the new Cold War rhetoric and the framing of Russians as responsible for the Climategate hack. Although the global media often portrays individuals and groups of Eastern European or post-Soviet origin as a uniform category, the main focus here is on the media portrayal of Russia and the Russians.

Cyber Conflict Events: A Brief Background

Before I proceed to discuss the ways Russian hackers were represented in the media, I provide a very brief description of the cyber conflict incidents themselves. The Estonia cyber attacks lasted roughly a month (beginning on 27 April 2007) and handicapped Estonian government, media and bank sites. The attacks served as a protest platform for ethnic Russians objecting to the relocation of the Bronze Soldier of Tallinn, and included defacement of web sites, 'denial of service' attacks and the use of botnets previously used for spam.

The South Ossetian-Georgian cyber conflict occurred right before and during the actual armed conflict in August 2008 between Georgia and Russia. On the 7th of August, Georgia launched a military attack in South Ossetia in an attempt to re-establish control of the area.[3] Russia retaliated by bombing and occupying Georgian cities. The war ended after five days; in the aftermath Russia supported the independence of South Ossetia and Abkhazia (another region seeking independence from Georgia), keeping troops in the areas. The cyber conflict began several days before the actual war, when the virtual infrastructures of various South Ossetian, Russian and Georgian organisations were attacked, leading to defacement of web sites, services denied and botnets. According to internet rumours, the Russian Business Network (RBN), a well known cyber crime gang linked to malicious software and hacking, was involved in the attacks, together with the Russian security services. Several governments such as Estonia, Poland and Ukraine offered assistance to Georgia.

In November 2009 the 'Climategate hack', as it was termed by the media, was discovered: thousands of e-mails, files and other communication among scientists at the Climate Research Unit (CRU) at the University of East Anglia were hacked into and the materials posted on a Siberian server. The controversy, which portrayed climate change scientists as manipulating data and the peer-reviewing process, coincided with the Copenhagen summit, where world leaders were meeting to discuss climate change. Three independent inquiries in

tion.

[3] Since the early 1990s South Ossetia was controlled by a Russian-backed government seeking international recognition.

the UK rejected allegations of wrong-doing by the scientists involved, though it was found there was room for improvement in the CRU's working practices (Gillis 7 July 2010).

Russia Portrayed as a Nation of Unemployed Superhackers and as a Centre of Cyber Crime

Many of the online news articles addressed here consistently describe Russian hackers as highly educated and talented people who, upon unemployment, are forced to turn to illegal activities. The examples of this type of explanation are plenty. For instance, a local media outlet in the USA called *Elk Grove Citizen* presented a story in which special agent LuAnna Harmon of the FBI's Sacramento division visits a high school to talk about cyber crime and frequently mentions Russian cyber crimes as her examples. When asked by the students about the reasons cyber crimes happen in Russia, she blamed the situation on highly educated people who turn to crime since there are few jobs for them (Macdonald 13 April 2010). In another report, by *The Register*, Dmitry Zakharov, director of communications at the Russian Association of Electronic Communications, is quoted saying '[W]e are not able to offer talented technology people jobs. So they get involved in illegal activity' (Leyden 12 April 2010).

Russia is consistently portrayed as a nation of superhackers, responsible for sophisticated attacks. Various media reports involve interviews with security professionals and Russian hackers about their background and motivations. For example, in the BBC interview with Evgeny Kaspersky, the 'computer security guru' and an owner of Internet security firm Kaspersky Labs, the reporter refers to the Russian city of Tomsk as a centre for producing hackers (Rainsford 11 March 2010). Tomsk is mentioned because the files relating to the 'Climategate hack' were leaked and posted on a server there.[4] In the interview, Kaspersky describes Russia as a nation of 'superhackers', and attributes their abilities to good technical education. The graduates at Tomsk are described in the article as facing a choice of either creating sophisticated information protection systems, or joining the ranks of Russia's hackers for hire. However, this description of unemployment as the main reason for hacking in Russia is not always consistent. For instance, *National Defence Magazine* features a former USA intelligence officer's description of Vladimir, who comes from a well educated Russian family and who could be anything he wanted to be, but chose instead to be a cyber thief (Magnuson May 2010).

Another theme in describing Russia as a nation of hackers is the portrayal of Russia and its relationship to its home-grown hackers and cyber crime gangs. Russia is presented as one of the top five countries from where international hacking attacks originate, and as a growing centre of cyber crime. Russia is also portrayed as a top cyber security concern in a Cold War style discourse, a topic to which I return below. Typical examples are representations of Russia as the top producer of viruses, Trojans and spyware, ranking second in generating spam (RT 19 February 2008); Russia as the second largest host of malware according to Sophos (Megerisi 22 March 2010); and Russia as a centre for selling private databases, for example, in the Savelovskii market (Stack 17 March 2010).

[4] In fact, the files were originally uploaded in Turkish and Saudi Arabian servers before Tomsk.

Furthermore, reports on cyber crime gangs, exploits and cyber attacks of various kinds frequently mention the Russian Business Network (RBN), which is described as capable of taking a whole country offline. NATO sees both the RBN and Russian hackers' community as a general threat (RT 8 January 2010). Botnets[5]—one of the frequent tools of cyber attacks—are universally mentioned as a trademark technique of RBN and of Russian hackers in general. Botnets distributing spam and controlling millions of computers are also reported in coverage of the Estonian and Georgian cyber conflicts. In 2009, 75 percent of business structures were reported to have been exposed to various cyber attacks, with Russia being among the top ten countries generating the threat (Secrest 29 April 2010). The reporting of cyber attacks often mentions interviews with experts, and statistics of computer security firms, such as Symantec, Sophos and Kaspersky.[6]

Russians are often described as being arrested for or linked to the most famous cyber crime incidents of the last five years, such as the Charles Schwab brokerage attack or the Royal Bank of Scotland (RBS) robbery of six million pounds in twelve hours (Hawkins 7 April 2010). And lastly, there is a recurrent reference to the Russian mafia's cyber capabilities. However, admittedly, the RBS robbery was not technically sophisticated: the gang hacked into the system cloning 44 debit cards, but it was the coordination of cashers (individuals draining ATMs) that helped pull the robbery off in different countries. Nevertheless, the impression is given that the hackers had super cyber capabilities, as they managed to 'blitz more than 2,000 machines in 28 cities worldwide' (Findlay 14 March 2010). [7]

A central issue that comes up in the cyber crime reports of this type is extradition and the difficulty of trying cyber criminals in the USA. The good cooperation between Russian business and the American Securities and Exchange Commission in the fight against cyber crime also tends to get coverage (Thomson 22 March 2010). Besides cyber crime activities involving millions of dollars, there are also several Internet safety problems and instances where Russians hackers were selling various personal accounts from Gmail to Facebook and to Twitter (Barratt 25 April 2010; Tynan 26 April 2010). As explained by one of the researchers at Kaspersky Labs, Russia comes second in the numbers of cases of password stealing Trojan viruses, accounting for 12 percent of all the incidents, with China accounting for 63 percent (McMillan 29 January 2010).

Inevitably, these stories create a mythology surrounding the abilities of Russian hackers, where they emerge as superhackers with astonishing accomplishments. Russia itself appears as a nation of highly capable hackers, a nation that both nurtures its computer specialists (thanks to its reportedly high quality technical education) and fails them by dooming them to unemployment and lack of opportunities, 'forcing' them to turn to cyber crime.

[5] Botnet is a collection of automatic software agents, which are frequently associated with distribution of spam and malware.

[6] This is in itself problematic, as these companies make profit precisely by selling protection technologies against these types of incidents, thus having vested interests in fuelling anxieties around computer security.

7 A similar report stressed the origin of the cybercriminals: 'A group of Eastern Europeans was charged with hacking into the network of payment processor RBS WorldPay…' (Mills 10 November 2009). Other reports mention the Russian origin of hackers indirectly (Hawkins 7 April 2010; McIntyre 22 December 2009; Crosley 23 December 2009).

Russian Cyber Crime as 'Patriotic' Hacking

Another aspect of mediation of Russian hacking is the alleged link between cyber crime networks, cyber espionage and political hacking. The researcher and blogger Nart Villeneuve argues that there is a potential relationship there as the boundaries between crimeware networks and cyber espionage 'appear to be blurring, making issues of attribution increasingly more complex. It may also indicate that there is an emerging market for sensitive information and/or politically motivated attacks, as crimeware networks seek to monetise such information and capabilities' (Villeneuve 10 April 2010). More importantly, this prompts Villenueve to believe that such attacks demonstrate that botnets involved with criminal activity are being used to conduct both political and apolitical distributed denial-of-service attacks (DDoS) (Villeneuve 10 April 2010).

