SERBIA

Digital Threat Landscape: Civil Society & Media

Internews
Local voices. Global change.

SHARE FOUNDATION

Table of Contents

Background

Under the current regime, Serbia has experienced democratic backsliding that impacts the ability of independent media to operate without interference and puts increasing pressure on civil society. This backsliding has led to increased risk of digital threats to Serbian civil society and media. This report was prepared by Internews' Internet Freedom & Resilience team under a stream of work which strengthens civil society organizations (CSOs), journalists, and other human rights defenders (HRD) ability to detect, analyze, and build resilience to digital attacks through localized expertise in threat analysis and incident response. This report is intended to provide an overview of the threats faced by civil society and media organizations in Serbia and guidance for digital safety experts supporting this community. It is also intended to provide context for the cybersecurity industry which may need to analyze security incidents affecting Serbian civil society and media. We conclude with a discussion of mitigation measures that digital security experts can propose to the organizations with whom they work, as well as for civil society and media organizations to implement.

This report was written in close collaboration with the SHARE Foundation, a Serbia-based non-profit organization established in 2012 to advance human rights and freedoms online and promote positive values of an open and decentralized internet, as well as free access to information, knowledge, and technology. SHARE Foundation's primary areas of activities are freedom of expression online, data privacy, digital security, and open access to knowledge.

The threats, trends, and case studies highlighted in this report were identified through direct digital safety support for at-risk communities (provided by Internews and SHARE Foundation), desk research, and conversations with trusted members of the Internet Freedom community. This report aggregates data from incident response work and documents attack patterns specific to Serbia.

October 2023

Written and Edited: Martijn Grooten, Ashley Fowler, Marc Shaffer, and Skyler Sallick
Copyediting, Design, and Layout: Skyler Sallick

Digital Threat Landscape

Political Context, Civil Society, and the Media

Under the current president, Aleksandar Vučić, Serbia has experienced democratic backsliding and increased accusations of human rights and freedom of the press violations. Freedom House ranks Serbia as "partly free", with a score of 60 out of 100,[1] marking a continued downward trend.[i,2] Serbia is involved in a significant regional dispute over Kosovo, which unilaterally declared independence in 2008. Kosovo is recognized as a sovereign state by 101 members of the United Nations, but Serbia maintains that the Autonomous Province of Kosovo and Metohija is Serbian territory. The dispute with Kosovo continues to be one of the defining issues in Serbian politics with occasional flare ups of violence, most recently in mid-2023.[3]

Under Vučić, civil society and independent media organizations have come under increased pressure. Journalists whose reporting goes against the official government line face frequent strategic lawsuits against public participation (SLAPP), including accusations of links to organized crime.[4] In general, domestic and international non-governmental organizations can operate freely, but those that are too openly critical of the government face harassment and threats.[5]

When compared to the rest of the region, a significant number of pro-regime tabloids publish hate speech against independent journalists, often running their pictures alongside accusations that they are enemies of the state. Due to increased government pressure, the market for independent media is shrinking. As a result, media outlets are required to look for donors to sustain their operations.

Under Vučić, civil society and independent media organizations have come under increased pressure. Journalists whose reporting goes against the official government line face frequent strategic lawsuits against public participation (SLAPP), including accusations of links to organized crime.

According to the International Federation of Journalists, Serbia is among the most dangerous countries for journalists in Europe. Physical attacks on journalists remain common, and while ongoing attempts to improve the situation have had some success, the hostile environment created by the government undermines the work being done by independent journalists.[6]

Cybersecurity in Serbia

Cyberattacks are a growing concern in Serbia. Although Serbia is party to the Budapest Convention[ii,7] and has a framework to combat cybercrime, the issue remains prevalent due to

[i] Freedom House last categorized Serbia as "free" in 2018 with a score of 73 out of 100, [2].

