35 ▶ 46

State Responsibility in the Cyber Age: The Course towards Indirect Evidence

LUCIE KADLECOVÁ

Abstract: The problem of attributing responsibility for cyber-attacks is almost as old as cyberspace itself, yet it remains one of the most troublesome issues of that domain. It is often impossible to uncover direct evidence that would reveal the identities of the attackers. Investigators must therefore rely on other, more indirect avenues of proof. The aim of this exploratory study is to develop a basic categorisation of indirect evidence that can be used to attribute state responsibility for cyber-attacks in international relations. To do so, the article works with international legal concepts but transposes them into the analysis of international relations. The categorization of indirect proof is based on the Russian-Georgian conflict of 2008, which provides one of the richest arrays of this kind of evidence. The analysis identifies four kinds of indirect evidence: level of coordination, level of preparedness, state relations with the national hacker community, and state conception of cyber-security.

Key words: attribution, state responsibility, indirect evidence, cyberspace, Russia, Georgia.

DOI: <https://doi.org/10.32422/mv.1585>.

The cyber operations during the Russian-Georgian conflict in August 2008 might initially appear to be a strategically unimportant example of an attack in cyberspace that was overshadowed by the military campaign on the ground. The kinetic military operations lasted five days and were characterised by conventional warfare that was constrained by the limited communication environment. However, cyber-attacks on Georgian websites played a crucial *"if not decisive"* role in the overall campaign (Deibert – Rohozinski – Crete-Nishihata 2012: 4), as control of cyberspace quickly became a strategic advantage in the conflict. Security experts immediately became concerned about the identities of the perpetrators of the cyber-attacks on Georgia. Although the Kremlin has never acknowledged any involvement of Russia in activities against Georgia in cyberspace in August 2008, a number of state representatives and cyber experts, together with most of the media, either directly or indirectly pointed their fingers at the Russian government in connection with this matter.[1] On what basis could these actors claim what they claim?

We are often in lack of convincing direct evidence which would allow us to attribute responsibility for cyber-attacks in terms of international law. Yet, many international actors do not hesitate to attribute responsibility in political terms, and with political consequences. It is clear that key actors in international law and international relations understand the issue of attribution in different ways – international law perceives it through the work of international courts of justice and lawyers who apply binding international legal rules while international relations are based on the (oftentimes rather

pragmatic) behaviour of governments and international organisations, and the work of politicians, journalists or, for example, activists. They have different understandings of what is viable and legitimate in their fields. There are various methods which define states' behaviour within international relations which, however, might not be necessarily supported by international legal norms. On the other hand, states oftentimes acknowledge international legal governance, but their reaction is political in the end. In this regard, this article works with international legal concepts, but transposes them into the analysis of international relations. As such, the article at hand is an exploratory study which aims to highlight and examine the importance of indirect evidence, which is an international legal concept, in the political attribution of state responsibility for cyber-attacks in international relations.[2] The goal of this article is to introduce a basic categorisation of indirect evidence which could serve as a starting point for future research on the given topic. In other words, accepting that direct evidence is mostly unavailable, the article asks which indirect evidence might be available to reliably establish attribution in international relations.

Attribution and state responsibility in other contexts than cyber security are amongst the most fully developed concepts in international relations and law. However, given the peculiar characteristics of cyberspace, where attributing the cyber-attack to a particular perpetrator can become a highly difficult political issue, there exists only a paucity of well-argued sources that would focus on the key role of indirect evidence. Nevertheless, the debate on the topic has been evolving quickly lately and there are certain works which deserve to be highlighted at this point. The most significant contribution in this regard is, without hesitation, *Tallinn Manual 2.0* by Professor Michael Schmitt (2017) and his team of experts, who, among other things, formulated several rules for attribution of cyber operations by various actors and, subsequently, state responsibility for such operations. Although the rules of *Tallinn Manual 2.0* are non-binding, the book is, to date, one of the most authoritative sources in legal writing on how international law applies to cyber operations. Recent works by Professor Nicholas Tsagourias (2016) and Kubo Mačák (2016) must also be mentioned as valuable contributions to the latest debate on non-state actors and attribution. Two studies by Richard Andres and Scott Shackelford (2010–2011) and Jason Healey (2011) should be mentioned too as they address the threshold of proof necessary to constitute responsibility, which is important for this study. Still, none of these most recent works on attribution and state responsibility addresses the importance of indirect evidence enough and thus, this article aspires to contribute to filling the above-described gap in the literature.

The importance of indirect evidence in the attribution of state responsibility in cyberspace will be illustrated on the case of the Russian-Georgian conflict of 2008. Although that case is a decade old, it is an example which involved the richest variety of indirect evidence of different kinds given that the cyber campaign accompanied military attacks on ground and thus served as a force multiplier. Moreover, because of the lapse of time between the campaign itself and the publication of this article, there is a sufficient number of quality sources for the discussion, as other potential cases for a study of this sort such as the 2015 cyber-attacks against Ukrainian power grids would not provide such an advantage. The Russian-Georgian war was a typical example of the high degree of care with which cyber-attacks are usually prepared and of the timing and coordination of cyber and kinetic operations. The alleged good relations between the Kremlin, Russian organised crime and Russian youth organisations can serve as further possible indirect proof of certain involvement of Russian government in the cyber-attacks during the war. Because the Russian government has rejected all accusations of its involvement in the cyber-attacks, and no substantive direct link between the perpetrators of the attacks and the Russian government has ever been found, the chance that direct evidence would be uncovered to establish state responsibility in this case is marginal, as it is in the majority

of similar cases. The Georgian case thus emphasises the importance of indirect evidence and illustrates the broad range of its types.