Examples of this type of activity abound in the Russian and post-Soviet landscape. For instance, the web site of the Russian newspaper, *Novaya Gazeta* [New newspaper], critical of Russian authorities, had experienced six days of downtime due to a hacker attack in 2003 (Periscopeit 3 February 2003). In 2010, *The Guardian* reported a more recent attack on *Novaya Gazeta*, in which the newspaper staff described the scale of the attack as comprising more than a million hits a second on the server. This report suggested that the attack was carried out by a 'highly sophisticated' state agency, displeased with the newspaper's editorial direction (Harding 27 January 2010). Other incidents include attacks on the Polish government system, which coincided with the 70th anniversary of the outbreak of World War II and a visit by Russian Prime Minister Vladimir Putin (Leyden 13 October 2009). In Kyrgyzstan in 2009, two of the country's main Internet service providers, ns.kg and domain.kg, came under a massive denial-of-service attack. Some reports stated the assault had shut down 80 percent of the country's bandwidth. Media descriptions presented this as a case of suspected Russian influence (Weinberger 14 May 2010).

The linking of cyber crime to cyber conflict is explicit in media reports that one of the botnets drafted for the Georgian cyber attack was 'Black Energy', a Trojan horse-hijacked army of PCs thought to have been used to hit Citibank, while 'Black Energy 2' was being used to launch DDoS attacks against Russian banks (Keizer 7 April 2010). The Georgian press also makes the link to cyber conflict explicit by suggesting the involvement of the Russian intelligence service, the Federal Security Service (FSB). According to these reports, the FSB attacked the National Bolshevik Party and moderate opposition groups like 'The Marc of Those Who Disagree', and mainstream media outlets such as *Kommersant* and *Ekho Moskvy*. The reports quote Andrei Soldatov's piece in *Novaya Gazeta*, where he suggests that the FSB did not have to use their own in-house resources, but could simply point the growing community of 'hacker-patriots' in the right direction (Goble 31 May 2007).

In another report from an outlet specialising in national defence, Paul Joyal, the National Strategies Inc. managing director for public safety and homeland security, is quoted saying that there is a nexus between cybercrime and state actors: 'You can be a criminal, a member of an intelligence organisation and a businessman all at the same time' (Magnuson May

2010). RBN, he continues, was 'deeply involved in a cyber attack on Georgia that began weeks before Russian forces invaded the nation in 2008' (Magnuson May 2010).[8]

The reporting of cyber crime, the brilliance of Russian hackers, Russia's portrayal as a centre of cyber crime with the mafia allegedly connected both to government, intelligence services and patriotic hacking are all mentioned in reports of the Estonian and Georgian cyber conflicts in the global media:

> In Estonia in 2007 and in Georgia during the war in 2008, hackers were able to freeze all Internet activity and crucially deny service to banking and government systems. Many accused the Russian government of orchestrating the cyber attacks – a claim Moscow denies, even though *hacking in Russia has a long and well-established history*. (RT 8 January 2010) {emphasis—AK}

The real life event that sparked the cyber conflict in Estonia was the removal of a Soviet war hero statue from Tallinn's square and the subsequent riots that took place in Estonia for several days around the 26th of April 2007, leading to several casualties. By 20th April 2007, although the real world riots calmed down, the country's digital infrastructure was crumbling from cyber attacks. The statue incident reflected deeper tensions and the cultural conflict between the Estonian state and ethnic Russians in Estonia, who make up around one-quarter of the Baltic republic's population of 1.34 million.

Estonia is considered to be an Internet success story due to its e-commerce, and also has strong e-government presence. The Estonian cyber conflict included denial of service attacks, clogging the country's servers and routers, infiltrating the world with botnets, banding computers together and transforming them into 'zombies' hijacked by viruses to take part in such raids without their owners' knowledge. Multiple sources flowed into the system and the attackers even rented time in botnets. The attacks lasted three weeks. The plans of the attackers were posted in Russian language chat rooms with instructions on how to send disruptive messages and which web sites to target. The attacks targeted all levels of the social, political and economic infrastructure: the Estonian presidency and its Parliament, almost all of the country's government ministries and political parties, three of the country's six big news organisations, two of the biggest banks and other firms specialising in communications. Blaming the Russian state for the attacks, the Estonian authorities rapidly mobilized to fight the war, utilising contacts in several countries and requesting NATO and the EU for help.

Although Estonia claimed that the attacks had originated in Russia and the global press similarly linked the attacks to the Russian government, others claimed that nationalist hackers had done most of the work: 'it had been perpetrated by an impromptu "flashmob"…' (Slideshare, n.d.).[9] The Estonian government was also portrayed as going through a 'panic attack', exaggerating the situation when its networks were attacked in cyber space: 'Faced

8 This connection, however, has not been proven.

[9] Members of Nashi, a private pro-Kremlin youth group, also claimed to have had a hand in launching attacks and state-controlled media were reported to have helped whip up Anti-Estonian fervour that may have aided in recruiting hackers. (Weinberger 14 May 2010). According to *Agence France-Presse*, an ethnic Russian student Dmitri Galushkevic, was convicted of attacks against the web site of Estonian Prime Minister, Andrus Ansip (Nichols 25 January 2008).

with DDoS and nationalistic, cross-border hacktivism—nuisances that have plagued the rest of the wired world for the better part of a decade—Estonia's leaders lost perspective' (Poulsen 22 August 2007).

To use the lens of cyber conflict theory, the Estonian case points to ethnonational and cultural elements, with ethnic Russians utilising ICTs to protest their anger at the treatment of Russians in Estonia.[10] The use of patriotic hacking as a facet of hacktivism creates questions in terms of how the groups were organised, their mobilisation, framing and organisation of the attacks. Similar elements of organising are found in sociopolitical cyber conflicts. At the same time, wider issues of cultural conflict and geopolitical tensions need to be explored. Article 5 in NATO's charter states that if a NATO ally is the victim of an armed attack, each and every other member of the alliance should consider this act of violence as an armed attack against all members and should take the actions it deems necessary to assist the ally attacked. As NATO does not yet define electronic attacks as military action, it cannot intervene even when the origin of attack can be proven. Also, the use of information communication technologies is a very convenient and cost-effective tool for protest, usually related to hacktivism and the ethical debates surrounding it. Linked to the real life protests and their online incarnation is the uncertainty about the 'enemy within' and the anxiety about the always incomplete project of national purity, as manifested in the lives of the ethnic Russians in Estonia and elsewhere. These cultural struggles are exacerbated by the media and propaganda, with groups defending the purity of their national space using online technologies.[11]

In the case of the Georgian cyber conflict, the circumstances were different, but here, too, patriotic hacking was the main element. It was reported as a 'virtual war' in cyber space accompanying the brief war in the summer of 2008 between Georgia and Russia. Once again, the media accused Russia of orchestrating the cyber attacks even though it appeared to be due to patriotic hacking by individuals or groups of hackers. Various reports suggested that state organisations provided no support for the cyber attacks during the Georgian cyber conflict.[12]

[10] For a further discussion of Estonian cyber conflict, see Karatzogianni 2009a; Belot and Stroobants 17 June 2007.

[11] The Estonian cyber conflict is also a reflection of the instability of the EU/NATO enlargement project, especially in relation to Russia's hegemonic aspirations, energy and weapon disputes (Karatzogianni 2009a, 6-7).

[12] Sharon Weinberger cites Project Grey Goose, an open-source intelligence initiative, whose analysts 'concluded that nationalist hackers had honed a "cyber-kill chain", which involved recruiting novices by posting patriotic rhetoric and images; publishing and sharing a list of target web sites; discussing malware to use in the attack; and evaluating results for follow-on attacks' (Weinberger 14 May 2010). Another report by a non-profit research group, The USA Cyber Consequences Unit, stated that most of the attackers were Russians, but Russian sympathisers in countries such as Ukraine and Latvia were also involved (Goodin 18 August 2009). The same report confirmed that although the cyber attacks were carried out with little or no direct involvement from the Russian government or military, the timing of the attacks, launched within hours of the Russian military's invasion, could only have come with a fair amount of cooperation from Russian officials (Goodin 18 August 2009).

