Virtual attacks and the problem of responsibility: the case of China and Russia

Daniel Oppermann

Virtual attacks are forming a new threat scenario for governments and other actors of global society. The first decade of the XXI century saw an intensification of cyberattacks on government networks which could not be traced back. However, due to political circumstances there were often actors suspected of being involved in cyberattacks. This case study is analyzing the methods and reasons of potential attackers in Russia and China which between 2004 and 2009 appeared in several cyber threat scenarios.

Keywords: cybersecurity, cyberattack, China, Russia

Ataques virtuais representam um novo cenário de ameaça para governos e outros atores da sociedade global. Durante a primeira década do século XXI houve uma intensificação de ataques cibernéticos de origem desconhecida contra redes governamentais. Porém, devido às circunstâncias políticas, muitas vezes havia atores suspeitos de estarem envolvidos em ataques virtuais. Essa pesquisa de caso está analisando os métodos e razões dos atacantes potenciais na Rússia e na China, os quais apareceram em vários cenários de ameaças cibernéticas entre 2004 e 2009.

Palavras-chave: segurança cibernética, ataque cibernético, China, Rússia

In January 2009 the US administration under then recently elected US President Obama released a new US Agenda for Homeland Security underlining growing attention to virtual attacks and cybersecurity by announcing the position of a national cybersecurity advisor reporting directly to the President. Four months later, in May 2009, Obama confirmed his plans during a speech in the White House, without having appointed an advisor so far. When in September 2009 Melissa Hathaway resigned from her position as the Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils, speculations about the difficulties to find a qualified candidate to coordinate national cybersecurity issues in the US started putting pressure on the US administration (Nakashima, 2009). In those first eight months of hesitation hundreds of cyberattacks happened on governmental and private economy severs in the US and other countries. Most of them were not covered in the media and many stayed unknown even to the institutions or companies being attacked. In most cases it was unclear where the attackers agitated from or what their intentions were. Nevertheless in some cases cybersecurity experts succeed to trace back online attacks although they hardly had any legal possibilities against the possible attackers due to the borderless character of the Internet and the lack of appropriate policies or legal frameworks. In other cases political circumstances alluded to where attackers might have come from and what their intentions were.

The US are not the only victim of cyberattacks. Almost all states have suffered virtual attacks in the past ten years but so far only few resulted in serious concerns or have been made public. While some (and those are more relevant for this article) have a political background, others are more connected to criminal activites. As being among the strongest global economies with a well developed telecommunication infrastructure the US are having high interests in protecting their networks from such hostile activities. Therefore they have a crucial role in developing means of protection against virtual attacks (and probably seeking ways to launch attacks by themselves). Besides them also the European Union is addressing the problem and watching global developments with concern, discussing cybersecurity policies.

Concerns over cybersecurity in the past five years have frequently included Russia and China, both fast growing Internet markets and several times being suspected of

***Daniel Oppermann** é doutorando do Instituto de Relações Internacionais da Universidade de Brasília (IREL-UnB) e pesquisador do Observatório Político Sul-Americano (OPSA) do Instituto de Estudos Sociais e Políticos na Universidade Estadual do Rio de Janeiro (IESP-UERJ).*

using their IT infrastructure to infiltrate other countries' networks. This article will concentrate on the problem of virtual attacks and the role the two countries had in this context between 2004 and 2009. Regarding Russia especially the 2004 cyberattacks in Estonia and also the 2008 attacks on Georgia will be discussed. The Chinese case includes GhostNet, an espionage network that was investigated by Canadian researchers in 2008/2009.

The article is structured in six chapters. After this introduction, the second chapter is going to introduce the research method applied and will present the research questions. The third chapter concentrates on the general phenomenon of cybersecurity. It includes the theoretical basic knowledge regarding cybersecurity, cybercrime, cyberterror, and cyberwar. Furthermore it discusses different methods of cyberattacks. The forth and fifth chapter are analysing the two cases of Russia and China and their function in recent cyberattacks on other countries. Following those two, the final conclusion will pick up the research questions again to develop final statements regarding the problem underlying this article.

Almost all states have suffered virtual attacks in the past ten years but so far only few resulted in serious concerns or have been made public.

Research methodology

This article is going to analyse the current situation of cybersecurity regarding nation states with a focus on virtual attacks and the question who is responsible for them. A special focus is given on Russia and China which in the past five years have been accused several times by Western governments of undertaking virtual attacks on governmental institutions and private companies in different countries. The research method applied is the qualitative case study design. "A case study (...) is the analysis of an object: a country, a political system, an institution, an organization, or a problem in a certain context (...). In a comparative analyses different cases on the same topic are used."(Nohlen, 1994, p. 128, translated by the author). The case study design is among the most applied methods in political research. Its origin goes back to 1948 at Harvard University (McNabb, 2004, p. 357). It helps to explain an individual case and is also able to make a generalization (although quantitative methods are stronger for generalization). It can be conducted with one or several cases. "Through the study of cases, political scientists are able to learn about political events, agencies, parties and levels of government and politics around the globe. Cases are also written to serve as examples of approved management practices." (McNabb, 2004, p. 357).

Robert Stakes divides case studies into three categories: intrinsic, instrumental and collective case studies. This way he tries to differentiate the motives of the researchers. An intrinsic study aims at understanding the case itself. The case is the central aspect of the study. The objective is nor the development of theories neither the analysis of a phenomenon behind the case. An instrumental study treats the case as an example for a theory or a political or social phenomenon. This phenomenon is the actual interest of the researcher. The case helps to explain it. The third category is a collective case study. The researcher uses it to investigate several cases that help to explain a certain phenomenon. Similar to Stakes, Robert Yin divides case studies into two categories: single-case studies and multiple-case studies (Yin, 2002, p. 45f). Both have the intent to explain the phenomenon behind the case.

This present case study is designed as a multiple, instrumental case study (n=2) to analyze the social phenomenon of virtual attacks on nation states and the question of responsibility for such attacks. The focus lies on virtual aggressions between 2004 and 2009 being traced back by the victims to China and Russia. The intention is to analyse information about virtual attacks as a social phenomenon and about the possibilities to trace them back to their origin. The leading research questions are: What are the main kinds of cyberthreats and virtual attacks pointed against political and economical networks? How is it possible to trace virtual attacks back to the attacker? Who is using virtual attacks against political and economical networks and with what kind of intention? What roles do Russia and China have concerning virtual attacks on foreign networks?

The concept of cybersecurity

Cybersecurity as a concepts has numerous different dimensions. This chapter is going to categorize the different dimensions of cybersecurity being cybercrime, cyberterrorism, and cyberwarfare. After that different forms of virtual attacks will be discussed in general as well as the question how they were conducted in the past years.

In the context of online security, cybersecurity could be a simple form of private protection against spam or other malware distributed on the Internet. It could also mean protection of family members (for example children) from accessing unwanted web content. Furthermore it means protection from ordinary crime or fraud occuring on the internet like phishing, identity theft, credit card fraud and others (McQuade III, 2006, p. 63ff). These types of activities are categorized as cybercrime. Cybercrime as a phenomenon plays a minor role in this article. Although, as the

following paragraphs will demonstrate, cybercrime itself does not have a purely economic side but also contains political interests which are closely connected to the aspects being investigated on the following pages. Examples for political cybercrimes are hate speech and cyberterrorist activities.

