PROBLEM OF ATTRIBUTION OF CYBER-ATTACKS POLITICAL ASPECTS

Ivana Damnjanović, PhD[1]
Faculty of Political Science, University of Belgrade, Serbia

Purpose

The rapid rise of cyberspace and, more generally, information and communication technologies and their thorough penetration into daily life, is frequently framed in terms of "new technologies" and discussed in purely technical (or technological) terms. This is not necessarily the best or even sufficient theoretical framework for consideration of their workings. On the contrary, minority voices in both scholarship and popular culture were and are warning again and again, that all technologies are *political*, in their making as well as in their impact and consequences (see Damnjanović, 2015, 2018; MacKenzie & Wajcman, 1999; Street, 1992).

Cyberspace is increasingly becoming an indistinguishable part of most people's everyday experience. It is not surprising, then, that various malicious actors are also staking their claims in this domain, trying to subvert it for their own purposes. The number of cyber-attacks is steadily growing and has now reached 2,200 attacks per day, totaling 800,000 per year (James, 2022). Companies, states, and international organizations are at the same time increasing their efforts to make cyberspace a safer place, using both technical and social - including legal and political - instruments. One of the significant problems, when it comes to dealing with cyber-attacks, is how to determine who the perpetrators are and where they come from. This is due to some particular features of cyberspace, seen by some authors as tempting for those who wish to exploit it for illicit purposes. As Parish and Madahar (2016, p. 1) point out, "[u]nconstrained by borders or geography, cyberspace is omnipresent, it permeates most, if not all, civil and military sectors and is difficult, if not impossible, to regulate and impose national authority on. It is ethereal and complex offering a diversity of opportunities to do good as well as bad". Add the perceived anonymity and ambiguity of norms (Stalans & Donner, 2018, p. 36), or, similarly formulated, "conditions of unregulated interdependence, digital connectivity, and deterritorialisation" (Sandywell, 2010, p. 38), and the rise in various forms of misuse and malicious behavior in the cyberspace becomes, at the very least, expected.

To determine who is behind a particular instance of cyber-attack, or cyber-attack campaign, is a feat further complicated by conceptual confusion. The very definition of cyberspace is not at all undisputed: both administrative and academic definitions[2] abound but are frequently at odds with each other. Starodubtsev et al. (2020), for example, list no less than 23 different definitions of cyberspace. Furthermore, definitions of other key terms are also problematic - there is no consensus about "what constitutes an attack or what counts as critical infrastructure" (Edwards et al., 2017, p. 1). It is beyond doubt, however, that cyberspace has become a domain of political struggle, used by an array of political actors for distinctly political purposes. These aspects are especially pertinent in the discussion of the attribution of cyber-attacks, and yet, they were until recently virtually absent from the scholarly

1 ivana.damnjanovic@fpn.bg.ac.rs

2 Unlike academic definitions, developed by scholars, administrative definitions are produced by national or international institutions, in accordance to their mission and goals (for further discussion of the distinction between these two types of definitions, see Simeunović, 2009).

deliberation. This is why this paper aims to reconsider the problem of attribution of cyber-attacks, arguably one of the most important issues in cybersecurity, from the point of view of political science. The purpose is to show what political aspects are involved in cyber-attacks and in the process of attribution and why they are important, from both academic and practical points of view.

Design/Methods/Approach

Drawing from the notion developed by Rid and Buchanan (2015), that the process of attribution is *a techno-political problem*, this paper will, through three chapters, discuss political components in the context of the classification of cyber-attacks, political aspects of the attribution process as well as the politically meaningful relationship between attribution and possible retribution for cyber-attacks. Starting from qualitative analysis of recent scholarly literature as well as available data on politically motivated cyber-attacks, the author will then use methods of induction and deduction, analysis, and synthesis, to form the conclusions.

The issues related to the attribution of the cyber-attacks were, until recently, been studied mainly within the field of cybersecurity and restricted to purely technical processes. This is one of the factors that severely limit the public debate on the issue of cyber-attacks, a debate that is even more relevant for the general public when those cyber-attacks are political in their nature (Rid & Buchanan, 2018). The same highly technical language, when used in the process of documenting and presenting evidence for attribution, can sometimes also be an obstacle impeding the understanding of political actors, that is, those decision-makers who have the authority to act upon that evidence (Rid & Buchanan, 2015). Furthermore, academic research on cyber-attacks and their attribution is limited by the nature of sources - which are mostly in the intelligence community or in the private cybersecurity sector, thus unavailable to university-based researchers (Rid & Buchanan, 2018). The first issue that has to be dealt with, at least to some extent, is the conceptual framework.