This article begins by examining the concepts of attribution and state responsibility within the international legal framework applied to cyberspace. In that context, the article surveys the most often proposed doctrines of state responsibility attribution: the effective and the overall control doctrine. The following analytical section has five subsections. The first sub-section introduces the security and political context of the Russian-Georgian conflict in 2008. The following four sub-sections identify four different categories of indirect evidence of state responsibility for cyber-attacks: level of coordination, level of preparedness, state relations with the national hacker community, and the state conception of cyber-security.

ATTRIBUTION OF STATE RESPONSIBILITY IN CYBERSPACE

The cyber-attacks on Georgia during the Russian-Georgian conflict in the summer of 2008 most probably contributed to the current widespread trend of tagging cyberspace the "fifth domain" of military combat alongside land, sea, air, and space. However, unlike in the cases of these four historically codified domains, a suitable international legal regime of cyberspace which would regulate it and include both *jus ad bellum* and *jus in bello* has appeared to be elusive so far, notably regarding the crucial issues of attribution and state responsibility. Modern technological advancement and its subsequent use in practice raises a range of international relations and legal concerns. For instance, cyber warfare deeply challenges the nature and understanding of the traditional perception of warfare. The attribution of a kinetic attack launched through conventional weaponry is obviously much easier to determine than the identity of a perpetrator of a cyber-attack. Alternatively, the transnational character of cyber-attacks leads to questioning of the current treaty framework, which is helpful but not sufficient since it does not properly cover issues such as state responsibility and sovereignty in cyberspace. The problems regarding defence against or launching of a cyber-assault are numerous, but the most fundamental issues are associated with attribution of these attacks and state responsibility for them. Although it can be technically possible to trace the geographical location of the attacker and so attribute the attack to some extent, it is difficult to actually determine who was sitting in front of the computer screen in the moment when the attack was launched; it could be a state representative, a group of hackers or an individual. Therefore, one of the critical challenges to the international relations and legal systems is keeping up with technological development.[3]

In the realm of international law, we could localise two principal competing doctrines of state responsibility – the effective control doctrine and the overall control doctrine. The two standards of state responsibility differ on whether the state must directly control the operation planning or not.

The doctrine of effective control originated in the International Court of Justice's *Nicaragua case* between the Republic of Nicaragua and the USA from 1984. The International Court of Justice (ICJ) asserted that the responsibility for the actions of private actors – both entities and individuals – might be attributed to the state only if the government executed its effective control over these actors. Since the USA did not have effective control over the paramilitaries in Nicaragua, the ICJ could not find Washington responsible for the activities of the contras (ICJ 1986). Hence, in order for a state to be found responsible for the conduct of private actors under the effective control doctrine, based on the *Nicaragua case*, it must explicitly delegate at least part of the tasks to such non-state actors (Tikk et al. 2008: 21). The effective control standard was reaffirmed in practice by the Court in the *Bosnian Genocide case* in 2007 so that Serbia was exculpated from the genocide in Srebrenica (ICJ 2007, paragraph 406). However, in contrast to the effective control doctrine, in its judgment in the *Tadić case* the International Criminal Tribunal for the former Yugoslavia (ICTY) concluded that the effective control

standard is inconsistent with the practice of states and is not in accord with the logic of principles of state responsibility (Tikk et al. 2008: 21). The ICTY (1999) concluded that if a state participates in the organisation and coordination of private actors, in addition to supporting them, it possesses sufficient overall control over them and so the conduct of the non-state actors can be attributed to the state.[4]

Given the secretive nature of cyberspace and cyber-attacks, the flexible overall control doctrine appears to be much more suitable for this kind of environment. According to this doctrine, it should be sufficient to find a proof of an operational control or support coming from a state, rather than a government's complete control over a cyber-attack. The following section employs the overall control doctrine in an analysis of the Russian-Georgian conflict of 2008.

CYBER-ATTACKS AND THE RUSSIAN-GEORGIAN CONFLICT

This section analyses the cyber-warfare in the Russian-Georgian conflict of 2008 and distils four different categories of indirect evidence from it. The analysis works mainly with secondary sources, such as publications from Project Grey Goose and other publications by recognised cyber experts (e.g. Dmitri Alperovitch [2009], Jeffrey Carr [2008], Jart Armin [2008a, 2008b], Eneken Tikk [et al. 2008] or Ronald Deibert, Rafal Rohozinski and Masashi Crete-Nishihata [2012]). The following analysis will begin with an introduction to the political and security background to the Russian-Georgian conflict in cyber-space in 2008. Later on, this section will introduce four different types of indirect evidence that can be used to attribute state responsibility for cyber-attacks.