[ii] Serbia is a party to the Budapest Convention, "a framework that permits hundreds of practitioners from Parties to share experience and create relationships that facilitate cooperation in specific cases, including in emergency situations, beyond the specific provisions foreseen in this Convention." [7]

staffing shortages in relevant governmental departments and a general lack of awareness among the broader population.[8]

Financially motivated cybercrimes have been used to target private entities and the state itself. Serbia was the main target of an advanced, financially motivated campaign uncovered by security company ESET in 2019.[9] At the beginning of the COVID-19 pandemic, a public utility company in Serbia's second largest city, Novi Sad, was hit with ransomware. Luckily, a bug was found in the encryption mechanism which enabled the recovery of 50TB of encrypted data without ransom payment.[10] For more information about this incident, please see this report, available in Serbian, published by SHARE Foundation.[11]

Relatively little is known about the state-sponsored malware targeting Serbia. However, in 2021, PwC uncovered a campaign that targeted government and military institutions in Serbia and the Republika Srbska[iii] region of Bosnia and Herzegovina.[12] PwC refers to the actor behind this campaign as 'White Tur' and remains unable to link these cybercriminals to a specific country. In 2023, the Serbian Ministry of Internal Affairs was the target of several distributed denial-of-service (DDoS) attacks linked to regional tensions, including violent clashes between ethnic Serbs in northern Kosovo and ethnic Albanian authorities.[13]

Serbia is also home to cybercriminals that operate out of the country. In 2017, it was revealed that a Serbian ultranationalist developer was behind the relatively obscure "SerbRansom" ransomware.[14] In 2018, a Serbian man was arrested on suspicion of affiliation with the Dark Overlord hacking crew, one of the most active online criminal groups at the time.[15] In 2022, a Serbian-Hungarian dual citizen pled guilty to a business email compromise (BEC) scheme that scammed victims out of $3.7m in total.[16]

The State of Cybersecurity of Civil Society and Media

Cyberattacks perpetuated in Serbia also target civil society organizations and the media landscape. While these attacks are also often financially motivated, there is evidence of suppressive pro-government activity, such as bot attacks orchestrated by pro-regime accounts, intended to disrupt the ability of these communities to carry out their work.

Balkan Investigative Reporting Network (BIRN) and SHARE Foundation verified 190 cases of digital rights violations between August 2019 and November 2020, most commonly in the form of "pressures because of expression and activities on the internet."[17] In terms of digital rights violations, the most common targets include citizens, journalists, online media, public persons, state officials, and activists.[18] An example of the types of attacks faced by journalists and civil society organizations can be found in the Case Study section of this report.

Media outlets and civil society organizations are commonly affected by digital threats—even if most of the attacks do not target them directly. Women face greater threat of digital attacks, often of a more personal nature with focus on gender.[19] An example of the types of attacks faced by female journalists can be found in the Case Study section of this report. For many civil society and

[iii] The Republika Srbska region of Bosnia and Herzegovina has a majority Serb population.

media organizations, the precarious nature of their funding prevents the use of digital security measures necessary to protect against surveillance and other targeting.

In recent years, tech companies have taken measures to combat pro-government accounts targeting opposition activity online. In 2020, Twitter removed 8,500 pro- Vučić accounts and more than 43 million tweets.[20] In 2023, Meta reported that it had acted against a "Coordinated Inauthentic Behavior" (CIB) network in Serbia with links to the ruling Serbian Progressive Party.[21] This campaign aimed to create the impression of widespread support for the Progressive Party and for President Vučić. Also in 2023, the Organized Crime and Corruption Reporting Project (OCCRP) uncovered a targeted disinformation campaign that involved the use of an Israeli "disinformation group" and attempted to smear one of Vučić's political rivals. [22]

For many civil society and media organizations, the precarious nature of their funding prevents the use of digital security measures necessary to protect against surveillance and other targeting.

Serbia's Security Information Agency purchased the Finfisher spyware and has negotiated the purchase of Hacking Team spyware.[23] It is unclear whether the Security Information Agency has used either spyware or whom they may target. Both types of spyware have been used to target members of civil society and journalists in other countries.