Cyber-Attacks

There is already a significant body of literature on cyber-attacks, replete with definitions and classifications. Still, there is no consensus on the definition of a cyber-attack, and it is deemed to be "a conflicted term" (Happa & Fairclough, 2017, p. 170). There are several reasons for this. Firstly, other terms, such as cybercrime or hacking, are sometimes used as synonyms for cyber-attacks. While certainly similar, and sometimes overlapping, they do not necessarily denote the same phenomena (see, for example, Shamsi et al., 2016). Secondly, cyber-attacks are defined from a variety of standpoints and within several fields of academic inquiry - from cyber-security studies to legal studies and philosophy (see, for example, Happa & Fairclough, 2017; Hathaway et al., 2012; Zhuang et al., 2015). In addition to these academic definitions, there are numerous administrative definitions developed by institutions and organizations.[3] For the purposes of this paper, the broader and non-technical definition of cyber-attack seems to be the most fitting. Thus, the cyber-attack will be understood as any deliberate access to the computer system or network with malicious intent, in order to disrupt the integrity or authenticity of data.

3 Several definitions used by USA government are listed on the National Institute of Standards and Technology website: https://csrc.nist.gov/glossary/term/Cyber_Attack (Accessed on July 15, 2023).

Attribution

The global nature of cyberspace, the open architecture of the Internet, as well as the hypothetical anonymity it provides, are among the key reasons why determining who is behind a particular cyber-attack is complicated. The process of identification of perpetrators of cyber-attacks is usually called attribution. It is usually defined as "the allocation of a cyber-attack to a certain attacker or a group of attackers in a first step and the unveiling of the real-world identity of the attacker in a second step" (Saalbach, 2019, p. 279). The attribution of cyber-attacks is important, among other reasons, because it allows for improvements in the protection of the systems, understanding of the rationale behind attacks, as well as pre-empting attacks against similar targets (Shamsi et al., 2016). Attribution is also a necessary prerequisite for any legal action against the attackers.

There is an extensive body of literature dealing with technical aspects of the problem of attribution. Several models for the investigation of cyber-attacks are developed, the diamond model being the most prominent (for a detailed description of this model, see Caltagirone et al., 2013). The quantity and complexity of the tools used in the investigations of cyber-attacks are constantly increasing, and the use of AI for these purposes seems to be rapidly developing (Iqbal et al., 2020; Nunes et al., 2018). However, as will be shown in the next section of this paper, technical forensics is not the only important aspect of the attribution.

Findings

In line with the stated purpose of this paper, the main findings of the paper - the identification of political aspects of the attribution process and their consequences - will be presented in the following sections. In order to complement the existing body of literature on attribution, political aspects of cyber-attacks, political actors and political issues emerging in the attribution process, and the politically significant relationship between attribution of cyber-attacks and the response to it will be identified and explained. Interestingly enough, despite the predominantly technical nature of the scholarly discussion, concepts of both cyber-attacks and attribution are seen by some as inherently and distinctly political (Steffens, 2020; *What Is a Cyberattack?*, 2022).

Political Aspects of Cyber-Attacks

The ever-expanding array of cyber-attacks, characterized by their growing diversity and sophistication, has underscored the imperative, driven by both academic and practical considerations, for the development of more precise tools for classifying these attacks. This resulted in a growing literature providing detailed classifications and taxonomies (see, for example, Simmons et al., 2009; Uma & Padmavathi, 2013). The primary criteria for classification, nevertheless, predominantly stay consistent, encompassing the means or methods of attack, the targeted entities, the underlying motivations, and the involved actors. It is worth noting that each of these factors can incorporate significant political elements, albeit to varying degrees.

The least controversial among the criteria are the tools and methods used in the execution of cyber-attacks. Most of the malicious actors use the same types of tools, even though the sophistication of those tools can vary - from readily available to custom-made. At times, though, the inherent nature of the employed methods can offer clues about the potentially politically motivated actors behind their use.

For example, strong suspicions that the state actors - in this particular case, the United States and Israel - were behind the Stuxnet attacks that targeted the centrifuges used by Iranian nuclear facilities were precisely due to the nature of the malware used. Not only was it extremely sophisticated, exploiting four zero-day[4] vulnerabilities (Bilge & Dumitraş, 2012), but testing it required access to the same model of centrifuges - a feat hardly possible for non-state actors (Rid & Buchanan, 2015).