Hate speech usually refers to racist, anti-semitic or anti-ziganistic content that is clearly of political nature but also treated as a cybercrime when it happens online. Cyberterrorism (or cyberterror) however is a more complex concept. It could be treated as a cybercrime in certain cases like the distribution of information to produce explosive devices. Nevertheless as the case of three young men in the UK shows, governments are tending to recognize such activities as acts of terrorism rather than simple cybercrimes (Stevens, 2008).

Terrorist groups are using the Internet for a wide spectrum of activities ranging from spreading information and propaganda, over networking and recruiting, until mobilization and fundraising (Weimann, 2006, p. 111ff). Mehan (2008) defines cyberterror as "the politically-motivated use of computers by terrorist groups, sub-nationals, or clandestine agents as weapons or as targets intended to result in violence, influence an audience, or affect national policies." (Mehan, 2008, p. 33). It is based on two definitions given by 1) the 22 US Code, section 2656, and 2) the US National Infrastructure Protection Division (NIPD). The first one mentioned concentrates on terrorism in general and says that it can be described as "premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience." (Mehan, 2008, p. 32). Following the NIPD "cyberterrorism is a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies." (Mehan, 2008, p. 32). A crucial point in Mehan's definition is the clarification that computers can be used "as weapons or as targets". This becomes clear when refering to Kerr's earlier contribution to the discussion on cyberterror in which she mentioned that out of 109 definitions of cyberterror four mentioned all of the three main aspects 1) use of violence, 2) political objectives, and 3) the purpose of spreading fear within the population (Kerr, 2004). Nevertheless two of those definitions refer to computers as being targets, the other two as being means of an attack. Mehan assembled these two different approaches and created a more complete definition of cyberterror.

The third category is cyberwarfare (or cyberwar). Cyberwarfare can be seen as a sub-category of information warfare, a term introduced by the US military in the 1980s which includes the domination of all possible means of information and communication (including psychological operations) to use them against the opponents. Different from information warfare, cyberwarfare is limited to the usage of computer networks to harm a country's critical infrastructure. By definition of the European Commission, critical infrastructure stands for

> those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical Infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services. (Commission of the European Communities, 2004, p. 3).

Other definitions like in a report of the US Congressional Research Service include basicly the same sectors (Moteff; Parfomak, 2004, p. 4).

Mehan distinguishes four different kinds of cyberwar:

> ...Class I cyberwar is concerned with the protection of personal information...Class II cyberwar concerns itself with industrial and economic espionage...Class III cyberwar is officially about global war and terrorism... Class IV cyberwar is the use of all the techniques of Classes I-III in combination with military activities in an effort to obtain a battlefield advantage or a force multiplier. (Mehan, 2008, p. 28).

Early cyberwar attacks go back to the 1980s when the US used hacking methods to infiltrate computer networks of the Soviet Union, mainly with the intention of espionage. With the further development of IT networks in the 1990s the Kosovo war in 1999 saw the first big application of cyberwar measures. While the US used different me-

Concerns over cybersecurity in the past five years have frequently included Russia and China, both fast growing Internet markets and several times being suspected of using their IT infrastructure to infiltrate other countries' networks.

thods to manipulate Serbian weapon and communication systems (Arkin, 1999; Dunn, 2001), also the Serbian and Albanian side used IT for their own interests. In most cases this involved spreading information and propaganda accusing the other side of war crimes and cruel activities but also to connect with supporters or diasporas in other countries. Furthermore NATO and US server and websites were attacked. When in May 1999 the US bombed the Chinese embassy in Belgrade, a wave of cyberattacks from China hit American and NATO infrastructure (Messmer, 1999) many of them being denial of service (DoS) attacks conducted by private citizens from their home compute in what Timothy Thomas of the US Foreign Military Studies Office called a "take-home-battle" (Thomas, 2000).

DoS attacks

Besides simple hacking activities to access information on foreign computers, spreading malware, or changing website content (website defacement), DoS attacks are one of the most frequently used measures to conduct virtual attacks. The effect of such an attack is the inability to access a network or information on a website. DoS attacks can cause massive data traffic on foreign networks which as a consequence break down temporarily. The better protected the network under attack, the higher the necessary number of attacking computers. While for a smaller network a few hundred computers can already cause problems with data processing, government networks or those of bigger companies are more difficult to corrupt. In that case distributed denial of service (DDoS) attacks can be operated as they include a higher number of computers that can be controlled by one single person. Before launching a DDoS attack the aggressor needs to get control over a number of computers which are usually kidnapped from ordinary users who are unaware of their unwanted participation in the attack. To get access to other computers malicious codes distributed by spam, fraudulent websites, or other means of capture is connecting private user PCs to a controling server. An aggressor can also easily get access to a required number of captured computers by simply hiring botnets online.

Botnets

Originating from the suffix of "robot", a botnet consists of several computers under control of a single authority which can command the single units (drones) of the botnet to simultaneously access a hostile network at a chosen point of time. This kind of DDoS attacks based on botnets are common virtual attacks and can be executed by a single person. Botnets are offered for hire to cybercriminals, cyberterrorists, cyberwarriors or any individual on the Internet. Contact between supplier and renter can be made on several forums on the Internet. The prices differ from 50 US$ per day for a small botnet up to thousands of dollars for more complex networks. In 2009 huge botnets existed consisting of millions of captured computers (GRANT 2009). Generating botnets became a worthwhile business supplying thousands of cyber aggressors who altogether paid a few million dollars to botnet providers.

Virtual attacks and their origins

The majority of virtual attacks stays unknown. Whenever detected by the attacked, the first priority for the victims is to reduce damage. Especially larger companies but also governmental institutions suffer frequent cyberattacks although they do not necessarily cause serious damage nor do they regularly have a political background. The reasons for not publicly debating all virtual attacks are therefore a question of quantity and (lack of) quality of the attacks, but also to hide vulnerability of the victim. A public or private entity being known for its defectivness towards virtual attacks (and therefore sensitivity for espionage) would easily loose its reputation which could cost clients, partners, or votes. Cyberattacks that do appear in the media are usually 1) of larger dimension, 2) have a serious economical or political impact, or 3) are published in strategic moments. One example for the first two categories (which will be further discussed later in this article) are the attacks on Estonia in 2007 when both the questions of dimension and seriousness came together. Also the cyberattacks during the Caucasus war in August 2008 belong to these categories.

Two examples for virtual attacks that were published at strategic moments are the attacks on German, British, and US government networks publicly announced in August 2007, and the DDoS attacks on US American and South Korean government and business websites in July 2009. In the first example the German magazine Spiegel revealed on 25 August 2007 that cyberattacks on German government institutions like the Ministry of Exterior, the Ministry of Research, the Ministry of Economy and the office of chancelor Angela Merkel had happened with the intention of installing spyware. The actual problem had already been recognized by IT security analyst months before but became a bigger issue at the dawn of Chancelor Merkels visit to the Chinese government starting on 26 August 2009. In the following week the Spiegel and other newspapers additionally published articles about similar incidents in the US and the UK which also had happened some time before already (Spiegel Online, 2007b; Sueddeutsche.de, 2007b). The intention of this strategically published articles to start a German-Chinese dialogue on the issue was successful. Chancelor Merkel and Premier Wen Jiaboa discussed the issue with the result that Wen declared the rejection of the Chinese government to conduct cyberattacks. Contrary to this statement the German Domestic Intelligence Agency

(Verfassungsschutz) declared having traced back the attackers to computers of the Chinese Army (Spiegel Online, 2007a).