The Security Information Agency is also a known customer of the Circles mobile surveillance firm whose products can be used to intercept phone calls and SMS numbers.[24] Such software can be used to target WhatsApp or Signal accounts that do not have passcodes for extra protection.

Researchers at Citizen Lab identified Serbia as a likely customer of the Predator spyware, developed by the North Macedonia-based company Cytrox.[25] This was later confirmed by Google.[26] Here too it is unclear who the targets were, but the government spread the Predator infections using two domains impersonating Serbian media outlets. The use of Serbian media sites suggests at least some of the targets are based in the country itself, as they would likely use domains in other languages for foreign targets.

In order to protect their ability to operate effectively, action needs to be taken at both the individual and societal level. Digital security trainers can help protect these vulnerable organizations by assisting in implementing the following mitigation tactics.

The security of civil society organizations and the media is under threat in Serbia. In order to protect their ability to operate effectively, action needs to be taken at both the individual and societal level. Digital security trainers can help protect these vulnerable organizations by assisting in implementing the following mitigation tactics.

Mitigation Measures

Account security is important for anyone in Serbia, but crucial for members of civil society. **Two-factor authentication is a must** – and mitigates the use of weak and/or reused passwords. Organizations cannot control their employees' passwords, so enabling two-factor authentication mitigates the risk of employee use of weak passwords. Though better than no two-factor authentication at all, SMS shouldn't be considered secure, especially for at-risk users. Using an authentication app is better than SMS, and using a hardware token generally provides the best security, although this requires additional equipment.

For accounts linked to a phone number on platforms such as Telegram, WhatsApp, and Signal, two-factor authentication involves **adding a passcode to the account** in addition to linking SMS being used to link an account to a phone number. When this feature is enabled, the app will periodically ask the user to input their passcode to ensure the messages are not being accessed by someone besides the owner of the account. This prevents account takeover through SMS interception, either through social engineering or the use of services like Circles.

Endpoints, such as laptops and mobile phones, should be kept up to date by applying security patches to operating systems and other software whenever they become available. **Software should only be acquired from official sources**. In many cases, this requires payment. NGOs should not be shy to discuss this with funders, or to look for free alternatives such as open-source software and programs that provide software free of cost or at reduced prices to eligible NGOs.

While it is unknown whether civil society in Serbia has been targeted by advanced spyware such as Predator, those considered high-value targets should understand that such spyware commonly uses zero-day vulnerabilities and zero-click infections. This kind of advanced spyware can infect a completely patched device without clicking a link or opening an attachment. As users cannot prevent this kind of infection, those at risk of such spyware should keep this in mind.

Potential targets are urged to **use disappearing messages** on messaging apps where messages automatically delete after a fixed amount of time as this can limit the damage of account compromise. Compartmentalization such as the **use of separate devices for work and personal use**, or even a **separate device for high-risk work**, also limits potential damage but comes with extra costs and inconveniences.

In addition to keeping phones up to date, **regularly rebooting iPhones** – ideally once a day – and **using Apple's Lockdown Mode** also mitigates the likelihood of attacks, as attacks will be likely to be successful.

Much less is known about spyware targeting Android devices, though that does not mean Android users are less at risk. More expensive Android devices, including Google's Pixel devices, are more secure and usually have fixes for vulnerabilities available more quickly than cheaper Android devices. Regularly rebooting devices will likely mitigate damage as spyware is generally

removed from devices after a reboot.[iv] Rooting an Android device may also remove evidence of a previous infection, which may be a concern for some users.

Case Studies

Suspension of EuroPride's Instagram Account

Belgrade Pride, an event held in the Serbian capital to celebrate the local LGBTQ+ community and its allies, was first held in 2001. This event was met with violence from sports hooligans and far-right activists.[27] The event was not held again until 2010 and was once again met with violence from the same groups. This led to fighting between far-right extremists attempting to disrupt the event and thousands of police officers.[28]

Threats of violence led to the Serbian government banning future pride events, but this ban was ruled unconstitutional in 2013. Apart from 2020 (due to the COVID-19 pandemic), the event has taken place every year since 2014.