Tracking the New Cold War rhetoric: Espionage, Security and Crime in Cyberspace

Diplomacy, espionage and security in cyber space were frequently discussed in media narratives of Russia and Russian hackers implicated in cyber conflicts.[13] These issues form part of the narrative which consistently blames Russian hackers for any types of activity involving the use of computers. What emerges here is a new Cold War discourse, often used to discuss together the geopolitics in the region, the role of NATO in maintaining cyber security, and the specific cases linked to Russian hackers.

One telling example is the discussion in the global media of cyber espionage perpetrated by Russia and China.[14] In a report in UK's *Telegraph* Jonathan Evans, the head of MI5, has warned that Britain faces 'unreconstructed attempts by Russia, China and others' who were using 'sophisticated technical attacks' to try and steal sensitive technology on civilian and military projects, along with political and economic intelligence (Gardham 4 December 2009). In the *Times* Evans is mentioned once again, writing to 300 businesses in 2007 to warn them of Chinese hacking attacks and data theft (Loyd 8 March 2010). Anthony Loyd links the interests of hostile state intelligence agencies and cyber criminal syndicates known as *partnerka* [syndicate, partnership], claiming they lead 'commercial espionage in Europe and are known to have links with Harry and his comrades in the FSB' (Loyd 8 March 2010).

Such narratives regarding global security espionage and cyber security are linked in the media to questions about Russia and the participation of countries previously within the Soviet sphere of influence in the NATO. This is particularly prevalent in the media debates around the coverage of Estonian and Georgian cyber conflicts, as well as around NATO's cyber security capabilities, doctrine and general regulation of cyber conflict. The problem is viewed in the mainstream media as NATO's need to develop an agreed concept of what constitutes worldwide cyber security (Austin 10 January 2010). Most of the coverage related to Russia and NATO makes extensive use of the Cold War framework. For example, NATO Secretary-General Rasmussen is reported to have understood the special security concerns of East Europeans 'who chafed under Moscow's decades-long domination during the Cold War, and criticised Russia's new military doctrine' (Reuters 12 March 2010).[15]

Questions of cyber security are also embedded in international politics of secession and recognition. For example, the United States Secretary of State Hilary Clinton has stated that they support Georgia and will neither recognise Abkhazia nor South Ossetia (Civil.Ge 5 De-

[13] An interesting example of how new media and web 2.0 are impacting diplomacy is the use of social networking to raise awareness, raise funds, organise for global issues and boost grass roots diplomacy. This use of new media tools takes place on different levels, from influencing official diplomacy, with Russian President Dmitry Medvedev making the tongue-in-cheek suggestion that he and his USA counterpart Barack Obama begin conducting diplomacy via text message (Earthtimes 14 April 2010) to 'Twitter diplomacy', with a delegation organised by Washington and sent to Russia (Barry 23 February 2010).

[14] For a detailed analysis of Chinese hackers, the Google-China cyber conflict, business and the Sino-American relationship in the global system, see Karatzogiannni 10 March 2010.

15 In terms of the real environment and geopolitics of the Georgian cyber conflict, Russia sees armament in Georgia as a serious problem and it has brought it up in NATO meetings in Brussels after the war. (Petro 13 November 2009). In December 4 2009, NATO and Russia resumed their political dialogue, which NATO had broken off after the war in Georgia (Khashig and Ponomarev 13 December 2009).

cember 2009). South Ossetia was the reason for the war between Russia and Georgia, with Russia recognising South Ossetia and Abkhazia's quest for independence.[16] As Nikolai Petro explains in an interview, set up by Saylor Company (a USA public relations firm employed by the governments of Abkhazia and South Ossetia), these two countries seem to be on quite different trajectories. While Abkhaz leaders have always been clearly focused on obtaining international recognition as a sovereign state, some South Ossetian leaders seem to aspire to some form of integration with North Ossetia, within the Russian Federation (Petro 13 November 2009). Paul Goble, writing in the *Georgian Daily*, mentions the analysis of Anatoly Chekhoyev, a former secretary of the South Ossetian Oblast' committee of the Communist Party of the Soviet Union (CPSU), who also served in the USASR Supreme Soviet and Russian Duma. He asked his listeners to consider what might have happened if Moscow had not acted as it did; 'if Russia had stayed silent, then one could have shaken loose Daghestan, Chechnya, Ingushetia and all the rest with the wave of a hand' (Goble 28 November 2009).

Besides the international relations aspects of the Russian-Georgian war, there are regional media issues linked to this case. 'The only war we can win against Russia is an information war, so we shouldn't miss our chance', argued the Georgian politician analyst Tornike Sharashenidze (Kiguradze 13 November 2009). The Georgian media environment is described as highly politicised with broadcasters providing either intensely pro-government or pro-opposition view (UNCHR 16 February 2009). In that kind of environment, it is not surprising that there are conflicts beyond what my brief discussion of cyber conflict has shown.[17]

The actual Georgia-South Ossetia cyber conflict started the same day as the military offensive on the 8th of August 2008, although attacks were also registered in July. The web sites of the president of Georgia, the Georgian Parliament, the ministries of defence and foreign affairs, the National Bank of Georgia and online news agencies were attacked, with the cyber conflict becoming more intense as the real conflict escalated. Images of Hitler were manipulated and juxtaposed on the Georgian President. The Georgian response involved using filters to block Russian IP addresses, moving web sites elsewhere, and appealing to Estonia and other countries for help. Estonia dispatched specialists and Poland provided web sites for Georgian use (Heickero March 2010).

Possibly the most fascinating discussion on the Georgian cyber conflict comes in the form of a journal article written by Stephen Korns and Josua Kastenberg and published in *Parameters*. In their article, they reaffirm the view that most security experts have attributed

16 The only other countries recognizing them are Venezuela and Nicaragua, Peru and small states like Nauru (The Georgian Times 14 April 2009). For a detailed discussion of cyber conflict in unrecognized states see Karatzogianni, forthcoming.

17 For instance, there are efforts at operating television channels from both sides of the conflict. In January 2010, the Georgian Public Broadcaster inaugurated its first Russian language television channel, *Pervyi Kavkazskii* [First Caucasian]. When the channel further widened its range of coverage by becoming available on the French-operated satellite provider Eutelsat across almost the entire post-Soviet space, Eutelsat discontinued transmitting the channel, invoking suspicions that the Russian authorities were implicated in the decision. Oleg Panfilov, the Head of the Center for Journalism in Extreme Situations, and a host on First Caucasus, said to *Eurasia Monitor:* 'During the Russian aggression against Georgia in August 2008, ordinary people in various parts of the post-Soviet space could not receive objective information in the Russian language, while the Kremlin enjoyed an information monopoly' (Kvelashvili 5 February 2010). Meanwhile, *Russia Today* reported that as the channel is targeting ethnic minorities in the Caucasus region, it would act as a Georgian propaganda tool (RT 14 November 2009).

the 2008 DDoS attacks to 'an amalgam of government-incentivised agents, hackers and cyber citizen protestors' (Korns and Kastenberg 2009, 66). They give the example of an Internet journalist who accessed a Web site and downloaded prepackaged software that would have enabled him, to join in the attacks, had he chosen to do so (Morozov 2008 in Korns and Kastenbeg 2009, 65).

Korns and Kastenberg make very interesting observations about this cyber conflict. First, they bring up the issue of cyber neutrality: in contrast to Estonia, which experienced cyber attacks, but essentially defended in place, Georgia maneuvered by relocating strategic IP-based cyber capabilities to a private company in the USA (Korns and Kastenberg 2009, 68). Korns and Kastenberg believe that Georgia's unconventional response to the August 2008 DDoS attacks, supported by USA private industry, adds a new element of complication for cyber strategists (Korns and Kastenberg 2009, 61). Secondly, they show that since the 2001 Council of Europe Convention on Cyber crime, to which the United States is a party, omits any reference to the terms 'cyber attack' or 'cyber weapons', cyber attacks are currently part of cyber *crime* and not cyber *war* as such. From that perspective it would have been Interpol, rather than NATO that would have to respond to Estonia and Georgia (Korns and Kastenberg 2009, 64-65).

To push Korns' and Kastenberg's argumentation further, any cyber attack could be framed as cyber crime and prosecuted as such, unless it is part of an armed conflict. This implies that any political hacking could be prosecuted as a (cyber) crime. Indeed one of the patriotic hackers (or a cultural protester, as he was portrayed by some) in the Estonian cyber conflict discussed earlier was convicted and fined for his activities. This shift could potentially mean that electronic disobedience or hacktivism as we know them, could also be prosecuted as criminal activities, despite their mostly symbolic effects. An additional problem here is the difficulty in determining with certainty the origin of cyber attacks, or establishing whether an attack is a state-sponsored mission or ad hoc initiative. As Korns and Kastenberg put it, 'cyber conflict between nations is a serious concern, but as the Georgian DDoS attacks demonstrate, perhaps of even greater concern is the growing trend of cyber conflict between nations and ad hoc assemblages' (Korns and Kastenberg 2009, 70).