While the case of the German government networks was discovered long before its coverage in the media, the example of the 2009 DDoS attacks on the USA and South Korea did happen at a strategic moment and were immediately published. On the American Independence Day July 4 2009, 27 US governmental and later also business networks became victims of a DDoS attack which later was expanded on South Korean official and private economy networks. Some of the victims in the US were the Treasure Department, the Secret Service, the Federal Trade Commission, the White House, and the New York Stock Exchange while in South Korea the Presidential Blue House, the Ministry of Defense and the National Assembley were being attacked. The botnet used to conduct the DDoS attack consisted of 50.000-65.000 computers and can therefore be considered a smaller incident. Nevertheless several systems under attack broke down for up to five days. Further risks like the possible abstraction of information shortly before the attack were mentioned by the Commission on Cybersecurity but could not be proven (Chabrow, 2009).

South Korean intelligence analysts suspected foreign governments or pro-foreign government groups without directly mentioning North Korea. US American IT security experts assessed the attack to be little sophisticated judging from the simple character of the scripts used. This would also weaken the theory of the Commission on Cybersecurity about the probability of an act of espionage. What was expressed by the American analysts is that the script refered to China's internal routing system and that it contained data that could be traced back to a Korean-language browser (Markoff; Sang-Hun, 2009).

Besides China, Russia is the second country that is mentioned above average when it comes to cyberattacks. From January to March 2009 different embassies of Azerbaijan, Ethiopia, India and Portugal have reportedly been under virtual attacks (Constantin, 2009a). In the months before, also embassies and consulates of Brazil, France, the Netherlands, Syria and the US suffered cyberattacks (Constantin, 2009b). As cyberattackers usually do not leave written messages justifying their course of action it is difficult to analyse the reasons for all virtual attacks which happen and become public. Nevertheless in some cases like the parallel attacks on different websites connected to the Azerbaijanian government in March 2009, it is possible to draw relations to offline politics. During the week of the attacks, the Russian Foreign Minister Sergei Lavrovis was visiting Azerbaijan while Azerbaijans President Ilham Aliyev left the country to visit Iran. Although this still leaves open the question how this act was interpreted by the cyberattackers who were described by an IT security analyst as members of the Russian cybercrime organization Russian Business Network (RBN), a non-registered company working on an anonymous basis using more than a dozen synonyms in different countries. The RBN can be seen as a crucial non-state actor in cyberattacks world wide, whose members act as mercenaries for political or private economy interests.

Whenever virtual attacks on governmental institutions are discussed the question of responsibility comes up. Although in many and especially in cases of serious damage governmental representatives express suspicions, which are usually based on general political circumstances or on results of IT security analysts, it is almost impossible to prove where cyberattacks come from due to the character of the networks or the fact that botnets are used whose drones do not lead to the location of the real attacker. Furthermore cyber aggressors could use proxy servers to disguise their real location. Also the attack on the US American electricity grid in April 2009 lead to statements by US officials holding China and Russia responsible for infiltrating critical infrastructure on US territory without being able to prove it (Gorman, 2009). So far it is unclear in International Law what rights states have to react on virtual attacks. It is undefined if cyberattacks can be categorized as "armed attacks" which would give states the possibility of self-defense following article 51 of the UN Charta. Moreover it is open who they could attack as an act of self-defense.

Russia

Following the 2008 data of the International Telecommunication Union (ITU Internet Statistics 2008), 32,11% of Russia's 140 million inhabitants were using the Internet in 2008, 21,49% had their own Internet access. The country has one of the fastest growing Internet populations in Europe and the bordering regions. Following a research report of the Reuters Institute for the Study of Journalism at the University of Oxford, Russian users are mostly interested in websites containing sports, music, social activities and other forms of entertainment (Fossato; Lloyd; Verkhofsky, 2008, p. 14) plus the steadily growing blogosphere which had about 3,8 million blogs in 2008 (Fossato; Lloyd; Verkhofsky, 2008, p. 14). Furthermore the report stated the Russian government under President Medvedev and former President Putin refrained so far from extended Internet regulations which fostered economic development of the ICT market in recent years. Although some exceptions were made for the Federal Security Service FSB, which has the possibility to control Internet communication without knowledge of the Internet Service Providers

(ISP).

However researchers of the OpenNet Inititative see Russia's role in Internet regulation with more critical eyes. In a regional report about the Internet in the Commonwealth of Independent States (CIS) the authors argue that in Russia (and other member states of the CIS) a general tendency "toward greater government regulation of the Internet" can be observed, "to bring it in line with existing regulations that control the mass media" (Opennet Initiative). The authors also refer to the SORM II regulation which since the year 2000 offers the FSB advanced possibilities to control Internet communication within Russia. SORM II is comparable to a number of laws and regulations passed in the USA after 9/11 like the US Communications Assistance to Law Enforcement Act or parts of the Patriot Act.

The percentage of Russian Internet users who go online for political reasons is quite small. Political activism on the net does partly happen but is also closely watched by national authorities. Nevertheless Russian communication networks have played a crucial role during political crises or conflicts with the nation's neigbouring countries in the past five years. The two major events in this context are the conflicts with Estonia in April 2007 and with Georgia in August 2008. Both countries have a tense relation to Russia due to their history as members of the Soviet Union. The following paragraphs will concentrate on both crises in which cyberattacks happened on the critical infrastructure of the two countries.

While the case of the German government networks was discovered long before its coverage in the media, the example of the 2009 distributed denial of service (DDoS) attacks on the USA and South Korea did happen at a strategic moment and were immediately published.

Estonia

As many East European countries also Estonia has a multi-ethnic population, made up mainly of Estonians, Russians, and other smaller minority groups. Early Russian settlements in Estonia go back to the 17th century when a few thousand Russians migrated to the neighbouring country escaping religious persecution in Russia. During WWII Estonia was occupied by Russia in 1940 and got back its independece only in 1991. During these five decades of being part of the Soviet Union, Moscow forced its own population policy on Estonia in the same manner as on other countries and regions within their sphere of power (Rannut, 2004). Thousands of Estonians were settled by force to the Russian main territory while thousands of Russians moved to Estonia. By this measures the Russian part of the population of Estonia went up from 8% before the occupation to about 30% until 1991. This percentage went down to around 25% after the independence of the country.

As Russian used to be the official language for 50 years, many Russians never learnt to speak Estonian. With the independence also the Estonian language was reinstalled as the official language of the country, leaving the problem, that about 85% of the Russian minority were not able to speak the new official language, which was 21% of the country's whole population. Since then ethnic minority rights has been a constant challenge for Estonia and relations between Estonians and Russians were tensious at certain moments (Lang, 2008; Vetik, 1993).

One of this moments was the decision of the Estonian government in April 2007 to remove a statue of a Russian soldier from a central place in the capitol Tallinn to move it to a military cemetary outside the city center. The statue had been placed in the center of town by Moscow in 1947 to celebrate the end of WWII. The Estonian population considered it a symbol of occupation. The moment to remove the statue at the end of April was strategically chosen as the Russian-speaking minority used to meet frequently at the statue on 9 May to celebrate the end of WWII.