In 2022, Belgrade Pride was the host of EuroPride, an annual European event celebrating the LGBTQ+ community in the whole of Europe.[29] Despite the increased visibility of an international event, the same groups who have opposed the event since 2001 tried once again to disrupt the celebration. These disturbances extended to the online space via social media. Prior to the event, many individuals reported EuroPride's account to Instagram, alleging violation of Instagram's terms and conditions. Though difficult to confirm, this is likely what led to the "shadow banning" of EuroPride's Instagram account and subsequent temporary suspension less than a month before the event. The shadow ban meant that the EuroPride account could continue to share new posts and stories, but their reach was very limited. The subsequent suspension made the account unavailable.

SHARE Foundation, a Serbia-based non-profit organization that works to advance human rights and freedoms online and promote positive values of an open and decentralized Internet, in coordination with the Access Now Helpline, stepped in to assist. Although the suspension was eventually lifted by Meta, it had a significant impact on the event's ability to attract interest via social media.

Late in August, Serbian president Vučić announced EuroPride was not allowed to take place, citing political events and fear of disruption.[30] In the end the ban was lifted, and the event took place in September 2022 as initially planned and had an estimated 10,000 participants.[31]

Companies like Meta that own social networks such as Instagram, deal with countless user-generated reports of terms violations. Civil society is often the target of such violations, such as doxing or threatening language, and consequences can be severe. Civil society is also regularly targeted in false reports. Incorrect handling of user-generated reported violations can have

[iv] This is the case with all known iPhone spyware and likely also for Android spyware, especially the kind that 'roots' the device.

serious consequences, as the EuroPride 2022 organizers experienced. Meta and other social networks should be very cautious before moderating content of civil society organizations, especially in the context of high-profile events.

Facebook Account Hacked to Post CSAM

Minja Marđonović is a feminist activist based in Serbia, whose activism mostly occurs in the digital space. Like many digital activists, she relies heavily on social media platforms like Facebook and Instagram.

In September 2022, the Serbian pro-government tabloid *Informer* published an interview with a man who had recently finished a 15-year prison sentence for multiple counts of rape and physical assaults on women. The interviewee openly discussed feeling liberated after committing the attacks and gave "instructions" to women on how to behave during an attack. Minja was among many in Serbia outraged by the publication.[32]

A few days after sharing her frustration on social media and in an online column for *ELLE*, Minja received a phishing email targeting her Facebook account. The phishing attack was successful, and Minja's Facebook and linked Instagram account were hacked. This, unfortunately, is very common for those who hold undertaking activist work. What happened next, however, is less common.

The adversary with access to Minja's accounts posted child-sexual abuse material (CSAM, often referred to as "child pornography") on her Facebook and Instagram accounts. Meta, which owns both social networks, uses software to detect CSAM. When it is detected, as was the case here, the account is automatically shut down.

Not only did this leave Minja without the ability to advocate on behalf of women, now Minja was in need of support herself. In addition to the technical assistance needed to get her accounts back, she also now needed psychological support. In an interview for local website Zoomer, Minja discussed the sleepless nights she had after the incident, but also the support she received from other women that helped her feel less alone.[33]

Though uncommon, an account hack followed by the posting of content that automatically leads to account shutdown, such as CSAM or terrorist material, does happen. Social media platforms as well as the digital safety community ought to be aware of this threat and ensure that good procedures are in place to prevent these attacks and respond to them.

Recovering hacked social media accounts can be frustratingly hard and, in the case of civil society, often involves personal connections and third-party organizations who are "trusted partners" of the larger platforms. It is a lot harder when an algorithm flags an account for posting CSAM.