Background to the conflict

After two months of intensive military activities and exercises on both sides of the frontier, the conflict escalated on 7 August 2008 when Georgian forces launched an assault against separatist forces in South Ossetia in order to subdue their provocation.[5] A day later, on 8 August, Russian troops entered South Ossetia through the Roki tunnel while launching an airstrike against Georgian territory. Moscow justified its decision by its right to protect Russian citizens in South Ossetia. Tbilisi viewed Russia's behaviour as an act of military aggression and reacted with a declaration of a state of war. The hostilities officially ceased on 12 August when President Saakashvili and President Medvedev agreed on a six-point ceasefire drafted by French President Sarkozy on behalf of the European Union. The peace agreement was officially signed by both sides of the conflict on 15 and 16 August (Deibert – Rohozinski – Crete-Nishihata 2012: 7–8).

The dispute between Georgia and Russia was not, however, limited only to operations in the air, on the ground, and at sea. It was the first time that an international political and military conflict was accompanied by orchestrated cyber-attacks of such a scale.[6] Georgian websites became a target of the first cyber-attacks several weeks before the actual operation on the ground began. The most serious assault preceding the war took place on 19 July 2008, when the website of President Saakashvili was unavailable for 24 hours. This was caused by a heavy distributed denial of service[7] attack (Tikk et al. 2008: 36). The peak of the attacks in cyberspace took place in the week beginning on 8 August, coinciding with the rise of military operations on the Russian-Georgian borders. The cyber-attacks became well-orchestrated and coordinated with the development on the ground by that time. The last serious cyber-attack against Georgia's websites was registered on 27 August, only a couple of days after the peace agreement was signed.

It remains unclear exactly what role the Russian government played; whether the Kremlin encouraged the cyber operations against Georgia, coordinated them as an element of a wider political strategy, or simply tolerated them while they were launched by third parties. Nonetheless, there still exist enough clues from various sources which suggest at least some level of involvement of the Russian authorities in the cyber operations against

Georgia. These clues include the four types of indirect evidence that provide enough space for a political decision on attribution to be reached in this case.

Timing and coordination

The first category of indirect evidence is the timing and coordination of the attacks taking place in cyberspace and on the ground. Although some minor cyber-attacks on Georgian websites had been launched a couple of days or weeks before the Russian troops entered Georgian territory, the major wave of assaults in cyberspace was coordinated with the main military operation. It appears that the organisers of the cyber-attacks had advanced knowledge of what the Russian military intentions were and subsequently, they were given notice about the Russian campaign on the ground while the assaults were being executed. The cyber-attacks of the largest scale commenced at the same time that the Russian military began its operations, and they ended just a while after the Russians accomplished the aims of their campaign so it almost indicates that the operation in cyberspace supplemented those on the ground (Bumgarner – Borg 2009: 6). Asmus (2010: 167) also takes note of a high degree of *"discipline, coordination, command, and control"* in the cyber-attacks against the Georgian financial and banking sector, which closely followed the kinetic operations on the ground.

John Bumgarner and Scott Borg (2009: 6) from the U.S. Cyber Consequences Unit also point out the telling choices of the targets for the cyber-attacks, as in most of the cases, attacks against these targets would have brought benefits for Moscow. They claim that during an ordinary military assault the communication facilities and media stations are usually destroyed or at least damaged by airstrikes or bombs. In the case of Georgia, they were spared physical damage and were put out of order by cyber-attacks instead. A tangible example is the case of the city of Gori, where the official websites and news sites were shut down before the Russian military aircraft even reached the city (Menn 2008). Thus, it seems that quite a widespread consensus exists that the operations in cyberspace and on the ground appear coordinated from the beginning in regard to both timing and the choice of targets.

Level of preparedness

The second category of indirect proof which indicates a close cooperation between the civilian cyber perpetrators and Russian military staff is the level of preparedness of the cyber-attacks. Not only were the attacks on the ground and in cyberspace close in time. The cyber-attacks, after they were launched, skipped the mapping and reconnaissance stage and immediately started employing the right kind of packets that were well suited for the particular website attacks (Bumgarner – Borg 2009: 3). Moreover, many of the attackers' activities at the beginning of the campaign, such as setting up new websites or registration of new domain names, were carried out with noteworthy speed and readiness. This development suggests that the preparation stage and steps such as the writing of necessary attack scripts must have been done in advance. Bumgarner and Borg (2009: 3) point out that the signal to launch the cyber-attacks was most probably given even before the general public and media were notified about the situation on the ground.

The argument concerning the high level of preparedness of the attacks is further elaborated when one studies the defacement of Georgian official websites. The website of the National Bank of Georgia was defaced during the Russian-Georgian war and replaced with a collage which displayed a gallery of 20th century authoritarians and dictators, including Mikheil Saakashvili. Furthermore, the websites of the Georgian Ministry of Foreign Affairs and the President of Georgia were defaced with a collage of photographs portraying President Saakashvili and Adolf Hitler in identical postures during their public appearances (Tikk et al. 2008: 7). The preparation of this kind of defacement requires time in order to create the design and find the appropriate photo material.