The Estonian cyber conflict led to the establishment of a Cooperative Cyber Defence Centre of Excellence[18] by NATO in 2008 in Tallinn (Johnson 16 April 2009). Furthermore, in May 2010, the secretary of Defence Robert Gates announced the activation of the Pentagon's first comprehensive, multi-service cyber operation, the USA Cyber Command (CYBERCOM), with Keith Alexander as its commander. Talking about cyber space as the fifth battle space, transferring soldiers from communications and electronics to an Army Forces cyber command, and wondering on how cyber warriors should be trained, confirms a trend toward militarisation of what was previously a criminal and commercial matter (Rozoff 26 May 2010). With Russia and China frequently depicted as the main suspects, the USA and its NATO allies have had to address cyber warfare questions in its twenty first century strategic concept. With 120 countries developing cyber capabilities, NATO's Director of Policy Planning Jamie Shea commented that 'there are people in the strategic community who say cyber

[18] Known as CCD COE or K5.

attacks now will serve the same role in initiating hostilities as air campaigns played in the twentieth century' (Rozoff 26 May 2010).

NATO will have to eventually create a coherent strategy for cyber warfare. This problem has been addressed by various authors (Central European University, 7-8 June 2010). In June 2010, the *Sunday Times* reported that a team of NATO experts led by former USA Secretary of State, Madeleine Albright, prepared a document stating that a cyber attack on the critical infrastructure of a NATO country could equate an armed attack, justifying retaliation (Smith and Warren 6 June 2010). The organisation's lawyers were reported saying that since the effect of a cyber attack can be similar to an armed assault, there is no need to redraft existing treaties. If an attack on critical infrastructure resulted in casualties and destruction comparable to a military attack, then the mutual defence clause of Article 5 could be invoked. Still, the level of attack is not exactly clear, as the perception of dangers of cyber warfare continues to change.

The New Russian Stereotype and the 'Climategate Hack'

To conclude the discussion of Russian hackers, let me now turn to the Climategate hack – an incident which was consistently attributed to Russia by the global media. This attribution became particularly clear after several key figures, such as Professor Jean-Pascal Ypersele, the vice chairman of the Inter-governmental Panel on Climate Change, supported the Russian hackers scenario. Here are some typical examples of the narratives that followed: 'Russian hackers illegally obtained 10 years of e-mails between the world's top climate change scientists' (Kolasinski 4 December 2009); 'The British media and some U.N. scientists have suggested that the Russian secret service, the FSB, was complicit in the theft' (Snapple 7 January 2010); 'The guiding hand behind the leaks, the allegation went, was that of the Russian secret services' (Walker 7 December 2009); 'Russia, a major oil exporter, may be trying to undermine calls to reduce carbon emissions' (Telegraph 6 December 2009); 'This is not the first time Russian hackers have created global Internet disarray' (MacNicol 7 December 2009); 'Russian computer hackers are suspected of being behind the stolen e-mails' (McCarthy and Owen 6 December 2009). A typical coverage in the *Times* by Tony Halpin sums all the reasons why Russian hackers and Russia were immediately implicated: Russia's desire to discredit the summit, poor talented but unemployed hackers, the RBN and the use of patriotic hackers by the FSB. All these were connected together, fitting the overall move to blame Russian hackers – a move already built up by the global media (Halpin 7 December 2009).

Most media representations of the Climategate hack linked the events to other incidents in the past, suggesting a consistent narrative frame which blames the attacks on Russian hackers. Russian hackers were ideal in that respect. Although the Climategate material was uploaded on various servers in Turkey and Saudi Arabia before ending up in Tomsk in Siberia, it was Tomsk that became the key factor in the Russian hackers' story. Reporters interviewed students in Tomsk, where a computer school was located, and it was also states that 'in 2002 Tomsk students launched a 'denial of service' attack at the Kavkaz-Tsentr portal, a site whose reports about Chechnya angered Russian officials'. The FSB office in Tomsk put out a special Press release stating that the students' actions had been a legitimate 'expression

of their position as citizens, one worthy of respect' (Stewart and Delgado 6 December 2009; also reported by Merchant 7 December 2009). Around the same time, the media frequently linked the Georgian and Estonian cyber conflicts, implicating the Russian security service and accusing the Russian police of turning a blind eye to cyber crime (Judge 7 December 2009).

Several reports, however, began deviating from the general certainty and consensus that attributed the Climategate hack to the Russians. Since hackers used open proxies to mask their identities, they could have originated from anywhere in the world. And if Russian hackers where indeed involved, leaving the files at Tomsk would be too obvious. And yet, most reports pointed a finger at Russian hackers. The media repeatedly mentioned Russian hackers' sophistication, linking it to earlier, equally skilful attacks. In the case of the Climategate hack, the impression was given that the hackers selected specific information implicating the scientists of the past 13 years. None of the media reports mentioned that the files titled after freedom of information act might have been collected by someone working at the University of East Anglia. Fred Pearce reported, for example, a number of people claim to have stumbled on non-public files on the UEA server in the months prior to the hack. Among them was David Holland, a British engineer and an amateur climate skeptic, who in December 2008 notified the University that the search engine on their home page was broken and falling through to a directory. In November 2009, Charles Rotter, the moderator of the blog Whatts Up With That (http://wattsupwiththat.com/), wrote that in July of that year he had discovered that the University had left station data versions from 2003 and 1996 on its server, and that those who knew where to look could find the files available in public access (Pearce 9 February 2010).

There are other reasons why the leak version might be more plausible than an attack by Russia or Russian hackers. Lance Levsen, for example, has argued that if the file was not already collected and stolen, the actual collection of the material and cracking meant a super-sophisticated operation. A reasonable explanation for the archive being in such a state is that the FOI Officer at the University was practicing due diligence and that someone at UEA found the file and released it into the wild. The release of FOIA2009.zip could have occurred not because of a hacker, but because of a leak from UEA by a person with scruples (Levsen 7 December 2009). Also, notably, the 'hackers' made several efforts at disseminating the material before succeeding; this, once again, is not consistent with the pattern of how Russian hackers would operate.[19] And lastly, the fact that the documents were on a server due to computer security failure at UEA, and then 'magically' found their way to climate change bloggers (Pearce 9 February 2010), provides another competing explanation to the Russian hacking scenario. *The Guardian* reported that Norfolk police interviewed climate researcher Paul Dennis, who heads an adjacent laboratory at UEA and had e-mail contact with Ameri-

[19] Paul Hudson, a weatherman and climate change skeptic was sent a sample, a month before the documents were leaked, but did not use it (Leigh et al. 4 February 2010b). Matthew Taylor and Charles Arthur explain that a month after Hudson received his sample, someone hacked into the RealClimate web site, using a computer in Turkey, and uploaded a zip file containing all 4,000 emails and documents. At that point, the web site's co-founder shut down the site. Then hackers used a computer in Saudi Arabia to post a fresh copy of the zip file, this time stored on the Tomsk server. Then the incident was picked up by blogs and organisations all over the world (Taylor and Arthur 27 November 2009). Eventually the story spread through climate change skeptic sites and then found its way into the mainstream media (Hurlbut 20 November 2009).

can bloggers such as McIntyre of the Climategate Audit, Patrick Condon of the Air Vent and Anthony Watts of Watts Up With That. All these bloggers were sent the leaked material. A connection to Russian hackers, indeed, was not proven. Moreover, according to The Guardian, Norfolk police has discounted tabloid stories of links to Russian intelligence in this incident (Leigh et al. 4 February 2010a).

Conclusion

The way Russian cyber crime gangs and incidents are narrated by global mainstream media, alternative media and bloggers, shapes a very specific portrayal of Russian hackers and their superior abilities in relation to hacking and cyber crime. There is no significant difference between mainstream and independent media and blogs, except that in blogs the bias against Russians is often far more explicit. The hackers are consistently portrayed as having 'incredible' powers to support criminal activities, attack opposition groups' virtual presence or hack for the benefit of the state in time of need. This stereotypical depiction of Russian hackers is reminiscent of Cold War imagery, such as that of the incredibly intelligent Russian spies who are forced to work for their government to survive poor living conditions. At the same time, this depiction creates a consistent narrative frame to explain any international incident as one carried out by this specific ethnic and cultural group. This narrative frame helps explain the certainty with which the 'Climategate hack' was attributed to Russian hackers without any valid proof and based solely on speculation.

