EuRepoC

ADVANCED
PERSISTENT
THREAT profile

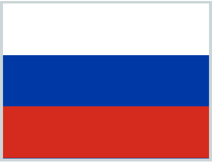
UNC1151

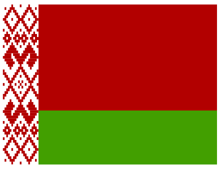
Fusing Technical and Social Vulnerabilities

Associated APT designations

- **UNC1151** (FireEye/Mandiant, ThreatConnect)
- **TA445** (Proofpoint)
- **PUSHCHA** (Google TAG)
- **Storm-0257/DEV-0257** (Microsoft)
- **Moonscape** (Secureworks)
- **UAC-0051** (CERT-UA)
- **Ghostwriter** (sometimes used as an actor designation for the group but more often describing its major "fingerprint" disinformation campaign against (Eastern) European countries and NATO since 2017; see section "Landmark operations" for details)

Countries of origin





Time period of activity

Since at least 2017-today

Sources [1][2][20]

Political affiliations

Over time, UNC1151's activity in the Ghostwriter influence campaign has been attributed to both the Russian and Belarusian military intelligence services and their governments as the state-sponsors. At a 6 September 2021 press conference, the German Federal Foreign Office attributed Ghostwriter activity in Germany to the Russian military intelligence agency GRU. Shortly thereafter, on 24 September, the EU High Representative issued a declaration on behalf of the European Union on respect for the EU's democratic processes, denouncing attempts at cyber-enabled interference tracked under the designation Ghostwriter. The statement described reports of several EU member states on Ghostwriter targeting, which associated it with the Russian state. In a report released two months later, the US threat intelligence company Mandiant concluded with high confidence that UNC1151 is linked to the Belarusian government. Additional industry reports from 2022 raised questions about the nature of suspected involvement by Russian military actors in the campaign. Until now tenuous, these assessments have sought to evaluate and, in part, substantiated similarities in tactics, techniques, and procedures (TTPs) between UNC1151 and other APTs associated with the GRU. Assessments by Recorded Future from March 2022 theorised that GRU actors may have operated from Belarusian soil or directed Belarusian operators as proxies, possibly to mask the direct involvement of Russian intelligence. Sources [3][4][5][6]

By Kerstin Zettl-Schabath, Jakob Bund, Lena Rottinger and Camille Borrett

Most frequent targets

- Belarus *(regime dissidents)*
- Colombia
- Estonia
- Germany
- Ireland
- Latvia
- Lithuania
- Poland
- Ukraine
- Switzerland
- NATO

Sources [1][3]

Agency type

State-integrated hacking group (members of the Belarusian military, potentially supported by "quasi-seconded" officers of the Russian military intelligence service) and/or **state-ordered hacking group** (Belarusian military actors operating as proxies of Russian military intelligence). If, as reported by industry experts, UNC1151 operates from Belarusian soil and (at least for a part of its activities) coordinates with Russian military intelligence actors, as indicated by Recorded Future reporting from March 2022, the group's further characterisation depends on whether its members are part of Belarusian military units or Russian citizens/military intelligence officers operating from Belarus. Based on the reported close connection between Belarusian and Russian intelligence services, Belarusian responsibility for the execution of UNC1151 activities, at the direction of or in consultation with Russian military intelligence actors, appears plausible.

Sources [3][4][29][30][31][32][33][34]

Group composition/organisational structure

Based on technical evidence, Mandiant located UNC1151 operators in Minsk, supporting the high-confidence judgment that the threat actor is associated with the Belarussian government and the medium-confidence assessment that the group is coordinated by the Belarusian military.

High-level overlaps with historical TTPS of the GRU-associated groups APT28 and Sandworm, as reported by Recorded Future, leave open the question of planning and implementation support from Russian agents. To date, forensic investigations have not revealed clear signs of direct Russian government involvement, although shared objectives between Russia and Belarus with respect to UNC1151 targets make Russian interest in the group's continued activity a possibility.

Recorded Future considers support from Belarus' domestic IT sector highly unlikely, as relevant capable actors have demonstrated their opposition to the Belarusian government, indicating that their involvement could adversely affect operational security.