Even the distribution of malicious software and information on how and which Georgian websites were to be attacked can arouse suspicion. Posting cyber-attack tools on specially designated websites was the main method for attackers to expand the cyber campaign. The fact that the attacked websites' vulnerabilities were discovered and exploited signals a certain level of planning, targeted reconnaissance and technical sophistication (Tikk et al. 2008: 38–39). Moreover, although the two types of cyber-attacks launched against Georgian websites – defacement and denial of service – are usually considered to have a rather unsophisticated nature, in this case, the operations were carried out in a highly sophisticated way. Cyber security researcher Jart Armin (2008a, 2008b) even notes that the character of these attacks strikingly reminds one of the methods usually employed by the organised cyber crime mob Russian Business Network (RBN)[8] in order to avoid investigation and put the blame on other suspects.

Social networks quickly became the attackers' main source of spreading malicious software and instructions as well as recruiting new people and discussing further development. Almost all of these blogs and forums were written in the Russian language.[9] An example of such a website is stopgeorgia.ru (or alternatively stopgeorgia.info as a redirect), which listed a number of targeted Georgian websites and provided denial of service tools for free download. Danchev (2008) uses the example of stopgeorgia.ru to illustrate that next to the dedicated hacktivists behind the attacks there is also the mass of the unskilled but keen script kiddies who might even serve to mask the real perpetrators. The website stopgeorgia.ru was also studied as part of research carried out by Project Grey Goose, an in-depth Open Source Intelligence (OSINT) initiative launched by a group of independent cyber experts on 22 August 2008 and led by Jeffrey Carr. Its key purpose was to study the ways in which the cyber-attacks against Georgian networks were conducted and whether the Kremlin was involved or whether it was purely an initiative of Russian patriotic hackers (Carr 2008: 2). While the researchers from Project Grey Goose claim that evidence such as that of advance preparation and reconnaissance suggests that Russian military or government officials primed hackers for the cyber-attacks, they also add that they could not find any direct proof which would confirm the link between the Kremlin and the stopgeorgia.ru website administrators or the attackers on Georgian computer networks in general. Nevertheless, they still defend their opinion and note that *"it is not reasonable to conclude that no such connection exists"*, pointing to the fact that past experience has already demonstrated support by the Russian government for Russian hacker attacks and its passive consent to the attacks, which was implied in its refusal to stop them (Carr 2008: 8; also see Krebs 2008).

State relations with the national hacker community

The relations between the government of the suspected state and the national hacker community represents the third possible type of indirect evidence that can be used to attribute responsibility for cyber-attacks to states. Russia is traditionally known for its distinctive features of a huge reliance on cyber-crime structures, such as the aforementioned RBN, and technologically educated individuals from youth organisations such as *Nashi*, which is controlled by the Kremlin, and one has to bear in mind that the boundary between the two might often be very thin (Smith 2012: 3).

After the dissolution of the Soviet Union, an unstable economy and limited labour market opportunities resulted in many highly educated and technologically qualified Russian individuals starting their own cyber-crime activities. These factors combined with a lack of legal enforcement and a power vacuum then contributed to the boom of cyber-crime business in Russia (Kadlecová 2015), including clandestine activities for the Russian government in the post-Soviet era (Alperovitch 2009). Oleg Gordievsky, a former KGB Colonel until his defection to the British MI6 in 1985, openly explained to the public at an international conference in 1998 how hackers convicted of cyber-crimes in Russia are

occasionally offered an alternative to imprisonment – employing their technological skills and working for the Russian FSB (Krebs 2008). Khatuna Mshvidobadze (2011) highlights another example of such suspicious Russian cyber activities – the Russian internationally-known "hacker schools", where tuition fees are often paid by unspecified donors. One of such hacker education institutions in Russia is supposedly run by the former Federal Agency for Government Communications and Information (FAPSI) in Voronezh. Moreover, *Khaker: Computer Hooligan Magazine* is particularly popular among the young generation in Russia, where any print content unacceptable to the Kremlin usually suffers from serious existential obstacles (Mshvidobadze 2011). Hence, it appears that Russia has a great potential to preserve its status as a cyber-crime power.