In the end, with the help of local organizations such as the SHARE Foundation, a Serbia-based non-profit organization working to advance human rights and freedoms online and promote positive values of an open and decentralized internet, as well as free access to information, knowledge, and technology, Minja recovered her accounts. She continues her online activism.

Further Reading

As seen in this report, civil society organizations and journalists often face unique, advanced threats, while lacking the resources to detect, analyze, and prevent them. An in-depth understanding of the threats facing civil society and media allows digital security practitioners to tailor their responses and better support the organizations they work with, leading to customized mitigation measures that are more effective and easier for civil society and media organizations to implement. For more information on the threats faced by civil society and journalists, Internews and its partners have authored the report "Global Trends in Digital Threats: Civil Society & Media," as well as Digital Threat Reports for Armenia, Brazil, Mexico, and Ukraine. These resources can be found on the Internews' Technology Resources webpage.

History of Serbia

The Republic of Serbia (Република Србија) is a unitary parliamentary republic located in the Pannonian Basin and on the Balkan Peninsula. It is bordered by Hungary, Romania, Bulgaria, North Macedonia, Croatia, Bosnia-Herzegovina, and Montenegro. After the end of World War I, Serbia co-founded Yugoslavia with other South Slavic nations, first as the Kingdom of Serbs, Croats, and Slovenes. Following liberation from Axis occupation during World War II, Yugoslavia was reorganized into a federal republic under communist rule. In the 1980s and 1990s, Yugoslavia dissolved, leading to the Yugoslav Wars between the former constituent republics. Montenegro was formerly in a union with Serbia after the breakup of Yugoslavia until the union was peacefully dissolved in 2006, which marked the first independent Serbian state since 1918.[34] Since the 19th century when Serbia gained independence from the Ottoman Empire, Serbia has had a close relationship with Russia that remains to this day.[35]

Serbia is classified as an upper-middle income economy[36] and is a member of the United Nations,[37] the Council of Europe,[38] the Organization for Security and Co-operation in Europe,[39] the Partnership for Peace,[40] the Central European Free Trade Agreement,[41] and is currently acceding to the World Trade Organization.[42] Serbia applied for membership in the European Union in 2009, and its candidacy for accession was accepted in 2012. Serbia and the EU began accession negotiations in 2014. In 2021, 538 Members of the European Parliament voted in favor of a report that Serbia would need to normalize relations with Kosovo to join the EU, as well as make improvements to "the judiciary, freedom of expression, and the fight against corruption and organized crime."[43]

Acknowledgements

Since 2021, Internews has worked with seven Threat Labs (*local organizations with the technical capacity and appropriate tools to analyze suspicious phishing and malware samples and then share information back to the community regarding attack trends, emerging threats, and countermeasures*) to respond to incidents affecting the digital security of civil society and media organizations around the world. The data collected through the incident response program helped shape mitigations and response approaches for at-risk communities and informed this report.

Internews would like to express our gratitude to the community of Threat Labs that worked with us on this project. They are committed to assisting those in need and ensuring that their partners in civil society and media organizations can complete their important work safely and effectively. In total, this project supported Threat Labs in responding to over 200 digital security incidents and publishing over 60 educational resources through their websites and social media platforms.

Special thanks to SHARE Foundation for providing the information to document and share these case studies and for reviewing and contributing valuable feedback to this report. The report would not have been possible without Bojan Perkov and the SHARE Foundation team.

Endnotes

[1] "Freedom in the World 2023: Serbia." Freedom House. Accessed July 2023. https://freedomhouse.org/country/serbia/freedom-world/2023.

[2] "Freedom in the World 2019: Serbia." Freedom House. Accessed July 2023. https://freedomhouse.org/country/serbia/freedom-world/2019.

[3] Gec, Jovana. "Serbia to seek meeting with NATO chief, UN Security Council session on Kosovo tensions." *Associated Press*. July 6, 2023. https://apnews.com/article/serbia-kosovo-tensions-un-vucic-nato-542321f116c5cd368b0a98f53c9fc904.