The decision to relocate the statue caused protests mainly under young Russian-speaking Estonians that turned to riots on 26-27 April during which one person was killed and more than 1000 were arrested. In the days after the unrests Russia critized Estonia for its decision regarding the statue and requested the resignation of the government in Tallinn while anti-Estonian manifestations took place in front of the Estonian embassy in Moscow (Sueddeutsche.de, 2007a).

At the same time when the unrests started, cyberattacks were launched on several parts of the Estonian IT infrastructure (Hansen; Nissenbaum, 2009, p. 1168f). In the years before, the country had built up a highly sophisticated network environment ranking under the most developed systems worldwide. E-government services were implemented ranging from simple administration services to online elections. Today besides governmental services also the banking system and other sectors are based to an above average degree on IT networks. Due to the cyberattacks carried out for about three weeks, large parts of

the country's infrastructure suffered breakdowns, including governmental and banking infrastructure, and several online news services. To protect its infrastructre from foreign attacks Estonian Internet Service Providers (ISP) blocked online queries from outside the national borders. This also caused access problems for a great number of companies and private clients to financial resources within the Estonian Hansabank (Swedbank), one of the biggest financial institutions of the Baltic region. The attacks differed from similar incidents in other countries because of its comprehensive character impacting a whole country instead of individual institutions. Being concerned about the occurences also the European Union condemned the attacks although due to the upcoming EU-Russian summit officials refrained from addressing Moscow for possible responsibility. The NATO sent IT security analysts to Tallinn to investigate. One year later the alliance opened up its Cooperative Cyber Defence Centre of Excellence in Tallinn (Lang, 2008, p. 6).

Due to the political circumstances Estonian officials accused the Russian government to be responsible for the attacks while Moscow denied having any relations to it. Estonian Foreign Minister Urmas Paet and Minister of Justice Rein Lang both declared that IT analysis had proven the involvement of Russian government computers in the attacks. In this context they also mentioned the involvement of Russian Presidential administration networks in the attacks (Spiegel Online, 2007c).

Besides individual cases of webdefacement on governmental websites, DoS attacks were the main method used to interfere with Estonian infrastructure. Before and during the attacks, in several Russian webforums patriotic hackers informed users (especial the younger generation, so called script kiddies) how to participate in cyberattacks on Estonia. Driven by patriotic outrage there was a growing number of young Internet users in Russia wanting to harm Estonia by attacking its infrastructure. Nevertheless, the most serious attacks were the ones that had botnets involved controlled by more advanced attackers. Botnets used during the attacks consisted of drones from several countries including the Brazil, Canada, Egypt, Peru, Russia, the USA and Vietnam. This way hundreds of thousands of computers were guided to attack specific points at the same moment. IT analysts observing the attacks discovered that concentrated attacks started and ended at fixed points of time (after exactly two weeks) proving the use of botnets. Also the qualitative level of the more serious attacks pointed out that professional hackers were behind them (Davis, 2007). Additionally, some of the attacks happening during the day stopped at midnight (Faz.net, 2007). This fact suggested that hired botnets (that are usually paid per day) were in use which implies high costs for the attackers that can barely be carried by individual Internet users. Furthermore analysts from the IT security company Arbor Networks discovered, that some of the botnets used against Estonia were just a few weeks earlier employed to disturb the IT presence of an alliance of Russian opposition parties (Davis, 2007).

Especially larger companies but also governmental institutions suffer frequent cyberattacks although they do not necessarily cause serious damage nor do they regularly have a political background. The reasons for not publicly debating all virtual attacks are a question of quantity and (lack of) quality of the attacks, but also to hide vulnerability of the victim.

Estonian officials constantly blamed the Russian government to be responsible for the attacks, but this accusation could never been proven. Russia always denied having any responsibility but hardly considered to clear up the occurences by activating its secret service FSB. Due to the SORM II regulation mentioned above, the FSB has control over all Internet traffic in Russia. Although SORM II was developed to control the Internet for security reasons President Putin (a former FSB director) did not initiate an investigation.

In January 2008 a 20-year-old Russian Estonian was arrested and fined in the Baltic republic for conducting cyberattacks on Estonian infrastructure (Kirk, 2008). However, the facts presented above make clear that highly sophisticated actors were behind the attacks and not just a group of patriotic script kiddies. After two years without further clarifying information, Russian State Dume Deputy and member of the Russian delegation to the Parliamentary Assembley of the Council of Europe (PACE) Sergei Markov (accidently) revealed that one of his assistants was responsible for the cyberattacks. This man was later identified as Konstantin Goloskokov, a leading member of the Nashi youth movement, an organization founded by Putin supporter Vladislav Surkov in March 2005. Goloskokov confirmed his responsibility in the attacks. In an interview given to the Financial Times in March 2009 he stated that he and other members of his organization simply accessed Estonian websites until they crashed (Clover, 2009). In the interview he pointed out that all activities were undertaken without governmental instructions or support.

Considering the impact of the cyberattacks it is un-

likely that Goloskokov and his colleagues brought down the infrastructure of the whole country just by accessing websites. More interesting is to consider the possibility of Nashi being involved in concentrated botnet attacks. The organization had more than 120.000 members in 2008 and is famous for its street activities against Russian opposition parties. It was also involved in violent protests against the Estonian embassy in Moscow in May 2007. Estimations by the German Institute for Peace Research and Security Policy say that the Putin administration supported Nashi and other youth organizations with several 100.000 US dollars per month. Nashi's anual summer camp had an estimated budget of 6-7 million US dollars (Heller, 2008). Considering the costs for hiring extensive botnets how they were used against Estonia, Nashi exhibits not only strong motivation and confessing members but also possesses the necessary financial resources.

Georgia

The cyberattacks in July and August 2008 against Russia's neighbouring country Georgia happened in the context of the enduring conflict between the two countries over South Ossetia. The legal status of this Caucasian region has been the reason for disputes and military confrontations for several generations in history. During the Soviet Union a constant support of new Ossetian settlements by Moscow and a parallel relocation of Georgians from the region lead to a growing Ossetian population which today is about 66% in South Ossetia compared to 29% Georgians. It remained an autonomous region within the Georgian Soviet Socialist Republic until 1990 when it declared its independence which was not recognized by any other state. Since then Georgia claimed the region as part of its own state (independent since 1991) and is supported by the majority of states of the international community. Moscow supported the demand for independence and offered Russian citizenship to the inhabitants of the region for which reason about 90% of the population in South Ossetia is today formally Russian.

Besides China, Russia is the second country that is mentioned above average when it comes to cyberattacks.

Since the 1990s the conflict in the region resulted in numerous military disputes which were interrupted by phases of relative peace which was common also in other Caucasian countries after the end of the Soviet Union and described by researchers as "frozen conflict" (Borgen, 2009). Others questioned this term arguing that South Ossetia and also Abkhazia showed continuously violent clashes between rivaling actors (König, 2006). In August 2008 intensified clashes of the preceding months lead to an occupation of South Ossetia by Georgian troops, followed by a Russian invasion of South Ossetia and parts of Georgia as well as bombings of several Georgian cities (Closson; Halbach, 2008). After the withdrawal of Georgian troops a few days later, Russia officially recognized South Ossetia's (and Abkhazia's) independence in August 2008, later followed by Nicaragua (September 2008) and Venezuela (September 2009). This step can be interpreted as a consequence of the independence of Kosovo, accepted by a number of Western states in February the same year, which was emphatically critizised by the Russian government who is still concerned about independence struggles of a number of territories in the former Soviet region.