Furthermore, the Russian government does not rely merely on social trends and the development of Russian society but it attempts to influence and control the young generations, which also have a strong cyber security potential, through youth organisations and movements. The most notorious one is the Youth Democratic Anti-Fascist Movement "Ours!" (*Molodezhnoye Demokraticheskoye Antifashistskoye Dvizhenye* in Russian), also known as *Nashi*. *Nashi* was founded in 2005 with two main goals: firstly, it was meant as a counterweight to the growing popularity of Nazi ideology in the Russian Federation. Secondly, it was supposed to be a political tool to help Russia avoid a similar youth revolt like the one which evolved during the Orange Revolution in Ukraine in 2004 (Atwal 2009). Although it officially claims to be funded by Russian business elites, speculations exist which claim that it gains its finances from the Kremlin (Carr 2011, Betz – Stevens 2011: 32). The purported link between *Nashi* and the Russian government is also based on other strong evidence. For example, in the late 2000s Vladislav Surkov, the then First Deputy Chief of the Presidential Staff and one of the closest co-workers of Vladimir Putin, was a very keen supporter of *Nashi*. He even proclaimed the intention to use *Nashi*'s computer skills to enhance the will of the Kremlin in Russian cyberspace and to *"ensure the domination of pro-Kremlin views on the Internet"* (Carr 2009: 21). A practical example of this proclamation was reported in February 2009, when the Russian media published a story uncovering how the government encourages and funds the establishment of Russian youth organisations that are to get involved in cyber operations, including hacking and the subsequent suppression of opposition groups (Carr 2009: 21). Similarly, in 2009 Sergei Markov, a then State Duma Deputy, released the information that his assistant, most probably Konstantin Goloskov, a *Nashi* Commissar, had participated as one of the leaders in a cyber-attack against Estonia two years earlier (Carr 2009: 22). Thus, it appears that the Kremlin might be taking advantage of its very good relations with the youth organisations and their technologically educated and talented individual members as well.

The state conception of cyber-security

Russia's official approach toward cyber security might also offer a clue as to whether the Russian government was or was not involved in the cyber-attacks on Georgia, thus forming the last type of categorisation of indirect evidence introduced in the article. As early as September 2000, the *Information Security Doctrine of the Russian Federation* defined three major objectives: the first of them is common to most of the world – *to protect strategically important information* (Security Council of the Russian Federation 2000). However, the other two objectives distinguish Russia from most of the democratic world: *"to protect against deleterious foreign information and to inculcate in the people patriotism and values"* (Smith 2012: 2–3). This doctrine has then settled a broader Russian cyber security framework for both the military and civilian spheres for the next decade.

The Russian public stance on issues of cyber security might be illustrated by the examples of two documents – the *Concept of a Convention on International Information*

Security (Russian Federation 2011) and the *Convention on Cybercrime* (Council of Europe 2001). The former was released in September 2011 and it defines the key issues which concern Russia in cyberspace. As Keir Giles (2012: 64) notes, the document sets Russia apart from the Western approach when it perceives *"the use of content for influence on the social-humanitarian sphere"* as a threat while most of the other countries consider a hostile code to be a real danger in this respect. The Concept also touches upon Internet sovereignty, which is a bone of contention for Russia, along with several like-minded states, and the rest of the world. Russia advocates that a state should control all Internet resources which are based within its physical frontier and subsequently it should manage its cyberspace according to the local legislation. This step would cause each state to define its own regulations of the Internet, which, as argued by the West, would undermine human rights as well as the interoperability of the Internet (Giles 2012: 65–66).

The Russian military command has adopted a similar approach. Security experts notice that the Russian armed forces have recently put a growing emphasis on cyber-attacks in their military doctrine, acknowledging their strategic value (e.g. Giles 2011: 50). Russia has accordingly adopted a broad cyber warfare doctrine, paying particular attention to offensive cyber weapons. The Russian cyber warfare approach is developed as a "force multiplier" (Schaap 2009: 133), a military tool which, when employed together with other combat forces, increases the potential and effect of that military force. In theory, this would mean that Russia's cyber strategy includes disruptions of the enemy's critical infrastructure, civilian and military communications capabilities or financial markets prior to or alongside a traditional military campaign on the ground (Schaap 2009: 133). Therefore, the combined kinetic and cyber campaign against Georgia in the summer of 2008 appears to be the first diffident implementation of the Russian military cyber strategy in practice. Although the attack focussed mostly on the suppression of Georgian strategic communication, not the national critical infrastructure, it still caused enormous psychological harm and contributed to the destabilisation of Georgia's nation in a critical time of danger.

CONCLUSIONS

The goal of this exploratory study was to articulate a basic categorisation of indirect evidence that can be used by international actors to attribute responsibility to states for attacks in cyberspace. Cyber-attacks committed by non-state actors that were supported by governments in various manners and on various scales have generally been more common in the past several years. States use the non-state actors to hide behind them so as to avoid accountability for malicious cyber campaigns. Hence, there is an urgent need for states which become victims of such cyber-attacks to start invoking state responsibility and thus narrow this grey area if they want international norms to apply to this new domain. So far, it seems that the only reliable way to determine state responsibility is to analyse indirect proofs which have the potential to build a strong attribution beyond a reasonable doubt in a number of cases.

The article works with the international legal concepts of attribution and state responsibility and transfers them into an analysis of international relations. It begins from the assumption that the overall control doctrine of state responsibility is more suitable for cyberspace in international relations than the effective control doctrine. In the overall control doctrine, it suffices to find a proof of an operational control or support coming from a state to invoke state responsibility, which lowers the necessary threshold of evidence. Thus, our judgement could draw from the more common indirect evidence rather than from the oftentimes lacking direct evidence.