It is easier to see the political relevance of the chosen targets of cyber-attacks. Ever since the beginning of the Internet era, the states have recognized the need to protect their critical infrastructure from cyber-attacks. In one of the earliest works on the topic, Denning (2001) identifies some of the systems that could be targeted by terrorists through cyberspace, such as the electrical grid or telecommunications. Among other systems commonly listed as critical infrastructure are banking and financial sectors, oil and gas production and distribution, water processing facilities, transport, emergency services, and government agencies. Today, however, there seems to be a consensus among researchers that the nature of politically motivated cyber-attacks has changed. In the aftermath of the 9/11 attacks, terrorist use of cyber tools to wreak havoc on critical infrastructure was seen as the most serious threat. Now, states or state-sponsored groups are those who target other nations' political targets, which are not limited to critical infrastructure but include also institutions and intelligence, with computer network attacks (CNA) becoming "a preferred semi-covert action tool of the early 21st century" (Rid & Buchanan, 2018, p. 4).

Targeting infrastructure - as seen in the case of Stuxnet and the disruption of the electrical power grid in Ukraine in 2015 - can have serious consequences. But it is even more alarming that political institutions and actors are increasingly becoming the targets of cyber-attacks. Rid and Buchanan (2018) specifically mention actors and institutions related to elections, and civil society actors - particularly groups advocating for democracy and human rights. Another possible target is the infrastructure necessary for the election - databases of eligible voters, voting machines, tabulation of votes, etc. In the United States, for example, voting machines are especially vulnerable to hacking. Their security is for decades known to be notoriously bad (see, for example, Bannet et al., 2004), and the problems are further exacerbated by the fact that manufacturers use digital rights management (DRM) to prevent researchers from examining them and disclosing vulnerabilities they have found (see Giblin & Doctorow, 2022).[5] Attempts to influence public opinion in another country are now, especially if they are assisted or accompanied by hacking, also considered to be cyber-attacks on political targets. This was the case with the campaign attributed to Russian intelligence agencies, groups, and individuals during the 2016 US elections. The way Rid and Buchanan (2018, pp. 8–9) use it as an example illuminates not only the fact that the American cybersecurity sector and at least part of the government certainly saw these events as an attack, but also several other important political aspects of the attribution process and outcomes, which will be further elaborated on in the next section of the paper:

"…the 2016 influence operations were poorly disguised, perhaps even semi-overt by design. Not only was it obvious that a hacking-aided influence campaign was going on, but it was reasonably apparent which foreign power was conducting it. As early as mid-June 2016, a range of outside experts squarely placed the blame of the budding leaking operation on Russia, following the initial hacking attribution of the cybersecurity firm CrowdStrike. Politically there may have been partisan incentives to call the evidence into question. Technically and historically, however, the evidence of a Russian hand was inescapable early on."

4 Zero-day vulnerabilities are previously unknown (and therefore unpatched) vulnerabilities in software.

5 The issue here is that article 1201 of the US Digital Millennium Copyright Act (DMCA) passed in 1998 prohibits circumvention of technological measures that effectively control access to a work protected by copyright (such as DRM) for *any* reason, including research.

Classification of a cyber-attack as political based on the motivation of its perpetrators appears to be tautological. The motivation can be obvious from the intended targets of the attack, or self-proclaimed by the perpetrators. The latter is frequently the case when the attacks consist of spamming or website defacing when individuals or groups involved usually state their goals and political positions. This was the case in one of the first uses of cyberspace by terrorist groups - the spamming campaign of Tamil Tigers in 1998 (Denning, 2001) and "cyberwars" between hacking crews from different countries.[6] Sometimes even within more sophisticated attacks, such as the Iranian attack on Saudi Arabian oil company Aramco, perpetrators leave messages on the infected computers or within code stating their political reasons for the attack (Buchanan, 2020).

Another possible way to determine the motivation for the cyber-attack is to identify the actors responsible for it. If it turns out to be a state agency or group known for its political activities, the motivation is probably political. On the other hand, in cases where perpetrators are identified as "hackers for hire," their motivation is harder to determine. In the words of Rid and Buchanan (Rid & Buchanan, 2015, p. 11), "[i]dentifying a monetary incentive is easier than examining a political incentive". The identification of actors is definitely the most certain way to determine if the specific cyber-attack or campaign is politically motivated.