While violent outbreaks between Georgia and Russia had been a recurring phenomenon of the region since the early 1990s, the fights in August 2008 added a new component to the conflict. Already before the occupation of South Ossetia started in August, virtual attacks were launched against several parts of the Georgian infrastructure. These attacks, which started in July 2008 (Adair, 2008), included DDoS attacks, botnets, logic bombs and other measures. (A logic bomb is a piece of code which can be placed within a chosen part of an adversary's IT infrastructure to be activated at a strategic moment of time. Once activated the code can harm the adversary's IT system from the inside).

Affected by the attacks in Georgia were mainly the President's office and other governmental networks, financial networks, news services, and the US embassy. Before and during the virtual aggressions, potential targets were published on several Russian online discussion forums to mobilize patriotic hackers like it had happened in the Estonia attacks the year before. A large number of websites targeted was blocked for several days. Some governmental sites were moved to Turkish and US American servers to continue informing provisionary about the armed conflict in South Ossetia. The Ministry of Foreign Affairs continued publishing information on a blog after its own network broke down (Waterman, 2008). Also cell phone services broke down as a consequence of the attacks on financial networks (Corbin, 2009). To secure their own networks, foreign banks cut their connections to Georgian banks, leaving them isolated from the global financial system. Besides the Georgian networks, also in Russia and South Ossetia virtual attacks on critical infrastructre took place, albeit to a lesser extend.

Joseph Nye later pointed out that never before, armed conflicts and virtual attacks had happened in combination:

"The Russia-Georgia conflict represents the first significant cyberattacks accompanying armed conflict. Welcome to the twenty-first century." (Nye, 2008). Although as stated above, already the Kosovo conflict saw a combination of cyberwar measures and traditional armed aggressions, Nye is right that the Caucasus war 2008 included cyber measures on an intensified level compared to the Kosovo war in 1999.

Similar to the attacks on Estonia, also the Georgian government accused Moscow for being responsible for the breakdown of governmental and civic infrastructure. Moscow again denied its responsibility. There are different possible scenarios for who conducted virtual attacks on Georgia. They range from patriotic hackers over criminal organizations to the governmental level.

While violent outbreaks between Georgia and Russia had been a recurring phenomenon since the early 1990s, a new component was added to the August 2008 conflict in South Ossetia: virtual attacks were launched against several parts of the Georgian infrastructure.

The involvement of patriotic hackers and script kiddies in virtual attacks against Georgia is a widely accepted fact. Corresponding discussions in Russian online forums including instructions by experienced hackers and the supply of the necessary tools, but also the results of different IT security analysis have proven this to be true. Also the ongoing virtual attacks after the Russian government had officially ended its military campaign support this argument. Beyond that the Shadow Foundation, an organization specialized in Internet security research, had watched a number of servers for an extended period of time (some for more than one year) before the same servers became involved in the Georgia attacks. As those servers had been used before August 2008 to commit ordinary criminal activities which, following the researchers, were not connected to the Russian government, they concluded that the servers mentioned were rather used by individuals or criminal organizations (Johnson, 2008). Although it could be possible to hire these services also with public resources.

Looking at the participation of criminal organizations the situation becomes more complex. Besides providers of botnets, who can be considered cybercriminals as well, also the Russian Business Network (RBN) is a potential actor being involved in the attacks. As stated above, the network functions as a non-registered company which is responsible for a high percentage (approximately 60%) of all cybercrime activities worldwide (Warren, 2007). In spite of its activities the RBN, operating from St. Petersburg, was never charged by Russian authorities. Its probable relations to political officials might be one of the reasons (idem). Nevertheless the network disappeared in November 2007 and has since then been spotted on different locations outside of Russia, where the lack of IT policies and legal regulations facilitate their activities. The involvement of cybercriminal organizations in the attacks on Georgia and a certain level of cooperation with Russian officials were also confirmed by the US Cyber Consequence Unit's report handed to the US government in August 2009 (Kirk, 2009).

Looking at the governmental level it is unlikely that the Kremlin was directly involved in any cyberattacks on Georgia. Although some aspect indicate that officials from the (lower) political spectrum and the military could have been involved or at least have cooperated with virtual attackers. One example is the coordination of timing and location of both virtual and military strikes. On August 9, 2008 cyberattacks that brought down news service stations in the Georgian city of Gori happened just moments before the Russian airforce bombed strategic goals in the same city (Goodwin, 2008). This indicates a certain form of cooperation to prevent the spreading of information after the bomb attacks. Another indicator is the involvement of the two Russian government-controlled telecommunication companies Rostelecom and Comstar. Servers of both companies were identified having blocked Internet traffic going to Georgia as well as launching DDoS attacks against the country (Leyden, 2008).

China

The role of China in international telecommunication is seen as a complex and also complicated issue. Following the latest data of the International Telecommunication Union (ITU), China has 298 million Internet users leaving the USA with 230 million behind (ITU Internet Statistics 2008). Due to its population size this number refers to only a small part of the whole country: around 22%, mainly situated in the urban centers of the country. While ICT companies and analysts see China as the market with the biggest growth potential for further investments, global civil society organizations and foreign (mainly Western) governments regularly complain about national Internet filter and censorship as well as constantly occuring cyberattacks. Different than in the Russian case, cyberattacks from China have so far not targeted foreign networks in the same complexity and with comparable destructive results like in Estonia or Georgia. They were rather concentrated on individual networks in different countries often with the intention of espionage.

Early cases of cyberattacks from China go back to the end of the 1990s. As a response to a massive demonstration of Falun Gong members in Beijing in April 1999, a number of servers in the USA, Canada and the UK hosting websites of the movement fell victim to cyberattacks (Wacker, 2000, p. 36). In the same year cyberattacks happened on US networks after the bombing of the Chinese embassy in Belgrade as stated above. Interesting to mention is in this context, that at that time the Internet was a relatively new network that was used only by a small percentage of the population, a big part of them being university members. In December 1999 only 3,5 million computers in China had access to the Internet. They were used by an estimated number of 8,9 million people, less than 1% of the whole population (Wacker, 2000, p. 11).

Over the years more similar attacks occured that were connected to particular events like an airplane accident involving two machines from China and the USA, causing the death of the Chinese pilot in April 2001 (known as the Hainan Island incident). This crash resulted in massive cyberattacks from China on US governmental networks and vice versa (Smith, 2001). The attacks were conducted by Chinese and American patriotic hackers which openly declared responsibility on the net. While this "First World Hacker War" (Smith, 2001), which caused serious damage to parts of American critical infrastructure (Cornish, 2009, p. 14), was based on mutual cyber activities, in the following years China conducted more secret cyberattacks, targeting public institutions in different countries with the intention to illegitimately transfer information to their own networks.

It is unlikely that the Kremlin was directly involved in any cyberattacks on Georgia although there are indications that officials from the lower political spectrum and the military could have been involved or at least have cooperated with virtual attackers.

In the last five years especially Western industrialized countries discovered virtual attacks on their governmental networks. In most cases the attackers tried (often successfully) to access public networks like the British Foreign Office, the US Pentagon, or the German Ministry of Exterior and others. In the majority of the cases mentioned, the attacks were traced back to Chinese networks, in some cases even directly to the Chinese Army (Norton-Taylor, 2007). US investigators suspect a Chinese espionage ring they called Titan Rain to be responsible (Thornburgh, 2005). Alex Neill, Asian security analyst at the British Royal United Services Institute, declared the attacks could be part of the "pressure point warfare" strategy of China's Army to weaken its opponents by "attacking...specific nodes to leave the adversary paralysed" (Norton-Taylor, 2007).