The proposed categorisation of indirect evidence is based on an analysis of the Russian--Georgian conflict of 2008. On the one hand, the Russian government and officials have officially denied any engagement in the cyber-attacks and there is no first-hand evidence

proving their involvement. On the other hand, as a number of pieces of indirect evidence illustrate, it is most likely that the Kremlin encouraged the attacks and provided the attackers with the necessary information to coordinate the cyber and kinetic operations. This particular case study was chosen because it provides one of the richest arrays of indirect evidence of various kinds, illustrating the flexibility of this form of proof in comparison to investigating cyber-attacks solely with a focus on direct evidence.

The first category of significant indirect proof which can be considered during the process of attribution is the timing and coordination of the cyber-attacks. The more the attack's timing is orchestrated and the more it appears to be well-coordinated overall, the higher the probability of a state's involvement. A telling sign is how well the cyber-attacks are coordinated with events outside of cyberspace, especially when they are not publicly predictable, as a conventional military campaign would be. In such cases, the cyber-attacks can easily supplement the operations on the ground and multiply their effect. Without at least a certain degree of exchange of information between a sponsoring state and the perpetrators, a cyber campaign cannot be well-timed and coordinated.

A similar logic can be observed in regard to the second category of indirect proof – the level of preparedness. A number of different types of cyber-attacks require time for situation mapping, reconnaissance and implementation so that they reach the necessary sophistication and maximum psychological effect. For instance, the right offensive graphics or collage of pictures posted on a defaced ministerial website may cause not only a denial of information to citizens, but also an offensive effect targeting the citizens' psychology. To reach a certain level of sophistication in this respect, the perpetrators would need to receive intelligence from a state source and plan such cyber-attacks well in advance.

The third category of indirect evidence to investigate is the long-term relations between the state institutions and the national hacker community. For example, in countries with a long and prosperous history of criminal networks, criminal mobs oftentimes follow up on their usual activities with their malicious activities in cyberspace and thus might become convenient partners for a sponsoring state, especially if they can build on previously established contacts. A similar example is the case of youth organisations with a pro-government ideology and government contacts which unite young people with a talent for IT who are eager to support their state's activities.

Finally, the fourth category of indirect proof is the state conception of cyber security. The political, non-military national strategies and concepts of cyberspace are the first indicators suggesting the state's approach and behaviour in the cyber environment. Even more telling is the study of the military doctrines of the state, as they may indicate whether the state has inclinations toward building and using offensive cyber weapons or employing cyber-attacks as a force multiplier alongside conventional warfare.

The analysis provides the reader with a categorisation of indirect evidence which, however, has a limited impact. This article focussed only on one cyber campaign, thus offering only a limited number of types of indirect evidence, and not necessarily an exhaustive list of indirect evidence types. Thus, adding other categories to this categorisation of indirect evidence based on an analysis of a broader spectrum of individual cases from practice might certainly become a useful and much needed goal of future studies on the topic. Future research might also focus on other major cases of cyber-attacks – for example, the 2010 Stuxnet worm used against the Iranian nuclear programme, and the 2015 cyber-attacks against Ukrainian power grids, which can both potentially offer further indirect evidence for related studies.

[1] For example, the chief of Georgia's National Security Council Eka Tkeshelashvili (Shachtman, 2009), David J. Smith (2012: 1–2) from the Potomac Institute for Policy Studies, Khatuna Mshvidobadze (2011), a senior associate at the Georgian Foundation for Strategic and International Studies and the geopolitical intelligence

platform Stratfor (2008). An official statement published on Google's blog on 11 August 2008, as the blog was temporarily replacing the attacked website of the Georgian Ministry of Foreign Affairs, stated that *"a cyber warfare campaign by Russia is seriously disrupting many Georgian websites, including that of the Ministry of Foreign Affairs"* (MFA of Georgia 2008).

[2] *"Indirect or circumstantial evidence relies on an extrapolation to a conclusion of fact (such as fingerprints, DNA evidence, and so on). This is, of course, different from direct evidence. Direct evidence supports the truth of a proclamation without need for any additional evidence or interpretation"* (Cisco 2017).

[3] The importance of the attribution problem in international relations has recently been illustrated by initiatives of the international community to create organisations specifically dedicated to this issue. The Atlantic Council suggested the creation of the Multilateral Cyber Attribution and Adjudication Council (MCAAC) already in 2014 (Healey et al. 2014: 10–12). In 2017, Microsoft proposed the creation of the International Cyberattack Attribution Organization (Microsoft 2017). Finally, RAND suggested establishing the Global Cyber Attribution Consortium (Davis et al. 2017). The proposals for these three organisations differ in the expressed opinions on the inclusion of states or the organisations' enforcement role; yet, they all suggest an increasing interest in resolving the attribution problem.

[4] For more details on the theoretical and systematic reasons behind the application of the overall and effective control doctrines, see Cassese (2007).

[5] For a description of the tensions directly preceding the war see Iashvili and Yusin (2008) or Belov (2008).