There are several categories of actors who are interested in carrying out political cyber-attacks. First among them are, obviously, the states or, more specifically, their intelligence agencies or specialized military units. As it was already pointed out, the overt, covert, or semi-overt operations in cyberspace seem to be the new foreign-policy toolkit wholeheartedly embraced by great and regional powers alike. Great powers especially, Buchanan (2020) argues, are using cyber capabilities to shape the global political environment in line with their interests. This is generally done using specialized units or departments of military and intelligence organizations or proxies - more or less independent groups or hacking crews.

The United States was probably the first state to recognize the need for organizational adjustments in the age of the Internet. The formation of units for different tasks in cyberspace started already in the last years of the 20th century. After the recognition of cyberspace as one of the domains of conflict in 2004 National Military Strategy,[7] this process gained momentum, and culminated in the establishment of U.S. Cyber Command in 2009. The United States, according to most researchers[8], is at the moment in the lead regarding both offensive and defensive cyber capabilities. This stems, at least in part, from the "home advantage" provided by the fact that not only important parts of the Internet infrastructure but also most of the major global Internet platforms and companies are based in the United States. In recent years, however, this advantage may be shrinking (Buchanan, 2020).

Direct involvement of the states opens a certain set of issues in the attribution process, which will be addressed in the next chapter. The use of proxies, however, sets a completely different array of problems. The main motivation for states to use independent "contractors" for cyber operations is precisely to impede the attribution, that is, to establish plausible deniability (Steffens, 2020). Cyber proxies can be defined "as intermediaries that conduct or directly contribute to an offensive cyber action that is enabled knowingly, whether actively or passively, by a beneficiary" (Maurer, 2018, p.

6 Some of the examples include clashes between Israeli and Palestinian hackers, Indian and Pakistani crews, as well as several waves of "local" conflicts in cyberspace involving Serbian, Croatian and Albanian hackers.

7 The full text of the unclassified version of the Strategy is available at https://nssarchive.us/wp-content/uploads/library/nms/nms2004

8 This assessment should, however, be taken with the grain of salt for two reasons: 1) most of the scholarly research on these issues is published by Western scholars and in the Western academic journals, and 2) most of the attribution reports published by private cybersecurity companies also come from those enterprises that are either based in the West or are working mostly for Western clients (see, for example, Steffens, 2020).

xi). Not all proxy organizations, however, have identical relationships with the state employing them. Maurer (2018) identifies three different types of proxy relationships - delegation, orchestration, and sanctioning. Proxies who are in the first type of the relationship - delegation - are under the effective control of the state. Orchestration, according to Maurer, applies to those organizations that are funded by the state and provided with tools, and that share the state's ideology. Finally, sanctioning refers to the situation where "a state is aware of the activity of a non-state actor but turns a blind eye towards it and indirectly benefits from its actions" (Maurer, 2018, p. xii). Sanctioning seems to be very close to the concept of "patriotic hacking", described by Dahan (2013, p. 54) as " actions by private citizens of a country acting on their own initiative against a perceived threat by an enemy of the state or attacking countries involved in a conflict with their own."

There are also non-state actors who may use cyber-attacks in order to achieve political goals. Two groups have especially captured the attention of researchers - terrorists and hacktivists. While the use of the Internet by terrorist organizations is not only acknowledged but very well documented in scholarly literature, they generally do not seem to use cyberspace offensively (Damnjanović, 2009; Denning, 2010, 2001; Weimann, 2006, 2016). After the early spamming campaigns, occasional website defacing or DDoS attacks seem to be the extent of their efforts. Terrorist organizations have since realized that propaganda and recruiting are, for them, the most effective uses of cyberspace (see Liu, 2015).

Hacktivism is seen as different from patriotic hacking mostly by its ideology (Dahan, 2013), but this distinction tends to blur lately (Romagna, 2020). While usually associated with a distinct set of ideas about freedom of information and human rights, hacktivist groups (and occasionally "lone wolf" hacktivists) sometimes hold very specific political views and use cyberspace to present and promote them. Some hacktivist groups have achieved high visibility and caught the attention of the general public, political decision-makers, and academic researchers. Among them are collectives such as the *Cult of the Dead Cow*[9], *Electronic Disturbance Theater,* and the *Anonymous* (Coleman, 2001; Jordan & Taylor, 2004).