The main argument of this article is that the ammunition for blaming the Russian hackers for the Climategate hack is to be found in the public discourse that portrays Russians as super hackers and links cyber crime to patriotic hacking, international espionage and global politics. This explains media stories of Russia's government and politico-economic elite allegedly intermingling with the Russian mafia and cyber crime gangs to get support during cyber conflicts, in which the Russian state is opposed (cyber attacks against opponents), implicated (Estonia) or is engaged in a brief war, as was the case with Georgia.

The global media have portrayed Russian hackers in a consistent manner, playing up their capabilities (such as, for example, their sophistication) and linking them to cyber crime gangs, robberies and identity thefts. Even if there are indeed individuals from Russia or elsewhere in the post-Soviet space who are engaged in cyber crime, the assumption of Russian guilt in all cases reinforces the older Cold War portrayal of Russians in the Western world. There is a demonstrated tendency for the global media to look for a Russian hand and geopolitical implications in stories relating to former Soviet countries or countries under Soviet influence in the past. Also, there has been an exaggeration of the sophistication of Russian hackers, primarily because of their use of botnets to conduct attacks previous to the Climategate hack, particularly in patriotic hacking in the cases of Estonia and Georgia. By the time the 'Climategate hack' appeared with a huge impact just before the Copenhagen summit, the scene was set for Russian hackers to be blamed for what under a calmer mindset might have been more plausibly explained differently or at least reported alongside another, competing explanation.

Acknowledgements

Warmest thanks to the guest editor Adi Kuntsman for her detailed and highly constructive response to the earlier version of the article, and to the three anonymous reviewers for their creative suggestions for improvement. This article was written before the story of Russian spies, arrested by the FBI and later exchanged with counterparts in Russia, broke out in June 2010. It would be both amusing and academically worthwhile to explore the global coverage of that story in light of the discussion of espionage, cyber security and the new Cold War rhetoric presented in this article.

References

Karatzogianni, Athina. *The Politics of Cyber Conflict*, Routledge Research on Internet and Society. Routledge: London and New York, 2006.

————. 'Introduction: New media and the Reconfiguration of Power in Global Politics', in *Cyber Conflict and Global Politics*, edited by Athina Karatzogianni. Routledge Series Contemporary Security Studies, Routledge: London and New York, 2009a, pp. 1-10.

————. 'How small are small numbers in cyber space? Small, virtual, wannabe "states," minorities and their cyber conflicts', in *Cyber Conflict and Global Politics*, edited by Athina Karatzogianni. Routledge Series Contemporary Security Studies, Routledge: London and New York, 2009b, pp. 128-145.

————. 'The Thorny Triangle: Cyber Conflict, Business and the Sino-American relationship in the Global system', *e-International Relations*, 10 March 2010. <http://www.e-ir.info/?p=3420> (accessed April 2010)

————. *The Real, The Virtual, and the Imaginary State: Cyber Conflict in Small and Unrecognised States*, Media and Cultural Studies, Basingstoke: Palgrave Macmillan (forthcoming).

Simons, Greg. *Mass Media and Modern Warfare: Reporting on the Russian War on Terrorism*, Surrey: Ashgate, 2010.

Zhang, Juyan and Fahmy, Shahira. 'Color Revolutions in Colored Lenses: A Comparative Analysis of USA and Russian Press Coverage of Political Movements in Ukraine, Belarus and Uzbekistan', *International Journal of Communication*, 3 (2009), pp. 517-539.

Internet Sources [All articles were last accessed 10-17 May 2010]

AFP. 'EU satellite centre to monitor Georgia rebel zones: official'. 13 November 2009. <http://www.reliefweb.int/rw/rwb.nsf/db900SID/SNAA-7XU7T9?OpenDocument>..

Asia Computers. 'Russian hackers embarrass Microsoft'. 31 March 2010. <http://asia-computers.com/russian-hackers-embarrass-microsoft/>.

Austin, Greg. 'NATO and the 'Evil Cyber Empire': Surprising Futures!' *New Europe*, 10 January 2010. <http://www.neurope.eu/articles/98357.php>.

Backwell, Ben. 'Pachauri condemns hackers attempt to 'discredit' IPCC'. 7 December 2009. <http://www.rechargenews.com/business_area/politics/article200932.ece>.

Barley, Shanta. 'Climategate: Russian secret service blamed for hack'. *New Scientist*, 7 December 2009. <http://www.newscientist.com/blogs/shortsharpscience/2009/12/since-over-1000-confidential-e.html>.

Barratt, Joseph. 'Facebook hacker claims to be in NZ', *New Zealand Herald*, 25 April 2010. <http://www.nzherald.co.nz/connect/news/article.cfm?c_id=1501833&objectid=10640757>.

Barrett, Larry. 'Russian hackers manipulated stock prices: SEC'. 17 March 2010. <http://www.internetnews.com/security/article.php/3871201/Russian-Hackers-Manipulated-Stock-Prices-SEC.htm>.

Barry, Ellen. 'Washington sends delegation to Moscow, via Silicon Valley', *The New York Times*, 23 February 2010. <http://www.nytimes.com/2010/02/24/world/europe/24russia.html>.

BBCNews. 'No malpractice' by practice', 14 April 2010. <http://news.bbc.co.uk/1/hi/sci/tech/8618024.stm>.

Belot, Laure and Stroobants, Jean-Pierre. 'Les Temps des cyber guerres', *Le Monde*, 17 June 2007. <http://www.lemonde.fr/web/article/0,1-0,36-924253,0.html>.

Bentley, Ed. 'Were Russians hackers behind Climategate?' *Moscow News*, 14 December 2009. <http://www.mn.ru/interview/20091214/55397385.html>.

Booker, Christopher. 'Climategate: A scandal that won't go away', *Telegraph*, 17 April 2010. <http://www.telegraph.co.uk/comment/columnists/christopherbooker/7601929/Climategate-a-scandal-that-wont-go-away.html>.

Cavanaugh, Tim. 'Not with a bang but a twitter: Interwebs bring new dark ages'. 26 January 2010. <http://reason.com/blog/2010/01/26/not-with-a-bang-but-a-twitter>.

Central European University. Participants' reflections on workshop themes. 'Cyber security: Europe and the Global Society Revisited: Developing a network of scholars and agenda for social science research on cyber security', *Budapest Hungary*, 7-8 June 2010, <http://ww.cmcs.ceu.hu/cybersecurity/main>.

Charles the moderator. 'The CRUtape Letters™, an Alternative Explanation'. 23 November 2009. <http://wattsupwiththat.com/2009/11/23/the-crutape-letters®-an-alternate-explanation/>.

Cheek, Michael. 'What is Cyber war anyway? A conversation with Jeff Carr, author of Inside Cyber Warfare', 2 March 2010. <http://www.thenewnewinternet.com/2010/03/02/what-is-cyberwar-anyway-a-conversation-with-jeff-carr-author-of-inside-cyber-warfare/>.

Civil.Ge. 'Lavrov: 'Georgia Armament serious problem'. 5 December 2009. <http://www.civil.ge/eng/article.php/article.php?id=21754>.

Computer Fraud and Abuse Act, 18 U.S.C. 1030. <http://www4.law.cornell.edu/uscode/18/1030.html>.

Connor, Steve. 'Climate e-mails hacked by spies', *The Independent*, 1 February 2010. <http://www.independent.co.uk/environment/climate-change/climate-emails-hacked-by-spies-1885147.html>.

Cosgrove, Michael. 'The Great Climate debate commits suicide',10 February 2010. <http://www.fleshandstone.net/commentary/1759.html>.

Council of Europe. *Convention on Cyber Crime*, Budapest. 23 November 2001. <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

Crosley, Keith. 'Did Russian hackers attack Citibank?' *Business Computing World*, 23 December 2009. <http://www.businesscomputingworld.co.uk/did-russian-hackers-attack-citibank-also-top-banking-information-security-threats-and-a-great-security-resource/>.

Deutsche Presse-Agentur. 'NATO urges Georgia to improve ties with neighbouring countries', 4 December 2009. <http://www.india-server.com/news/nato-urges-georgia-to-improve-ties-with-17329.html>.

Earthtimes. 'Medvedev proposes 'text messages' diplomacy', 14 April 2010. <http://www.earthtimes.org/articles/show/318749,medvedev-proposes-text-message-diplomacy--summary.html>.