[6] Previously, there were some minor operations in cyberspace which accompanied a conflict on the ground, and some occurred as far back as the 1990s. For example, Chechen separatists were using the Internet to spread anti-Russian propaganda during the first Chechen war in 1994. During the second Chechen war, the Kremlin was accused of hacking activities against Chechen websites. Moreover, cyber operations were conducted against NATO, US and UK computers during the Kosovo crisis in 1999. Or to give a current example, Israeli and Arab hackers launch cyber attacks against each other every time a political situation related to Israel and Palestine escalates nowadays (Tikk et al. 2008: 5).

[7] A denial of service attack is an operation where *"multiple compromised systems are used to target a single system causing a denial of service"* (Harrison Dinniss 2012: 294).

[8] The roots of the RBN can be traced back to the 1990s, though it experienced the greatest boom of its activities in the first half of the following decade. As a service provider for cyber crime, the RBN was considered to be a middleman for a wide range of malicious internet activities such as malware hosting, phishing, gambling or spamming. The RBN activities publicly vanished in the autumn of 2007; however, according to some suspicions, its network has still been operating secretly in recent years. For more details about the RBN activities in general see Bizeul (2007).

[9] Bumgarner and Borg (2009: 3) mention that there was only one such forum on which the written communication was not in Russian – in this case, it was in English. An interesting fact to consider in connection with this topic is that Russian is a minority, but officially unrecognised, language in Georgia.

Literature

- Asmus, Ronald (2010): *A Little War That Shook the World: Georgia, Russia, and the Future of the West*. New York: Palgrave Macmillan.
- Atwal, Maya (2009): Evaluating Nashi's Sustainability: Autonomy, Agency and Activism. *Europe-Asia Studies*, Vol. 61, No. 5, pp. 743–758, <https://doi.org/10.1080/09668130902904878>.
- Betz, David – Stevens, Tim (2011): *Cyber Space and the State: Towards a Strategy for Cyber-Power*. London: Routledge, <https://doi.org/10.1080/01402390.2013.825434>.
- Cassese, Antonio (2007): The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. *European Journal of International Law*, Vol. 18, No. 4, pp. 649–668, <https://doi.org/10.1093/ejil/chm034>.
- Davis, John S. II – Boudreaux, Benjamin – Welburn, Jonathan William – Aguirre, Jair – Ogletree, Cordaye – McGovern, Geoffrey – Chase, Michael S. (2017): *Stateless Attribution. Toward International Accountability in Cyberspace*. Santa Monica: RAND, <https://doi.org/10.7249/RR2081>.
- Deibert, Ronald – Rohozinski, Rafal – Crete-Nishihata, Masashi (2012): Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russian-Georgian War. *Security Dialogue*, Vol. 43, No. 3, pp. 3–24, <https://doi.org/10.1177/0967010611431079>.
- Giles, Keir (2011): 'Information Troops': A Russian Cyber Command? Tallinn: 3rd International Conference on Cyber Conflict, NATO CCD COE.
- Giles, Keir (2012): Russia's Public Stance on Cyberspace Issues. Tallinn: 4th International Conference on Cyber Conflict, NATO CCD COE.
- Harrison Dinniss, Heather (2012): *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, <https://doi.org/10.1017/CBO9780511894527>.
- Healey, Jason (2011): *Beyond Attribution: Seeking National Responsibility for Cyber-attacks*. Issue brief, Atlantic Council, Cyber Statecraft Initiative.
- Healey, Jason – Tothova Jordan, Klara – Mallery, John C. – Youd, Nathaniel V. (2014): *Confidence-Building Measures in Cyberspace*. Washington: Atlantic Council.

- Kadlecová, Lucie (2015): Russian-Speaking Cyber Crime: Reasons behind Its Success. *The European Review of Organised Crime*, Vol. 2, No. 2, pp. 104–121.
- Mačák, Kubo (2016): Decoding Article 8 of the International Law Commission's Article on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict & Security Law*, Vol. 21, No. 3, pp. 405–428, <https://doi.org/10.1093/jcsl/krw014>.
- Schaap, Arie (2009): Cyber Warfare Operations: Development and Use under International Law. *Air Force Law Review*, Vol. 64, pp. 121–174.
- Schmitt, Michael (ed., 2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, <https://doi.org/10.1017/9781316822524>.
- Shackelford, Scott – Richard, Andres (2010–2011): State Responsibility for Cyber-attacks: Competing Standards for a Growing Problem. *Georgetown Journal of International Law*, Vol. 42, No. 4, pp. 971–1016.
- Smith, David (2012): *Russian Cyber Operations*. Potomac Institute for Policy Studies, Cyber Center.
- Tsagourias, Nicholas (2016): Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts. *Journal of Conflict & Security Law*, Vol. 21, No. 3, pp. 455–474, <https://doi.org/10.1093/jcsl/krw020>.
- Tikk, Eneken – Kaska, Kadri – Rünnimeri, Kristel – Kert, Mari – Talihärm, Anna-Maria – Vihul, Liis (eds., 2008): *Cyber-attacks against Georgia: Legal Lessons Identified*. Tallinn: NATO CCDCOE.