Attribution: Politics and Policy

In cybersecurity circles, there is a widely held belief that attribution is meaningless and unimportant - because the defenses built into the computer system should be designed in such a way that they are able to withstand any attack - no matter who is behind it and for what motives. While this is true in principle, in the real world there is scarcely an organization that can afford to implement all recommended security measures (Steffens, 2020). From the very definition used in the first chapter of this paper, it is obvious that the attribution is, essentially, a two-step process. These steps are described in different ways, but most authors agree that there is a difference between the attribution of the attack to the specific *machine* - host computer, server, or network from which the attack is launched, and the attribution of the attack to specific *persons* - groups and/or individuals performing the attack as well as their instigators. Boebert (2010) distinguishes these steps as different types of attribution techniques - technical attribution and human attribution, but seems more useful to see them as different phases of the attribution process (Clark & Landau, 2011).

The process itself is complex and multilayered. Shamsi et al. (2016, p. 3) describe it as an "ongoing interplay" between the types and level of attribution, the nature of the cybercrime, the desired level of attribution, and the level of proof that is required. They believe that in order to be complete, attribu-

9 This organization was, in a rather bizarre development, even mentioned during the trial of Slobodan Milošević in Hague (see "Hacktivism and How It Got Here," 2004).

tion must identify the cyberweapon, that is, the tool used for the attack, the location (country or city) of the attackers, and individuals or organizations behind the attack. The quality of attribution is, in the view of Rid and Buchanan, (2015) a function of available resources, available time, and the adversary's sophistication.

There is no dispute that the attribution is in its essence, at least on the operational level, a technical process. Cyber forensics is a highly specialized field, and, generally, only governments and cybersecurity companies are capable of effective attribution (Steffens, 2020). While it does seem that government agencies, at least in some countries of the West, do have superior capabilities, some of the biggest attacks, such as the long-lasting Chinese campaign against the USA and Stuxnet attacks were actually attributed by cybersecurity companies (Buchanan, 2020; Rid & Buchanan, 2018). Yet, in order for complete attribution to be provided, many other actors have to be involved, contributing to the political nature of the process. These include government agencies, political leaders, civil society, the cybersecurity industry, executives in other industries, researchers and scholars from different fields, as well as journalists (Rid & Buchanan, 2015; Shamsi et al., 2016). This, by itself, lends credence to the characterization of attribution as a techno-political problem.

One important area where policy-makers have a significant impact is resource allocation. Attribution is resource resource-intensive endeavor, in terms of hardware, software, and expertise available. How these resources are to be used and allocated depends on several circumstances. One of the most important is the character of the attack, its targets, and the financial, physical, or reputational damage it inflicts (Rid & Buchanan, 2015).

The main obstacle that investigators have to overcome is anonymity as one of the inherent features of the Internet. Ever since the 1990s, when the Internet became available to the general public, the possibility to use it anonymously was one of its most enticing features. In recent decades, however, this promise of anonymity is not only forgotten but also actively undermined, for example by "real name policies" more or less successfully imposed by platforms such as Facebook and Google. Nevertheless, anonymity is baked into the very architecture of the Internet (Shamsi et al., 2016). That can still change in the future. The United States seems to be intent on using its aforementioned "home advantage" "to reengineer the Internet to make attribution, geolocation, intelligence analysis, and impact assessment—who did it, from where, why and what was the result—more manageable" (McConnell, 2010, according to Clark & Landau, 2011, p. 323).

Identification of perpetrators of cyber-attacks as an element of successful attribution can be difficult for various technical reasons. The attackers are using different methods for systematically hiding their identities, and their success depends both on their skills and the resources at their disposal. This aspect of attribution, as already mentioned, can lead to different levels of identification. It can point to the country from where the attack was launched, to the group or organization behind it, or, even, to the specific individuals responsible. The decision of which level of attribution is desirable, especially in the cases of politically motivated attack, is also political in its nature.

In some cases, such as cyber-espionage, it is commonly assumed that the states are ultimately behind them (Steffens, 2020), and the identification of the engaged individuals is not a priority, especially if government intelligence agencies and/or military units are confirmed as perpetrators of the attack. Sometimes, however, the prior identification of individuals is necessary in order to identify the organization that they belong to (Rid & Buchanan, 2015). Also, as Steffens (2020) points out, it is extremely satisfying for the public to know the names and sometimes even faces of the persons responsible for the attack, and on the intuitive level, the responsibility of the actors becomes more palpable when we real individuals can be pinpointed. A particularly relevant challenge in the process of attribution is

how to establish the relationship between individuals, organizations, and states beyond reasonable doubt. Even when the point of origin of the attack is confirmed to be, for example, a military facility, that does not necessarily prove that the operation was sanctioned by the state (Edwards et al., 2017). The situation is even more complicated when states are using proxies in order to conceal its involvement.[10] It seems, however, that "governments are increasingly willing to hold other states accountable for cyber intrusions by hackers and proxy organizations" (Lee, 2023, p. 200).