Eshel, David. 'Israel adds cyber-attack to IDF', *Military.com*, 10 February 2010. <http://www.military.com/features/0,15240,210486,00.html>.

Etengoff, Aharon. 'Hackers steal confidential global warming data', 21 November 2009. <http://www.tgdaily.com/security-features/44763-hackers-steal-confidential-global-warming-data>.

EUbusiness. 'EU calls on Russia to pull out of disputed Georgian village', 11 December 2009. <http://www.eubusiness.com/news-eu/georgia-russia.1x3>.

Evron, Gadi. 'Internet Attacks Against Georgian Websites', *CircleID*, 11 August 2008. <http://www.circleid.com/posts/88116_Internet_attacks_georgia>.

Freeguide. 'Windows phone 7 managed to be installed on HTC HD2', 1 April 2010. <http://www.freeguide.me/web/windows-phone-7>.

Findlay, Russel. 'Royal Bank of Scotland raiders' huge £6m haul in just 12 hours', 14 March 2010. <http://www.dailyrecord.co.uk/news/business-news/2010/03/14/royal-bank-of-scotland-raiders-huge-6m-haul-in-12-hours-86908-22110087/>.

FoxNews. 'Climate skeptics see 'smoking gun' in researchers' leaked e-emails'. 21 November 2009. <http://www.foxnews.com/scitech/2009/11/21/climate-skeptics-smoking-gun-researchers-leaked-e-mails/>.

Gardham, Duncan 'Cold war enemies Russia and China launch a cyber attack every day', *Telegraph*, 4 December 2009. <http://www.telegraph.co.uk/technology/news/6727100/Cold-war-enemies-Russia-and-China-launch-a-cyber-attack-every-day.html>.

Georgian Times. 'Nauru may recognise South Ossetia's independence', 14 April 2009. <http://www.geotimes.ge/index.php?m=home&newsid=19592>.

Gillis, Justin. 'British Panel Clears Scientists', 7 July 2010. *New York Times*. <http://www.nytimes.com/2010/07/08/science/earth/08climate.html?_r=1>.

Goble, Paul. 'Moscow might have lost North Caucasus if it hadn't aided South Ossetia, former CPSU official says', 28 November 2009. <http://georgiandaily.com/index.php?option=com_content&task=view&id=15833&Itemid=65>.

————. 'Window on Eurasia: FSB encourages, guides Russia's 'Hacker-Patriots', 31 May 2007 <http://windowoneurasia.blogspot.com/2007/05/window-on-eurasia-fsb-encourages-guides.html>.

Goodin, Dan. 'Georgian cyber attacks launched by Russian crime gangs', *The Register*, 18 August 2009. <http://www.theregister.co.uk/2009/08/18/georgian_cyber_attacks/>.

————. ‘Climate change hackers leave breadcrumb trail’, 25 November 2009. <http://www.theregister.co.uk/2009/11/25/cru_climate_hack_identity/>.

Halpin, Tony. ‘Is Russia behind the Climategate hackers?’ T*imes Online,* 7 December 2009. <http://www.timesonline.co.uk/tol/news/environment/article6946385.ece>.

Harding, Luke. ‘Alexander Lebedev sells Aeroflot and air-leasing stakes for $575m’, *The Guardian*, 27 January 2010. <http://www.guardian.co.uk/media/2010/jan/27/lebedev-sells-aeroflot-stake>.

Harvey, Fiona. ‘E-mail scandal dominates debate on rail road to Copenhagen’, *Financial Times blogs*, 5 December 2009. <http://blogs.ft.com/energy-source/2009/12/05/email-scandal-dominates-debate-on-rail-road-to-copenhagen/>.

Hawkins, Asher. ‘3 Year for hacker who ripped off Charles Schwab accounts’, *Forbes blogs*, 7 April 2010. <http://blogs.forbes.com/moneybuilder/2010/04/07/3-year-sentence-for-hacker-who-ripped-off-charles-schwab-accounts/>.

Heickero, Ronald. ‘Emerging cyber threats and Russian views on Information warfare and Information operations’, Swedish Defence Research Agency, Defence Analysis. March 2010. <http://www.foi.se>.

Hickman, Leo and Randerson, James. ‘Climate sceptics leaked e-mails are evidence of collusion among scientists’, *The Guardian*, 20 November 2009. <http://www.guardian.co.uk/environment/2009/nov/20/climate-sceptics-hackers-leaked-emails>.

Hoffman, Stefanie. ‘RSA: Security expert says USA is already engaged in cyber war’, *CRN*, 4 March 2010. <http://www.crn.com/security/223101637;jsessionid=34XLIZKR4BA4VQE1GHOSKHWATMY32JVN>.

House of Commons. ‘Science and Technology Committee - Eighth Report. The disclosure of climate data from the Climatic Research Unit at the University of East Anglia’, 24 March 2010. <http://www.publications.parliament.uk/pa/cm200910/cmselect/cmsctech/387/38702.htm>.

Hurlbut, Terry. ‘CRU files scandal reaches print media’, *The Examiner*, 20 November 2009. <http://www.examiner.com/x-28973-Essex-County-Conservative-Examiner~y2009m11d20-CRU-files-scandal-reaches-print-media>.

Immunet ‘Beware of hackers ‘liking your profile too much: Facebook changes call for user vigilance’, 27 April 2010. <http://blog.immunet.com/blog/2010/4/27/beware-of-hackers-liking-your-profile-too-much-facebook-chan.html>.

ITComputerzone. ‘Russian hackers accused mastermind of attacks Twitter’, 9 August 2009. <http://itcomputerzone.com/internet/russian-hackers-accused-mastermind-of-attacks-twitter.html>.

Johnson, Bobbie. ‘No one is ready for this’, *The Guardian*. 16 April 2009. <http://www.guardian.co.uk/technology/2009/apr/16/internet-hacking-cyber-war-nato>.

Johnson, Keith. ‘Climate: Whodunnit?’ *Wall Street Journal Blogs*, 8 December 2009. <http://blogs.wsj.com/environmentalcapital/2009/12/08/climategate-whodunnit/>.

————. ‘Climategate: The fallout continues from CRU hacking’, 30 November 2009. <http://blogs.wsj.com/environmentalcapital/2009/11/30/climategate-the-fallout-continues-from-cru-hacking/tab/article/>.

Judge, Peter. 'Russia accused of Climategate hack', *E-Week Europe*, 7 December 2009. <http://www.eweekeurope.co.uk/news/news-security/russia-accused-of-climategate-hack-2674>.

Kaplun, Alex. 'E-Mails Show Scientists Planning Push-Back Against 'McCarthyite' Attacks on Climate Science', *New York Times*, 5 March 2010. <http://www.nytimes.com/gwire/2010/03/05/05greenwire-e-mails-show-scientists-planning-push-back-aga-33296.html>.

Keizer, Gregg. 'Botnets 'the Swiss Army knife of attack tools', 7 April 2010. <http://www.computerworld.com/s/article/9174560/Botnets_the_Swiss_Army_knife_of_attack_tools_>.

Khashig, Ruslan and Ponomarev, Sergey. 'Abkhaz election again pits Russia against Georgia', 13 December 2009. <http://www.etaiwannews.com/etn/news_content.php?id=1131528&lang=eng_news&cate_img=logo_world&cate_rss=WORLD_eng>.

Kiguradze, Temuri. 'Public debates on the war report in Tbilisi', *The Messenger Online*, 13 November 2009. <http://www.messenger.com.ge/issues/1982_november_13_2009/1982_temo.html>.

Kolasinski, Taylor. 'An inconvenient hoax', *The Daily Evergreen Online*, 4 December 2009. <http://www.dailyevergreen.com/story/31800>.

Korns, Stephen.W. and Kastenberg, Joshua E. 'Georgia's cyber left hook', Parameters: 38.4 : 60-76, USA Army War College. 2009. <http://www.carlisle.army.mil/usawc/Parameters/08winter/korns.pdf>.

Kvelashvili, Giorgi. 'Georgia's Arduous Attempt to Challenge Moscow's Broadcasting Monopoly', *Eurasia Daily Monitor*, Volume: 7 Issue: 25. 5 February 2010. <http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=36017&tx_ttnews%5BbackPid%5D=7&cHash=30ac2d2fad>.

Leigh, David, Arthur, Charles and Evans, Rob. 'Detectives question climate change scientist over e-mail leaks', *The Guardian*, 4 February 2010a <http://www.guardian.co.uk/environment/2010/feb/04/climate-change-email-hacking-leaks>.