Documents

- Alperovitch, Dmitri (2009): Fighting Russian Cybercrime Mobsters: Report from the Trenches. Presented at *Black Hat USA 2009*, <http://www.blackhat.com/presentations/bh-usa-09/ALPEROVITCH/BHUSA09-Alperovitch-RussCybercrime-PAPER.pdf>.
- Armin, Jart (2008a): Georgia Cyberwarfare – Attribution & Spam Botnets. *RBNExploit*, 8/2008, <http://rbnexploit.blogspot.co.uk/2008/08/rbn-georgia-cyberwarfare-attribution.html>.
- Armin, Jart (2008b): Georgia Cyberwarfare – Continuation…. *RBNExploit*, 8/2008, <http://rbnexploit.blogspot.co.uk/2008/08/rbn-georgia-cyberwarfare-continuation.html>.
- Belov, Pavel (2008): Russia Is Prepared to Protect Abkhazia and South Ossetia by Force of Arms. *The Current Digest of the Post-Soviet Press*, Vol. 60, No. 17–18, 20. and 27. 5. 2008, p. 6, originally published in *Kommersant*, 26. 4. 2008.
- Bizeul, David (2007): Russian Business Network Study. *Bizeul.org*, 20. 11. 2007, <http://www.bizeul.org/files/RBN_study.pdf>.
- Bumgarner, John – Borg, Scott (2009): Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008. *US Cyber Consequences Unit*, <http://registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.
- Carr, Jeffrey (2008): Russia/Georgia Cyber War – Findings and Analysis. *Project Grey Goose: Phase I Report*, 17. 10. 2008, <http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>.
- Carr, Jeffrey (2009): The Evolving State of Cyber Warfare. *Project Grey Goose: Phase II Report*, 20. 3. 2009, <http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report>.
- Carr, Jeffrey (2011): 7 Reasons Why China Isn't the Biggest Cyber Threat (And Who Is). *Jeffrey Carr's Blog*, 29. 6. 2011, <http://jeffreycarr.blogspot.co.uk/2011/06/7-reasons-why-china-isnt-worlds-biggest.html>.
- Cisco (2017): CCNA Cyber Ops SECOPS, Official Cert Guide. Indianapolis: Cisco Press.
- Council of Europe (2001): Convention on Cybercrime. Eur. T.S. No. 185.
- Danchev, Dancho (2008): Coordinated Russia vs Georgia Cyber-attack in Progress. *ZDNet*, 11. 8. 2008, <http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670>.
- Iashvili, Aleksandr – Yusin, Maksim (2008): Russia Will Protect Its Citizens. *The Current Digest of the Post-Soviet Press*, Vol. 60, No. 28, 5. 8. 2008, pp. 12–13, originally published in *Izvestia*, 14. 7. 2008.
- ICJ (1986): Nicaragua Judgment: Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. U.S.), ICJ 14.
- ICJ (2007): Genocide Case: Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia & Herzegovina v. Serbia & Montenegro), ICJ 108.
- ICTY (1999): Tadić Case: Prosecutor v. Tadić. No. IT-94-1.
- Krebs, Brian (2008): Report: Russian Hacker Forums Fueled Georgia Cyber-attacks. *The Washington Post*, 16. 10. 2008.
- Menn, Joseph (2008): Expert: Cyber-attacks on Georgia Websites Tied to Mob, Russian Government. *Los Angeles Times*, 13. 8. 2008.
- Microsoft (2017): An Attribution Organization to Strengthen Trust Online. Microsoft Policy Papers, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI>.
- Ministry of Foreign Affairs of Georgia (2008): Cyber-attacks Disable Georgian Websites, 11. 8. 2008, <http://georgiamfa.blogspot.co.uk/2008/08/cyber-attacks-disable-georgian-websites.html>.
- Mshvidobadze, Khatuna (2011): The Battlefield on Your Laptop. *Radio Free Europe*, 21. 3. 2011, <http://www.rferl.org/articleprintview/2345202.html>.
- Russian Federation (2011): *Concept of a Convention on International Information Security*, 28. 10. 2011, <http://rusemb.org.uk/policycontact/52>.
- Shachtman, Noah (2009): Top Georgian Official: Moscow Cyber-attacked Us – We Just Can't Prove It. *Wired*, 11. 3. 2009, <http://www.wired.com/dangerroom/2009/03/georgia-blames/>.

• Security Council of the Russian Federation (2000): Information Security Doctrine of the Russian Federation [Доктрина информационной безопасности Российской Федерации]. In Russian at <http://www.scrf.gov.ru/documents/6/5.html>, in English at <http://www.mid.ru/bdomp/ns-os-sndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument>.
• Stratfor (2008): Georgia, Russia: The Cyber-Warfare Angle, 12. 8. 2018, <http://www.stratfor.com/sample/analysis/georgia-russia-cyberwarfare-angle>.

Note
This work was supported by the Grant Agency of Charles University under grant number 250418. Part of the research was realized during the author's MA thesis research. The author would like to thank Dr Tomáš Weiss and Dr Tomáš Dopita for their invaluable comments and patience and the two anonymous reviewers for their reviews.