Another important political aspect of attribution lies in the fact that, so far, the states seem to have unsurpassed attribution capabilities. Although one of the most important breakthroughs and the event that, most scholars agree, brought attribution to the spotlight and introduced it to the public debate, was the publication of the APT1[11] report by cybersecurity company Mandiant, and Stuxnet, probably the most publicized attack, was first discovered by a small Belarusian antivirus company, states have resources at their disposal that are not available to private entities. These resources are, mostly, concentrated within intelligence agencies, and are not necessarily technical. Quite the opposite, the intelligence available to the states and its analysts are the key advantages in attribution, especially in the case of involvement of other states. Frequently, the process begins with the *cui bono* questions, which cannot be answered without a thorough knowledge of geopolitics and current political affairs (Steffens, 2020).

From Attribution to Retribution

Correct attribution is necessary primarily in order to initiate an appropriate response, which is usually aimed toward either deterrence or punishment (Shamsi et al., 2016). Incorrect attribution can have severe consequences (Shamsi et al., 2016), and in some cases, as Rid and Buchanan (2015, p. 4) point out, "[d]ecisions of life and death depend on attribution". Clark and Landau (2011, p. 323, italics in the original) put it even more succinctly: "Attribution is central to deterrence, the idea that one can dissuade attackers from acting through fear of some sort of retaliation. *Retaliation requires knowing with full certainty who the attackers are*".

The United States has already declared its right to retaliate for the cyber-attack back in 2011 (*International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 2011, pp. 13–14), especially underlying that those attacks that have offline effect may be sufficient grounds for self-defense. Tsagourias (2012) also emphasizes that self-defense is in line with international law only if cyber-attack qualifies as an armed attack. That, however, does not prevent states from retaliating in other ways. Yet, at this moment, it seems that governments are quite reluctant to respond to cyber-attacks in kind. One significant, although somewhat confusing, exception is the Iranian retaliation for the Stuxnet attack. Even though the attack was attributed by cybersecurity experts to the United States and Israel with a significant degree of certainty, Iranian hackers retaliated by launching devastating cyber-attacks against Saudi state-owned oil company Aramco (Buchanan, 2020). Even milder responses, such as public and official statements about attribution, or legal action against individuals or organizations involved, are still rare, although their frequency seems to be increasing in the last decade. The turning point, at least for the United States, was the Russian interference in the 2016 election.

10 It is important to note that plausible deniability is not the only reason the states use proxies for cyber-attacks. Stephens (2020, p. 102) mentions "lack of skills on the government side, temporary demand for additional personnel, or paying higher salaries than rigid government pay schemes allow".

11 APT stands for Advanced Persistent Threats and is lately sometimes used as a synonym for cyber-espionage (see Steffens, 2020). Mandiant's APT1 report was published in February 2013 and detailed Chinese cyber-attacks on American networks. The company has since published reports on 41 groups associated with different countries. Summaries available at: https://www.mandiant.com/resources/insights/apt-groups

Since then, there have been several indictments against individuals identified as involved in the cyber-attacks against US targets. Legal action is, though, not always possible, since the standard for proof in the legal process is, as a rule, higher than for other types of response based on attribution. The public statements by elected officials and public servants attributing the attacks have also become more common, and are used as means of diplomatic pressure and possible deterrence.[12] The effectiveness of these actions seems to depend on a number of factors, including the level of direct involvement by the state and the type of the political regime, with democracies being more likely to cease cyber-operations when exposed, due to concerns about their public image and public opinion both within the country and internationally (see, for example, Steffens, 2020). Whatever the chosen course of action may be, the decision whether to retaliate, indict, publicly disclose attribution and evidence for it, or abstain from acting is in the hands of the political actors.

Originality/Value

While certain political aspects of the process of attribution of cyber-attacks have been considered in recent academic works, there seems to be no research focusing exclusively on this subject, nor starting from the point of view of political science. Therefore, the originality of the proposed paper is both in its scope and its approach. Apart from scientific contribution, the value of the paper consists in the production of tentative guidelines for state agencies tasked with dealing with the aftermath of cyber-attacks.