James Lewis from the Center for Strategic and International Studies in Washington DC is sceptical. Following his analysis the Chinese networks' vulnerability could attract third parties with the intention to attack foreign infrastructure and let investigators fall into the easy trap of (post-) Cold War logic:

> In the 1980s the Americans looked under their beds and believed they saw the KGB; now they believe they see the PLA [Peoples Liberation Army]. A hostile service from a third country might be drawn to use Chinese computers to launch an attack hoping that our proclivity to ascribe bad intent to China would cloud any investigation. (Lewis, 2005, p. 2).

Furthermore, Lewis pointed out that also China's officials would have used the way over a third country instead of leaving a trail back to their own networks. He suggested that cybercriminals could be responsible for virtual attacks on governmental networks to sell the information to any secret service that is willing to pay.

The most extensive cyberattack that was traced back to Chinese computers was discovered by researchers at the Munk Centre for International Studies at the University of Toronto and the Information Warfare Monitor. The results of their 10 months lasting research (June 2008 - March 2009) were published in March 2009. Initial point of the research was a request by the Office of the Dalai Lama to search its networks for probable malware. The infiltration of the office computers was assumed after Chinese officials proved to hold information about Tibetian exile politicians that they might have received through the Internet. During the investigations the researchers discovered that a large number of computers of the Tibetian community had been infiltrated by trojans which opened up the systems for intruders offering them access to content stored in the respective networks. Besides that, the attackers created the possibility for them to gather information by enabling microphones or webcams on the infiltrated computers (Deibert; Rohozinski, 2009, p. 34).

During the investigations the researchers discovered that besides Tibetian also a large number of other computers were connected to what they later called GhostNet. Between May 2007 and March 2009 at least 1295 computers from 103 countries were infiltrated by the espionage network (Deibert; Rohozinski, 2009, p. 40). 30% of the

networks attacked were considered by the researchers to be "high value targets" like ASEAN and NATO networks, embassies and foreign and other ministries of several countries like Bangladesh, Brunei, Germany, Indonesia, Pakistan, Portugal, South Korea, Taiwan and Vietnam, as well as news organizations, universities and private companies in Hong Kong, India, Russia the USA and more. A strong focus was found on governmental networks in South and South East Asia.

Tracing back the attackers, the researchers found out that 70% of the servers controlling GhostNet activities against Tibetian networks were located in China (Deibert; Rohozinski, 2009, p. 22). The rest was dispersed over different countries among them Sweden, Taiwan and the USA. Also a vast amount of servers attacking non-Tibetian goals was located in China. In this context it is interesting to notice that several servers were situated on the Chinese Hainan Island where intelligence and technical army facilities reside. Moreover the concentration on political, economic and military targets in South and South East Asian countries indicated that Chinese officials could be the operators of GhostNet. Nevertheless the report of the Information Warfare Monitor concluded that the necessary tools to built up espionage networks are available on the net and are not exclusively accessible by military or secret service officials. Also cybercriminals could build similar networks to gather and sell information, although GhostNet has a strong political character compared to formerly discovered criminal networks. What in turn suggests a non-responsibility of Chinese officials is the argument also brought up by James Lewis before, stating that other states could have built GhostNet using Chinese infrastructure to lead investigators on the wrong track.

Considering the cautiousness of the report concerning responsibles behind the virtual attacks, it is remarkable to compare it to a second one, composed by two researchers from the University of Cambridge who also have been involved in the research on GhostNet. In "The Snooping Dragon", Shishir Nagaraja and Ross Anderson give a different point of view about the origins of GhostNet. They clearly stated the responsibility of the Chinese government to attack Tibetian networks. In the first sentence of the abstract they introduced their paper as treating "a case of malware-based electronic surveillance of a political organization by agents of a nation state." (Anderson; Nagaraja, 2009, p. 3). They further claimed that the "surveillance attack [was] designed to collect intelligence for use by the police and security service of a repressive state..." (Anderson; Nagaraja, 2009, p. 3). In their conclusion they amplified this aspect by pointing out: "People in Tibet may have died as a result." (Anderson; Nagaraja, 2009, p. 11).

Conclusion

The first decade of the 21st century has seen a rise in both quantity and quality of virtual attacks on political and economic networks in different countries. Although already in the 1990s information warfare campaigns like in the Kosovo war or hacker attacks like between Chinese and American citizens took place, since 2004 a growing number of serious cyber aggressions could be watched. Besides website defacements, the spreading of different types of malwares, hacking and distributed denial of service attacks were among the most applicated measures in several countries. The motivation of the attackers ranged from pure and openly announced destructiveness to secret espionage activities. While in the cases of Estonia and Georgia, cyber activities took place parallel to inter-ethnic or military conflicts, the GhostNet operators tried to gather information from different locations while trying to hide its own existence to not endanger the online operations.

In most cases, attackers tried (often successfully) to access public networks like the British Foreign Office, the US Pentagon, or the German Ministry of Exterior and others. In the majority of the cases mentioned, the attacks were traced back to Chinese networks, in some cases even directly to the Chinese Army.

The questions of who are the main actors and how to trace back virtual attacks are closely connected to each other. Analysing the attacks on Estonia and Georgia and also the GhostNet activities it is obvious that most victims almost automatically refered to Russia and China and in general blamed the national governments, its secret services or military arms to be responsible. Nevertheless in none of the cases it was possible to prove the involvement of the respective actors. Comparing different research reports it becomes clear, that some tend to make national governments responsible for the reason of logical conclusions based on political relations between different actors. One example for this is the Cambridge University report on GhostNet in which the authors clearly stated Beijings responsibility. A strong argument for the involvement of political actors, for example in case of Estonia, is the revelation of the Kremlin's youth organization Nashi as well as their financial resources that could make the payment

of botnets possible. Also the involvement of botnets used against Estonia in former activities against Russian opposition parties indicate the responsibility of political actors.

In other cases like the Information Warfare Monitor report, the editors pointed out, that a variety of actors could be involved, coming from the governmental level or from a non-political criminal background. Although information gathered during the GhostNet process showed a high concentration on political targets, especially in the South and South East Asian region, the intruders do not necessarily need to have a political background. Cybercriminal activities are a constantly growing phenomenon and while some of its protagonist try to enrich themselves by stealing creditcard passwords, others might collect and sell political information. In this context also the Russian Business Network appears as a criminal organization whose servers were involved in DDoS attacks in the post-Soviet region. The possibility for the RBN to act freely within Russia for years must be considered as an international problem of cybercrime activities.

Analysing the attacks on Estonia and Georgia and also the GhostNet activities it is obvious that most victims almost automatically refered to Russia and China and in general blamed the national governments, its secret services or military arms to be responsible. Nevertheless in none of the cases it was possible to prove the involvement of the respective actors.

Besides possible governmental and cybercriminal participation also patriotic hackers and script kiddies play an important role in both cases of Russia and China. As they usually announce their activities on public online forums, their participation in different virtual attacks is much more obvious. With their big population both Russia and especially China pose a certain threat to smaller states' networks as patriotic hacker attacks with a significant number of participants can cause serious damage. The growing number of Internet users in China can in situations of political tensions be considered a factor of possible network instability in competing countries.