Leigh, David, Arthur, Charles and Evans, Rob and Pearce, Fred. 'Climate e-mails: were they really hacked or just sitting in cyber space?' *The Guardian*, 4 February 2010b. <http://www.guardian.co.uk/environment/2010/feb/04/climate-change-email-hacker-police-investigation>.

Le Page, Michael. 'Why there is no sign of a climate conspiracy in hacked e-mails'. New Scientist. 4 December 2009 <http://www.newscientist.com/article/dn18238-why-theres-no-sign-of-a-climate-conspiracy-in-hacked-emails.html>.

Levsen, Lance. 'Comprehensive network analysis shows Climategate likely to be a leak', 7 December 2009. <http://wattsupwiththat.com/2009/12/07/comprhensive-network-analysis-shows-climategate-likely-to-be-a-leak/>.

Leyden, John. 'Polish government cyber attack blamed on Russia', *The Register*, 13 October 2009. <http://www.theregister.co.uk/2009/10/13/poland_cyberattacks/>.

————. 'Russian trade body aims to fight cyber crime', *The Register*, 12 April 2010. <http://www.theregister.co.uk/2010/04/12/russia_cybercrime_feature/>.

Loginof.com 'Famous researcher talks about Internet in Russia', 18 February 2010. <http://loginof.com/2010/02/famous-researcher-talks-about-internet-in-russia/>.

Loyd, Anthony. 'Britain applies military thinking to the growing spectre of cyber war', 8 March 2010. <http://technology.timesonline.co.uk/tol/news/tech_and_web/article7053270.ece>.

Macdonald, Cameron. 'FBI agent visits Monterey Trail High', *Elk Grove Citizen*, 13 April 2010. <http://www.egcitizen.com/articles/2010/04/13/news/doc4bc4fe6887a33275902281.txt>.

MacNicol, Glynnis. 'Are Russian hackers responsible for creating Climategate?' 7 December 2009. <http://www.mediaite.com/online/are-russian-hackers-responsible-for-creating-climategate/>.

Magnuson, Stew. 'Russian Cyber thief case illustrates security risks for U.S>. corporations', May 2010. <http://www.nationaldefensemagazine.org/archive/2010/May/Pages/RussianCyberthiefCaseIllustratesSecurityRisks.aspx>.

McCarthy, Michael and Owen, Jonathan. 'Climate change conspiracies: Stolen e-mails used to ridicule global warming', *The Independent*, 6 December 2009. <http://www.independent.co.uk/environment/climate-change/climate-change-conspiracies-stolen-emails-used-to-ridicule-global-warming-1835031.html>.

McIntyre, Douglas. 'FBI says Russian hackers hit Citigroup for tens of millions', *Daily Finance*, 22 December 2009. <http://www.dailyfinance.com/story/fbi-says-russian-hackers-hit-citigroup-for-tens-of-millions/19290466/>.

McMillan, Robert. 'Stolen Twitter accounts can fetch $1,000', 29 January 2010. <http://www.computerworld.com/s/article/9150001/Stolen_Twitter_accounts_can_fetch_1_000>.

Megerisi, Hani. 'Russia arrests $9million cash machine hackers', 22 March 2010. <http://www.pcpro.co.uk/news/security/356617/russia-arrests-9-million-cash-machine-hackers>.

Merchant, Brian. 'Ex-KGB officers may be the hackers behind ClimateGate', *Treehugger*, 7 December 2009. <http://www.treehugger.com/files/2009/12/ex-kgb-officers-hackers-climategate.php>.

Mills, Elinor. 'Eastern Europeans charged in payment processor hack', *CNET News*, 10 November 2009. <http://news.cnet.com/8301-27080_3-10394558-245.html>.

Morozov, Evgeny. 'An Army of Ones and Zeroes: How I Became a Soldier in the Georgia-Russia Cyber war', *Slate.com*, 14 August 2008. <http://www.slate.com/id/2197514>.

Newton, Paula. 'Tracking down the 'Climategate' hackers', *CNN*, 11 December 2009. <http://edition.cnn.com/2009/WORLD/europe/12/11/hacking.emails.climate.skeptics/index.html>.

Nichols, Shaun. 'First hacker convicted for Estonia attacks', 25 January 2008. <http://www.v3.co.uk/vnunet/news/2208059/first-hacker-convicted-estonia>.

Parker, Judson. 'Climategate debunked', *The Examiner*, 27 November 2009. <http://www.examiner.com/x-29137-Tallahassee-Environmental-News-Examiner~y2009m11d27-Climategate-debunked>.

Pearce, Fred. 'Hacked archive provides fodder for climate sceptics', 24 November 2009. <http://www.newscientist.com/article/dn18192-hacked-archive-provides-fodder-for-climate-sceptics.html>.

————. ‘Search for hacker may lead police back to East Anglia’s climate research unit’, *The Guardian*, 9 February 2010. <http://www.guardian.co.uk/environment/2010/feb/09/hacked-emails-police-investigation>.

————. ‘How the “climategate” scandal is bogus and based on climate sceptics' lies’, *The Guardian*, 9 February 2010. <http://www.guardian.co.uk/environment/2010/feb/09/climategate-bogus-sceptics-lies>.

Periscope it. ‘Hacker attack takes Russian newspaper offline for days’, 3 February 2003. <http://www.periscopeit.co.uk/website-monitoring-news/article/hacker-attack-takes-russian-newspaper-offline-for-days/594>.

Petro, Nicolai. N. ‘Russia is miscast in the Georgian tragedy’, 13 November 2009. <http://www.opednews.com/populum/diarypage.php?did=14946>. [questions prepared by Saylor Company, a USA public relations firm employed by the governments of Abkhazia and South Ossetia].

PINewswire. ‘New Blackenergy Trojan targeting Russian, Ukrainian banks’, 12 March 2010. <http://www.pinewswire.net/2010/03/new-blackenergy-trojan-targeting-russian-ukrainian-banks/>.

Poulsen. Kevin. ‘Cyber war’ and Estonia’s panic attack’, *Wired*, 22 August 2007. <http://www.wired.com/threatlevel/2007/08/cyber-war-and-e/>.

RA-10 Inquiry Report: Concerning the Allegations of Research Misconduct Against Dr. Michael E. Mann, Department of Meteorology, College of Earth and Mineral Sciences, The Pennsylvania State University. 3 February 2010 <http://www.research.psu.edu/orp/Findings_Mann_Inquiry.pdf>.

Radio New Zealand News. ‘UN defends scientists over leaked e-mails’, 6 December 2009. <http://www.infowars.com/un-defends-scientists-over-leaked-emails/>.

Rainsford, Sarah. ‘Inside the mind of a Russian hacker’, *BBC*, 11 March 2010. <http://news.bbc.co.uk/1/hi/8561910.stm>.

Ravilious, Kate. ‘Hacked e-mail climate scientists receive death threats’, *The Guardian*, 8 December 2009. <http://www.guardian.co.uk/environment/2009/dec/08/hacked-climate-emails-death-threats>.

Raywood, Dan. ‘Colorado bank locks down debit cards after links made to Heartland breach’, *SCMagazine*, 9 March 2010.. <http://www.scmagazineuk.com/colorado-bank-locks-down-debit-cards-after-links-made-to-heartland-breach/article/165338/>.

Reuters. ‘Georgia releases Ossetians in likely prisoner swap’, 2 December 2009. <http://www.reuters.com/article/idUSATRE5B122Q20091202>.

————. ‘NATO chief tries to quell E.Europe’s security fears’, 12 March 2010. <http://www.khaleejtimes.com/DisplayArticle08.asp?xfile=data/international/2010/March/international_March499.xml&section=international>.

RiaNovosti. ‘Russian envoy optimistic over joint threat assessment with NATO’, 3 December 2009. <http://en.rian.ru/russia/20091203/157089431.html>.

Rozoff, Rick. ‘USA Cyber Command: Waging War in World’s Fifth Battlespace’, 26 May 2010. <http://rickrozoff.wordpress.com/2010/05/26/u-s-cyber-command-waging-war-in-worlds-fifth-battlespace/>.

RT. ‘Russia named ‘spam superpower’, 19 February 2008. <http://rt.com/Business/2008-02-19/Russia_named_spam_superpower_.html>.

————. ‘Anti-Russian propaganda on Georgian TV channel’, 14 November 2009. <http://rt.com/Top_News/2009-11-14/anti-russian-propaganda-georgia.html>.