The key political aspects of cyber-attacks are identified - methods, targets, actors and motivations, as well as the most important political aspects of attribution.

The Republic of Serbia has already been targeted by politically motivated cyber-attacks in the recent past. In the early 2000s, there were several "hacking wars" involving Croatian and Albanian hacking crews, mostly interested in taking down or defacing commercial and public websites. Later, in 2012, cyberspace became an arena for internal political struggle, with the website defacing campaigns of a person (or persons) under the handle of John the Ripper and attacks on several high-profile institutional websites. More recently, the computer systems of the Republic Geodetic Authority were attacked and their operation was interrupted. Various media portals are frequently reporting being under distributed denial of service (DDoS) attacks. Therefore, findings presented in previous sections of this paper could be, at least, a useful reminder that building and improving attribution capabilities should be among the priorities of the corresponding government agencies. Furthermore, the experiences of other countries and the ways they used attribution and response to cyber-attacks in their internal and international politics can provide valuable lessons and guidelines for future decision-making in similar cases.

References

Bannet, J., Price, D. W., Rudys, A., Singer, J., & Wallach, D. S. (2004). Hack-a-vote: Security issues with electronic voting systems. *IEEE Security & Privacy*, *2*(1), 32–37. DOI: 10.1109/MSECP.2004.1264851

Bilge, L., & Dumitraş, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. *Proceedings of the 2012 ACM conference on Computer and communications security*. 833–844. DOI: 10.1145/2382196.2382284

12 Even before 2016, president Obama used evidence against Chinese groups as diplomatic leverage, but there were no public statements attributing the cyber-attacks.

Boebert, W. E. (2010). A survey of challenges in attribution. *Proceedings of a workshop on Deterring Cyber Attacks*. 41–54.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard: Harvard University Press.

Caltagirone, S., Pendergast, A., & Betz, C. (2013). The diamond model of intrusion analysis. *Threat Connect*, *298*(0704), 1–61.

Clark, D. D., & Landau, S. (2011). Untangling attribution. *Harvard National Security Journal*, *2*, 323.

Coleman, S. (2001). The transformation of citizenship. In B. Axford & R. Huggins (Eds.), *New media and politics* (pp. 109–126). London: Sage.

Dahan, M. (2013). Hacking for the homeland: Patriotic hackers versus hacktivists. *Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013,* 51–57.

Damnjanović, I. (2009). Postoji li sajberterorizam? *Politička revija*, *8*(1), 237–253. DOI: 10.22182/pr.1912009.13

Damnjanović, I. (2015). Polity Without Politics? Artificial Intelligence Versus Democracy: Lessons From Neal Asher's Polity Universe. *Bulletin of Science, Technology & Society*, *35*(3–4), 76–83. DOI: 10.1177/0270467615623877

Damnjanović, I. (2018). *Politika i tehnologija: teorijski pristupi*. Beograd: Udruženje Nauka i društvo.

Denning, D. E. (2010). Terror's web: How the Internet is transforming terrorism. In: Y. Jewkes & M. Yar (Eds.), *Handbook of Internet Crime* (pp. 194–213). London: Routledge.

Denning, D. E. (2001, November 1). Is Cyber Terror Next? *Items,* http://essays.ssrc.org/sept11/essays/denning.htm

Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences*, *114*(11), 2825–2830. DOI: 10.1073/pnas.1700442114

Giblin, R., & Doctorow, C. (2022). *Chokepoint Capitalism: How Big Tech and Big Content Captured Creative Labor Markets and How We'll Win Them Back*. Boston: Beacon Press.

Delio, M. Hacktivism and How It Got Here. (2004, July 14). *Wired*. https://www.wired.com/2004/07/hacktivism-and-how-it-got-here/

Happa, J., & Fairclough, G. (2017). A Model to Facilitate Discussions About Cyber Attacks. In M. Taddeo & L. Glorioso (Eds.), *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative* (pp. 169–185). Cham: Springer International Publishing. DOI: 10.1007/978-3-319-45300-2_10

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 817–885.