The fact that it is impossible to track down responsibles for virtual attacks lies also in the impossibility to trace back online activities. Although IT analysts frequently spot attacking servers via their IP numbers, it cannot be said for sure if those servers are in deed responsible or if they serve as proxy servers, disguising the true attackers.

In the coming years the Internet will be accessed by a permanently growing number of people. National governments still have a long way to go to guarantee safe access and usage of the net. Therefore the problem of cybersecurity must be taken more seriously by all governments and other actors involved. The attention paid by US President Obama, as it was mentioned in the introduction of this article, is a clear sign in the right direction. Now other governments have to take similar measures to enhance the development of cybersecurity policies on a global scale. Badly protected networks can result in the breakdown of crucial infrastructure which especially in times of political crises can make a country extremely vulnerable. Considering the results of this article, the words of Joseph Nye so far will remain true: "In the murky world of the Internet, attackers are difficult to identify." (Nye, 2008, p. 1).

Bibliography

ADAIR, STEVEN: The Website for the President of Georgia Under Attack – Politically Motivated? Shadowserver Foundation, 20 July 2008. Available at: http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080720 - Accessed 22 March 2009

ANDERSON, ROSS; NAGARAJA, SHISHIR: The Snooping Dragon: Social-Malware Surveillance of the Tibetian Movement, University of Cambridge, Computer Laboratory, Technical Report No 746, March 2009. Available at: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf - Accessed 22 March 2009

ARKIN, WILLIAM M.: The Cyber Bomb in Yugoslavia, Washington Post, 25 October 1999

Available at: http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm - Accessed 22 March 2009

BORGEN, CHRISTOPHER J.: Imagining Sovereignty, Managing Secession: The Legal Geography of Eurasia´s "Frozen Conflicts", Legal Studies Research Paper Series, Paper #09-0168, St John´s University School of Law, February 2009. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1345846 - Accessed 22 March 2009

CHABROW, ERIC: cyberattacks: How Worried Should We Be? Holiday Hackers Victimize White House, Pentagon, NYSE Sites, GovInfo Security, 9 July 2009. Available at: http://www.govinfosecurity.com/articles.php?art_id=1613 - Accessed 22 March 2009

CLOSSON, STACY; HALBACH, UWE: Die

Georgienkrise In Ihrer Kaukasischen Dimension, SWP-Aktuell 75, Berlin, Oktober 2008. Available at: http://www.swp-berlin.org/produkte/swp_aktuell_detail.php?id=9805 - Accessed 22 March 2009

CLOVER, CHARLES: Kremlin-Backed Group Behind Estonia Cyber-Blitz, Financial Times, 11 March 2009. Available at: http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.htmlnclick_ check=1 - Accessed 22 March 2009

COMMISSION OF THE EUROPEAN COMMUNITIES: Critical Infrastructure Protection in the Fight Against Terrorism, COM (2004) 702 final, Brussels, 20 October 2004

CONSTANTIN, LUCIAN: The Embassy of Portugal in India Falls Victim To Hackers, Softpedia.com, 21 March 2009a. Available at: http://news.softpedia.com/news/The-Embassy-of-Portugal-in-India-Falls-Victim-to-Hackers-107420.shtml - Accessed 22 March 2009

CONSTANTIN, LUCIAN: Websites of Three More Embassies Spreading Malware, Softpedia.com, 17 March 2009b. Available at: http://news.softpedia.com/news/Websites-of-Three-More-Embassies-Spreading-Malware-106995.shtml - Accessed 22 March 2009

CORBIN, KENNETH: Lessons From The Georgia-Russia Cyberwar, Institute of Communication Studies, University of Leeds, 12 March 2009. Available at: http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=gdr&requesttimeout=500&folder= 442&paper=750 - Accessed 22 March 2009

DAVIS, JOSHUA: Hackers Take Down the Most Wired Country in Europe, Wired Magazien, Issue 15.09, 21 August 2007. Available at: http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all - Accessed 22 March 2009

DEIBERT, RON; ROHOZINSKI, RAFAL: Tracking GhostNet: Investigating a Cyber Espionage Network, Information Warfare Monitor, March 2009, Toronto. Available at: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network - Accessed 22 March 2009

DUNN, MYRIAM A.: The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue With Assistance of the Morphological Method. In: Information and Security, Vol 7, 2001, pp 145-158

CORNISH, PAUL: Cyber Security and Politically, Socially and Religiously Motivated cyberattacks, European Parliament, Policy Department External Policies, February 2009

Available at: http://www.chathamhouse.org.uk/publications/papers/view/-/id/702/ - Accessed 22 March 2009

FAZ.NET: Ist Ein Internetangriff der Ernstfall? 18 June 2007.

Available at: http://www.faz.net/s/RubDDBDABB9457A437BAA85A49C26FB23A0/Doc~E7CCF 88CEFB 6F467BB8D75A400C07B959~ATpl~Ecommon~Scontent.html - Accessed 22 March 2009

FOSSATO, FLORIANA; LLOYD, JOHN; VERKHOFSKY, ALEXANDER: The Web That Failed, Reuters Institute for the Study of Journalism, University of Oxford, 2008. Available at: http://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/The_Web_that_Failed.pdf - Accessed 22 March 2009

GERRING, JOHN: What Is a Case Study and What Is It Good for? American Political Science Review. Vol 98 No 2. May 2004

GOODWIN, JACOB: Russian "Hacktivists" Used Turkish Botnets to Attack Georgia, Government Security News Magazine, 23 September 2008. Available at: http://www.gsnmagazine.com/cms/market-segments/intelligence/1042.html - Accessed 22 March 2009

GORMAN, SIOBHAN: Electricity Grid in U.S. Penetrated by Spies, Wall Street Journal, 8 April 2009. Available at: http://online.wsj.com/article/SB123914805204099085.html - Accessed 22 March 2009

GRANT, IAN: Kaspersky reveals price list for botnet attacks, ComputerWeekly.com, 23 July 2009

Available at: http://www.computerweekly.com/Articles/2009/07/23/237015/kaspersky-reveals-price--list-for-botnet-attacks.htm - Accessed 22 March 2009

HANSEN, LENE; NISSENBAUM, HELEN: Digital Disaster, Cyber Security, and the Copenhagen School, in: International Studies Quarterly, Vol 53, No 4, December 2009, pp. 1155-1175

HELLER, REGINE: Die Russische Jugendbewegung „Naschi". Aufstieg Und Fall Eines Polittechnologischen Projekts in der Era Putin, in: Russland-Analysen Nr 168, Deutsche Gesellschaft für Osteueropakunde, 11 July 2008. Available at: http://www.laender-analysen.de/dlcounter/dlcounter.php?url=../russland/pdf/Russlandanalysen168.pdf - Accessed 22 March 2009

ITU Internet Statistics 2008. Available at: http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&RP_intYear=2008&RP_intLanguageID=1 - Accessed 22 March 2009

JOHNSON, MIKE: Georgian Websites Under Attack – Don´t Believe the Hype. Shadowserver Foundation, 12 August 2008. Available at: http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080812 - Accessed 22 March 2009

KERR, KATHRYN: Putting Cyberterrorim into Context, Computer Crime Research Center, 09 October 2004. Available at: http://www.crime-research.org/articles/putting_cyberterrorism/1 - Accessed 22 March 2009