————. ‘Global Warning: Leaked ‘Climate Fraud’ e-mails under probe’, 25 November 2009. <http://rt.com/Top_News/2009-11-25/hackers-global-warming-scandal.html>.

————. ‘Global hacker threat comes from Russia?’ 8 January 2010. <http://rt.com/Top_News/2010-01-08/global-hacker-threat-russia.html>.

Secrest, Barry. ‘Cyber Crime: Russian hackers threaten the world’, 29 April 2010. <http://www.conservativerefocus.com/blog5.php/2010/04/29/cyber-crime-russian-hackers-threaten-the-world>.

Shackelford, Scott. J. ‘Estonia two-and-a-half years later: A progress report on combating cyber attacks’, *Journal of Internet Law*, Forthcoming. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1499849>.

Sheppard, Noel. ‘CNN FINALLY reports ClimateGate – To downplay it of course’, 26 November 2009. <http://newsbusters.org/blogs/noel-sheppard/2009/11/26/russian-tv-does-better-job-reporting-climategate-cnn>.

————. ‘Scientist uses UN security to stop questions about ClimateGate’, 11 December 2009. <http://newsbusters.org/blogs/noel-sheppard/2009/12/11/climategater-uses-un-security-halt-questions-about-scandal>.

Simmons, Amy. ‘Facebook probes password hackings’, *ABC News*, 30 April 2010. <http://www.abc.net.au/news/stories/2010/04/30/2887235.htm>.

Slideshare. (n.d.) ‘Whos Hacking Your Pc?’ <http://www.slideshare.net/vbdotnetnrew/whos-hacking-your-pc>.

Smith, Michael and Warren, Peter. ‘NATO warns of strike against cyber attackers’, *The Sunday Times*, 6 June 2010. <http://www.timesonline.co.uk/tol/news/world/article7144856.ece>.?>.

Snapple. ‘Tomsk hackers Part III: FBI investigating death threats against global warming scientists’, 7 January 2010. <http://legendofpineridge.blogspot.com/2010/01/tomsk-hackers-part-iii-fbi.html>.

————. ‘The BBC interviews of a reformed hacker’, 21 March 2010. <http://legendofpineridge.blogspot.com/2010/03/bbc-interviews-reformed-russian-hacker.html>.

Softpedia. ‘Mastermind Behind the RBS WorldPay Hit Arrested in Russia’. <http://news.softpedia.com/news/Mastermind-Behind-the-RBS-WorldPay-Hit-Arrested-in-Russia-138240.shtml>.

Spamfighter News. ‘Russian hacker could face imprisonment of 17-25 years’, 5 January 2010. <http://www.spamfighter.com/News-13697-Russian-Hacker-Could-Face-Imprisonment-of-17-25-Years.htm>.

————. ‘Legally designed cloud computing used for malicious purposes’, 10 March 2010. <http://spamnews.com/The-News/Latest/Legally-Designed-Cloud-Computing-Used-for-Malicious-Purposes-2010031012686/>.

————. ‘BlackEnergy Trojan attacks Russian, Ukrainian banks on new version’, 12 March 2010. <http://www.spamfighter.com/News-14021-BlackEnergy-Trojan-Attacks-Russian-Ukrainian-Banks-in-New-Version.htm>.

————. ‘Botnets, Hackers’ instant attack weapons’, 16 April 2010. <http://www.spamfighter.com/News-14215-Botnets-Hackers-Instant-Attack-Weapons.htm>.

Stack, Megan. ‘Russian secrets for sale, no questions asked’, *LA Times*, 17 March 2010. <http://articles.latimes.com/2010/mar/17/world/la-fg-secrets-for-sale17-2010mar17>.

Stewart, Will and Delgado, Martin. ‘Were Russian security services behind the leak of ‘Climategate’ e-mails?’ 6 December 2009. <http://www.climateark.org/shared/reader/welcome.aspx?linkid=144998&keybold=climate%20AND%20%20deal%20AND%20%20post%20AND%20%20Kyoto>.

Streetwise Professor (SWP). ‘In which SWP actually defends the FSB’, 8 December 2009. <http://streetwiseprofessor.com/?p=3022>.

Takahashi, Dean. ‘SINET event draws feds and security entrepreneurs together’, *VentureBeat*, 17 March 2010. <http://venturebeat.com/2010/03/17/sinet-event-draws-feds-and-security-entrepreneurs-together/>.

Taylor, Matthew and Arthur, Charles. ‘Climate e-mail hackers had access for more than a month’, *The Guardian*, 27 November 2009. <http://www.guardian.co.uk/environment/2009/nov/27/climate-email-hackers-access-month>.

Telegraph. ‘Climategate: was Russian secret service behind email hacking plot?’ *Telegraph*, 6 December 2009. <http://www.telegraph.co.uk/earth/copenhagen-climate-change-confe/6746370/Climategate-was-Russian-secret-service-behind-email-hacking-plot.html>.

Thomson, Iain. ‘Russia and USA working together to shut down stock hacker’, 22 March 2010. <http://www.securecomputing.net.au/News/170201,russia-and-us-working-together-to-shut-down-stock-hacker.aspx>.

Thomson, Iain ‘Estonia attacks down to online mob’, 27 September 2007. <http://www.v3.co.uk/vnunet/news/2199732/estonia-attack-online-flashmob>.

Tynan, Dan. ‘Your Facebook profile may be sold by Russian hacker’, 26 April 2010. <http://www.pcworld.com/article/195005/your_facebook_profile_may_be_sold_by_russian_hacker.html>.

UNCHR. ‘Attacks on the Press 2009 – Georgia’, Refworld, 16 February 2009. <http://www.unhcr.org/refworld/country,,,,GEO,,4b7bc2e82d,0.html>.

USA Department of State, ‘United States Joins Council of Europe Convention on Cyber crime’, press statement, 29 September 2006. <http://www.state.gov/r/pa/prs/ps/2006/73353.htm>.

Villeneuve, Nart. ‘Blurring the boundaries between cyber crime and politically motivated attacks’, 10 April 2010. <http://www.nartv.org/2010/04/10/blurring-the-boundaries-between-cybercrime-and-politicaly-motivated-attacks/>.

Walker, Shaun. ‘Was Russian secret service behind leak of climate-change e-mails?’ *The Independent*, 7 December 2009. <http://www.independent.co.uk/news/world/europe/was-russian-secret-service-behind-leak-of-climatechange-emails-1835502.html>.

Watts, Anthony. ‘Media now blaming Russians for Climategate leak’, 6 December 2009. <http://wattsupwiththat.com/2009/12/06/media-now-blaming-russians-for-climategate-leak/>.

Weinberger, Sharon. 'Hackers are Internet Shock troops', *Aviation Week*, 14 May 2010. <http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/dti/2010/05/01/DT_05_01_2010_p19-218221.xml&headline=Hackers%20Are%20Internet%20Shock%20Troops>.

Werz, Michael and Manlove, Kari. 'Climate migration will affect the world's security', 9 December 2009. <http://www.truthout.org/topstories/120909sg02>.

Wilson, Ray. 'Cyber security is a worldwide imperative', *The Bulletin*, 7 May 2010. <http://thebulletin.us/articles/2010/02/10/business/doc4b72565659bf0979208886.txt>.

Yribarren, Bobby. 'Status update: College publisher hacked!' 9 February 2010. <http://www.coscampusonline.com/status-update-college-publisher-hacked-1.2145417>.

Zetter, Kim. 'Russia arrests alleged mastermind of RBS WorldPay hack', *Wired*, 22 March 2010. <http://www.wired.com/threatlevel/2010/03/alleged-rbs-hacker-arrested/>.

Zimmer, Carl. 'George Will: Uncheckable?' *Discover Magazine blogs*, 6 December 2009. <http://blogs.discovermagazine.com/loom/2009/12/06/george-will-uncheckable/>.

ATHINA KARATZOGIANNI is lecturer in Media, Culture and Society at the University of Hull, UK. She is the author of *The Politics of Cyberconfict* (2006), *Power, Conflict and Resistance: Social Movements, Networks and Hierarchies* with Andrew Robinson (2010), and the editor of *Cyber Conflict and Global Politics* (2009). She is currently writing on cyberconflicts of unrecognised and small states. She is also contributing to work theorising ultraviolent subjectivities in cyberspace, examining conflict analysis and war coverage of crises in global hotspots and exploring the potential of ICTs and network forms of organisation for social movements, resistance and open knowledge production. [a.karatzogianni@hull.ac.uk]