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. (2011). The White House. https://nsarchive.gwu.edu/document/20843-04

Iqbal, F., Debbabi, M., & Fung, B. C. M. (2020). *Machine Learning for Authorship Attribution and Cyber Forensics*. Cham: Springer International Publishing. DOI: 10.1007/978-3-030-61675-5

James, N. (2022, December 19). *160 Cybersecurity Statistics: Updated Report 2023*. https://www.getastra.com/blog/security-audit/cyber-security-statistics/

Jordan, T., & Taylor, P. (2004). *Hacktivism and Cyberwars: Rebels with a Cause?* (1st edition). London: Routledge.

Lee, H. (2023). Public attribution in the US government: Implications for diplomacy and norms in cyberspace. *Policy Design and Practice*, *6*(2), 198–216. DOI: 10.1080/25741292.2023.2199964

Liu, E. (2015). Al Qaeda Electronic: A Sleeping Dog. *A Report by the Critical Threats Project of the American Enterprise Institute*, 4–7. https://www.criticalthreats.org/analysis/al-qaeda-electronic-a-sleeping-dog

MacKenzie, D., & Wajcman, J. (1999). Introductory essay: The social shaping of technology. In D. MacKenzie & J. Wajcman, *The Social Shaping of Technology* (2nd ed., pp. 3–28). Maidenhead: Open University Press/McGraw-Hill.

Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press. DOI: 10.1017/9781316422724

Nunes, E., Shakarian, P., Simari, G. I., & Ruef, A. (2018). *Artificial Intelligence Tools for Cyber Attribution*. Cham: Springer International Publishing. DOI: 10.1007/978-3-319-73788-1

Parish, M., & Madahar, B. (2016). *Understanding Cyberspace Through Cyber Situational Awareness*. Defence Science and Technology Laboratory Cyber and Information Systems Division.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. DOI: 10.1080/01402390.2014.977382

Rid, T., & Buchanan, B. (2018). Hacking democracy. *SAIS Review of International Affairs*, *38* (1), 3–16.

Romagna, M. (2020). Hacktivism: Conceptualization, techniques, and historical view. In: T.J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 743–769.

Saalbach, K.-P. (2019). Attribution of Cyber Attacks. In: C. Reuter (Ed.), *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace* (pp. 279–303). Springer Fachmedien Wiesbaden. DOI: 10.1007/978-3-658-25652-4_13

Sandywell, B. (2010). On the globalisation of crime: The Internet and new criminality. Y. Jewkes & M. Yar (Eds.), *Handbook of Internet Crime*, 38–66. London: Routledge.

Shamsi, J. A., Zeadally, S., Sheikh, F., & Flowers, A. (2016). Attribution in cyberspace: Techniques and legal implications. *Security and Communication Networks*, *9*(15), 2886–2900. DOI: 10.1002/sec.1485

Simeunović, D. (2009). *Terorizam—Opšti deo*. Beograd: Pravni fakultet Univerziteta u Beogradu.

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2009). AVOIDIT: A cyber attack taxonomy. *University of Memphis, Technical Report CS-09-003*.

Stalans, L. J., & Donner, C. M. (2018). Explaining Why Cybercrime Occurs: Criminological and Psychological Theories. In: H. Jahankhani (Ed.), *Cyber Criminology* (pp. 25–45). Springer International Publishing. DOI: 10.1007/978-3-319-97181-0_2

Starodubtsev, Yu. I., Balenko, E. G., Vershennik, E. V., & Fedorov, V. H. (2020). Cyberspace: Terminology, Properties, Problems of Operation. *2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, 1–3. DOI: 10.1109/FarEastCon50210.2020.9271282

Steffens, T. (2020). *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage*. Cham: Springer. DOI:10.1007/978-3-662-61313-9

Street, J. (1992). *Politics & Technology*. New York: The Guilford Press.

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, *17*(2), 229–244. DOI: 10.1093/jcsl/krs019

Uma, M., & Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *International Journal of Network Security*, *15*(5), 390–396.

Weimann, G. (2006). *Terror on the Internet: The new arena, the new challenges*. Washington: US Institute of Peace Press.

Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism*, *39*(3), 195–206. DOI: 10.1080/1057610X.2015.1119546

What is a cyberattack? (2022, February 18). | Chatham House – International Affairs Think Tank. https://www.chathamhouse.org/2022/02/what-cyber-attack

Zhuang, R., Bardas, A. G., DeLoach, S. A., & Ou, X. (2015). A theory of cyber attacks: A step towards analyzing MTD systems. Proceedings of the second ACM workshop on moving target defense. 11–20. DOI: 10.1145/2808475.2808478