KIRK, JEREMY: Student Fined For Attack On Estonian Website, InfoWorld, 24 January 2008

Available at: http://www.infoworld.com/d/security--central/student-fined-attack-against-estonian-web--site-794. Accessed 22 March 2009

KIRK, JEREMY: Georgia Cyberattacks Linked to Russian Organized Crime, PC World, 17 August 2009. Available at: http://www.pcworld.com/article/170289/georgia_cyberattacks_linked_to_russian_ organized_ crime.html - Accessed 22 March 2009

KÖNIG, MARIETTA S.: Not Frozen But Red Hot: Conflict Resolution in Georgia Following the Change of Government, in: OSCE Yearbook 2006, Centre for OSCE Research, Hamburg 2006

Available at: http://www.core-hamburg.de/CORE_English/pub_osce_inh_06.htm - Accessed 22 March 2009

LANG, KAI-OLAF: Die baltischen Staaten und ihr schwieriges Verhältnis zu Russland, SWP-Aktuell 2008/A 61, July 2008. Available at: http://www.swp-berlin.org/de/publikationen/swp-aktuell-de/swp-aktuell--detail/article/russland_baltische_staaten_schwieriges_verhaeltnis.html - Accessed 25 May 2009

LEWIS, JAMES ANDREW: Computer Espionage, Titan Rain and China, Center for Strategic and International Studies, Technology and Public Policy Program, December 2005, Washington DC

Available at: http://csis.org/publication/computer-espionage-titan-rain-and-china - Accessed 22 March 2009

LEYDEN, JOHN: Bear Prints Found on Georgian Cyber-Attacks, The Register, 14 August 2008

Available at: http://www.theregister.co.uk/2008/08/14/russia_georgia_cyberwar_latest/ - Accessed 22 March 2009

MARKOFF, JOHN; SANG-HUN, CHOE: Cyberattacks Jam Government And Commercial Websites in U.S. and South Korea, New York Times, 9 July 2009. Available at: http://www.nytimes.com/2009/07/09/technology/09cyber.html - Accessed 22 March 2009

McNABB, DAVID E.: Research Methods for Political Science. Quantitative and Qualitative Methods, M.E. Sharpe, London 2004

McQUADE, SAMUEL: Understanding and Managing Cybercrime, Pearson Boston, 2006

MEHAN, JULIE E.: Cyberwar, Cyberterror, Cybercrime, IT Governance Publishing Ely, 2008

MESSMER, ELLEN: Kosovo Cyber-War Intensifies: Chinese hackers Targeting US Sites, Government Says, CNN, 12 May 1999. Available at: http://www.cnn.com/TECH/computing/9905/12/cyberwar.idg/ - Accessed 22 March 2009

MOTEFF, JOHN; PARFOMAK, PAUL: Critical Infrastructure and Key Assets: Definition and Identification, CRS Report for Congress, 1 October 2004

NAKASHIMA, ELLEN: Top Cybersecurity Aide At White House Resigns, Washington Post, 4 August 2009. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2009/08/03/AR2009080 302697.html

NOHLEN, DIETER: Lexikon der Politik, Band 2: Politikwissenschaftliche Methoden, C.H. Beck, München 1994

NORTON-TAYLOR, RICHARD: Titan Rain – How Chinese Hackers Targeted Whitehall, Guardian, 5 September 2007. Available at: http://www.guardian.co.uk/technology/2007/sep/04/news.internet - Accessed 22 March 2009

NYE, JOSEPH S.: Cyber Insecurity, Project Syndicate, Cambridge, December 2008. Available at: http://www.project-syndicate.org/commentary/nye65 - Accessed 22 March 2009

OPENNET INITIATIVE: Commonwealth of Independent States. Available at: http://opennet.net/research/regions/cis - Accessed 22 March 2009

RANNUT, MART: Language Policy in Estonia, in: Noves SL, Revista de Sociolingüística, Spring- Summer 2004. Available at: http://www6.gencat.net/llengcat/noves/hm04primavera-estiu/rannut1_6.htm - Accessed 05 March 2009

SMITH, CRAIG S.: May 6-12; The First World Hacker War, New York Times, 13 May 2001

Available at: http://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html - Accessed 22 March 2009

SPIEGEL ONLINE: Chinesische Trojaner Auf PCs Im Kanzleramt, 25 August 2007a. Available at: http://www.spiegel.de/netzwelt/tech/0,1518,501954,00.html - Accessed 22 March 2009

SPIEGEL ONLINE: China-Hacker Griffen Auch Britische Regierung An, 5 September 2007b. Available at: http://www.spiegel.de/netzwelt/tech/0,1518,503921,00.html - Accessed 22 March 2009

SPIEGEL ONLINE: Cyberangriffe Auf Estland Alarmieren EU Und NATO, 17 May 2007c. Available at:

http://www.spiegel.de/netzwelt/web/0,1518,483416,00.html - Accessed 22 March 2009

STEVENS, TIM: The Internet smokescreen, Open Democracy, 21 August 2008, Available at: http://www.opendemocracy.net/terrorism/article/tim_stevens/internet_smokescreen - Accessed 22 March 2009

SUEDDEUTSCHE.DE: Jugendliche Greifen Estnische Botschafterin An, 2 Mai 2007a

Available at: http://www.sueddeutsche.de/politik/631/356459/text/ - Accessed 22 March 2009

SUEDDEUTSCHE.DE: Chinesische Hacker Greifen Pentagon An, 4 September 2007b

Available at: http://www.sueddeutsche.de/politik/460/417226/text/ - Accessed 22 March 2009

THOMAS, TIMOTHY L.: Like Adding Wings to the Tiger: Chinese Information War Theory and Practice, Foreign Military Studies Office Publications, 2000. Available at: http://www.au.af.mil/au/awc/awcgate/fmso/chinaiw.htm - Accessed 20 March 2009

THORNBURGH, NATHAN: Inside The Chinese Hack Attack, Time, 25 August 2005. Available at: http://www.time.com/time/nation/article/0,8599,1098371,00.html - Accessed 20 March 2009

VETIK, RAIVO: Ethnic Conflict and Accommodation in Post-Communist Estonia, in: Journal of Peace Research, Vol 30, No 3, 1993, pp. 271-280

WACKER, GUDRUN: Hinter Der Virtuellen Mauer: Die VR China Und Das Internet, Bundesinstitut für Ostwissenschaftliche und Internationale Studien, Köln 2000. Available at: http://www.ssoar.info/ssoar/View/?resid=4146 - Accessed 20 March 2009

WALL, DAVID S.: Cybercrime, Polity Cambridge, 2008

WARREN, PETER: Hunt For Russia´s Web Criminals, Guardian, 15 November 2007. Available at: http://www.guardian.co.uk/technology/2007/nov/15/news.crime - Accessed 20 March 2009

WATERMAN, SHAUN: Georgia Blames Russia for Cyberattack on Web Sites, Cell Phones, UPI.com, 11 August 2008. Available at: http://www.upi.com/Emerging_Threats/2008/08/11/Georgia-blames-Russia-for-cyberattack-on-Web-sites-cell-phones/UPI-37681218494483/ - Accessed 20 March 2009

WEIMANN, GABRIEL: Terror on the Internet, United States Institute of Peace Press, 2006

YIN, ROBERT K.: Case Study Research, Sage Publications London, 2003