[4] Mong, Attila. "'The most dangerous situation': Serbian journalists accused of links to organized crime." Committee to Protect Journalists. June 30, 2021. https://cpj.org/2021/06/serbian-journalists-accused-organized-crime/.

[5] Mong, "'The most dangerous situation': Serbian journalists accused of links to organized crime."

[6] "Serbia: Independent journalism faces biggest crisis in years." Independent Federation of Journalists. April 26, 2023. https://www.ifj.org/media-centre/news/detail/category/press-releases/article/serbia-independent-journalism-faces-biggest-crisis-in-years.

[7] "The Budapest Convention (ETS No. 185) and its Protocols." Could of Europe. Accessed September 2023. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[8] Stošić, Lazar and Aleksandra Janković. "Cybercrime in the Republic of Serbia: Prevalence, Situation and Perspectives." *Kultura polisa* 19, no. 4 (2022): 83. DOI:10.51738/Kpolisa2022.19.4r.82sj.

[9] Hromcová, Zuzana. "In the Balkans, businesses are under fire from a double-barreled weapon." ESET Research. August 14, 2019. https://www.welivesecurity.com/2019/08/14/balkans-businesses-double-barreled-weapon/.

[10] Abrams, Lawrence. "PwndLocker Ransomware Gets Pwned: Decryption Now Available." *Bleeping Computer.* March 5, 2020. https://www.bleepingcomputer.com/news/security/pwndlocker-ransomware-gets-pwned-decryption-now-available/.

[11] "Kako Je Novi Sad Otet I Zaključan." SHARE Foundacija. June 11, 2021. https://www.sharefoundation.info/sr/kako-je-novi-sad-otet-i-zakljucan/.

[12] Simpson, Jack. "Threat actor of in-Tur-Est." PwC, Cyber Threat Intelligence. January 27, 2022. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/threat-actor-of-in-tur-est.html.

[13] Martin, Alexander. "Serbian government reports 'massive DDoS attack' amid heightened tensions in Balkans." *The Record*. January 8, 2023. https://therecord.media/serbian-government-reports-massive-ddos-attack-amid-heightened-tensions-in-balkans.

[14] Cimpanu, Catalin. "Ultranationalist Developer Behind SerbRansom Ransomware." *Bleeping Computer.* February 11, 2017. https://www.bleepingcomputer.com/news/security/ultranationalist-developer-behind-serbransom-ransomware/.

[15] Cimpanu, Catalin. "Suspected Member of TheDarkOverlord Hacking Group Arrested in Serbia." *Bleeping Computer.* May 16, 2018. https://www.bleepingcomputer.com/news/security/suspected-member-of-thedarkoverlord-hacking-group-arrested-in-serbia/.

[16] Vail, Emma. "Serbian resident pleads guilty to multi-million dollar BEC scheme." *The Record*. February 8, 2022. https://therecord.media/serbian-resident-pleads-guilty-to-multi-million-dollar-bec-scheme.

[17] Perkov et al., "Digital Rights Falter Amid Political and Social Unrest," (53).

[18] Perkov et al., "Digital Rights Falter Amid Political and Social Unrest," (53).

[19] Šajkaš, Marija. "Two-fold risk for Serbia's women journalists as attackers target their work and gender." Committee to Protect Journalists. October 12, 2017. https://cpj.org/2017/10/two-fold-risk-for-serbias-women-journalists-as-att/.

[20] Bush, Daniel. "'Fighting Like A Lion for Serbia': An Analysis of Government-Linked Influence Operations in Serbia." Stanford Freeman Spogli Institute for International Studies. April 2, 2020. https://fsi.stanford.edu/publication/april-2020-serbia-takedown.

[21] Nimmo, Ben, Margarita Franklin, David Agranovich, Lindsey Hudley, and Mike Torrey. "Q4 2022 Quarterly Adversarial Threat Report." Meta. February 2023. https://about.fb.com/wp-content/uploads/2023/02/Meta-Quarterly-Adversarial-Threat-Report-Q4-2022.pdf.

[22] Sharife, Khadija, Milica Vojinović, and Gur Meggido. "A leaked report sheds light on the source of a mysterious media attack on the Serbian president's political rival." Organized Crime and Correction Reporting Protect. March 24, 2023. https://www.occrp.org/en/storykillers/israeli-disinformation-expert-linked-to-faked-bank-accounts-in-serbian-smear-campaign.

[23]Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune. "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation." The Citizen Lab. October 15, 2015. https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.; "Hacking Team: The 'Italian job' of Serbian security services." SHARE Lab. July 14, 2015. https://labs.rs/en/hacking-team-the-italian-job-of-serbian-security-services/.

[24] Marczak, Bill, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert. "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles." The Citizen Lab. December 1, 2020. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.

[25] Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert. "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware." The Citizen Lab. December 16, 2021. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

[26] Lecigne, Clement and Christian Resell. "Protecting Android users from 0-Day attacks." Google, Threat Analysis Group. May 19, 2022. https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/.

[27] "History of Prides in Serbia." Belgrade Pride 2022 EuroPride. Accessed September 2023. https://europride2022.com/history.

[28] "Scores arrested in Belgrade after anti-gay riot." *BBC*. October 10, 2010. https://www.bbc.com/news/world-europe-11507253.

[29] "It's time for EuroPride 2022." Belgrade Pride 2022 EuroPride. Accessed September 2023. https://europride2022.com/.

[30] "Serbia: Authorities must repeal 'shameful' ban on Euro Pride walk." Amnesty International. September 16, 2022. https://www.amnesty.org/en/latest/news/2022/09/serbia-authorities-must-repeal-shameful-ban-on-euro-pride-walk/.

[31] N1 Beograd. "Organizatori: Gotovo 10.000 ljudi u šetnji i borbi za ravnopravnost." N1 SRB. September 17, 2022. https://n1info.rs/vesti/organizatori-gotovo-10-000-ljudi-u-setnji-i-borbi-za-ravnopravnost/.

[32] Kalan, Dariusz. "How an interview with a rapist fired up Serbia's feminists." *Al Jazeera*. March 31, 2023. https://www.aljazeera.com/features/2023/3/31/how-an-interview-with-a-rapist-fired-up-serbias-feminists.

[33] Marinović, Nemanja. "Minja Marđonović : I experienced digital murder." *Zoomer*. November 27, 2022. http://zoomer.rs/minja-mardjonovic-dozivela-sam-digitalno-ubistvo/.

[34] "Serbia country profile," *BBC*. Last modified June 30, 2023. https://www.bbc.com/news/world-europe-17907947.

[35] McBride, James. "Russia's Influence in the Balkans." Council on Foreign Relations. Last modified December 2, 2022. https://www.cfr.org/backgrounder/russias-influence-balkans.

[36] "Middle income." World Bank Data. Accessed September 2023. https://data.worldbank.org/country/XP.

[37]"Member States." United Nations. Accessed September 2023. https://www.un.org/en/about-us/member-states.

[38] "46 Member States." Council of Europe. Accessed September 2023. https://www.coe.int/en/web/portal/46-members-states.

[39] "Participating States." OSCE. Accessed September 2023. https://www.osce.org/participating-states.

[40] "Signatures of Partnership for Peace Framework Document." North Atlantic Treaty Organizations. Last modified March 27, 2020. https://www.nato.int/cps/en/natolive/topics_82584.htm.

[41] "About." Central European Free Trade Agreement. Accessed September 2023. https://cefta.int/about/.

[42] "Members and Observers." World Trade Organization. Accessed September 2023. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm.

[43] "European Parliament adopts Serbia's EU progress report." Euractiv. March 26, 2021. https://www.euractiv.com/section/politics/short_news/european-parliament-adopts-serbias-eu-progress-report/.