Sources [3][4]

Impact type(s)

Direct

- **Intelligence Impact**; **Disinformation Impact** (attempts at eroding popular trust in government, directed against NATO member states)

Indirect

- **Reputational Impact** (as evidenced by activity against Polish politicians in 2021)

Sources [1] [7]

Incident type(s)

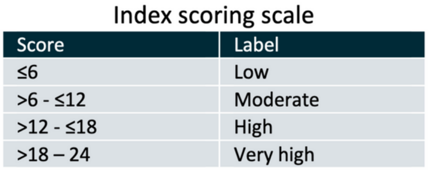
- **Data Theft** (cyber espionage)
- **Data Theft & Doxing** (hack-leak operations)
- **Disruption** (website defacements, DDoS attacks, dissemination of disinformation)

UNC1151 differentiates itself from many other APTs, including those affiliated with Russia, through the sustained engagement in disinformation campaigns. The reported hacking operations are only part of the group's overall activities, most of which are aimed at acquiring potentially compromising material and establishing a foothold on social media platforms to spread disinformation and fake news. Notable for these influence attempts is the strategic planning and timing of operations. The diversity of UNC1151's actions raises the bar for analytic efforts to develop an integrated picture of UNC1151. In- and outside government, analysis of malicious cyber activity and influence operations has traditionally been assigned to specialised units focused on individual facets, highlighting the need for intensified information exchange to see the sum of UNC1151's parts and to assess the impact of its activities.

Sources [1] [3] [21]

Threat Level Index

11/24 moderate threat level



Index scoring scale

Score	Label
≤6	Low
>6 - ≤12	Moderate
>12 - ≤18	High
>18 – 24	Very high

The Threat Level Index is derived from the EuRepoC dataset 1.0. It is a composite indicator covering five dimensions: the sectorial and geographical scope of the APT's attacks, the intensity of the attacks, the frequency of attacks and the use of zero-days. Please note that only attacks that have been publicly attributed to the APT group during its period of activity and which meet the specific EuRepoC criteria for inclusion are considered. The scores account for the practice of other APT groups analysed by EuRepoC, as thresholds used for determining low/high scores are based on the range of scores obtained across multiple APT groups. For more detailed information on the methodology underpinning the Threat Level Index see here and here.

Threat level sub-indicator	Score	Explanation
Intensity of attacks	1 /5	This sub-indicator represents the average "Weighted Cyber Intensity" score from the EuRepoC codebook for all attacks attributed to the APT for its period of activity. It assesses the type of attacks, their potential physical effects, and their socio-political severity – see here for more information
Sectorial scope of attacks	6 /8	This sub-indicator calculates average number of targeted sectors per attack attributed to the APT groups over its period of activity. If the majority of the targeted sectors are critical to the functioning of the targeted societies (i.e. political systems and critical infrastructure) a multiplier is applied. Incidents attributed to UNC1151 in the EuRepoC database, targeted, on average, 1.67 sectors per attack and all incidents were against state institutions/political systems.
Geographical scope of attacks	2 /4	This sub-indicator considers the average number of targeted countries per attack attributed to the APT group. Whole regions or continents affected during one attack are weighted higher. In the case of UNC1151, on average two countries were targeted per incident attributed to the group in the EuRepoC database.
Frequency of attacks	2 /4	This sub-indicator is calculated by dividing the total number of attacks attributed to the APT group within the EuRepoC database by the number of years of activity of the APT group. The obtained scores are then converted to a four-level scale. UNC1151 was responsible for less than 1 incident per year of activity (0.5).
Exploitation of Zero days	0 /3	This indicator calculates the percentage of attacks attributed to the APT that use one or multiple zero days. The score obtained is then converted to a three-level scale. None of the incidents in the EuRepoC database attributed to UNC1151 used zero-days.

→ Overall, UNC1151 obtains a moderate-level threat score compared to other APT groups. The cyber incidents analysed within the EuRepoC framework had a low intensity regarding their physical and socio-political effects, while also having limited geographical reach and no zero-day exploits. On the other hand, incidents attributed to the group targeted several sectors simultaneously and were slightly above average in terms of frequency.

TECHNICAL CHARACTERISTICS / PECULIARITIES / SOPHISTICATION

UNC1151 has gradually honed their technical skill set, demonstrating a capacity to absorb new tactics and learn from operational outcomes. Evolutions in tradecraft may have been further enabled by increased training/support from Russian military operators.

Basic attack pattern:

Prior to 2021, Ghostwriter initiated campaigns fabricating false narratives and corresponding content, such as made-up quotes from sitting officials, photographs, or other documents in support of these narratives. The group then seeded the narrative through compromised legitimate websites and sought to amplify the material via inauthentic personas who shared engineered articles on social media and by impersonating public figures to approach media outlets and governments officials via email for comment. Notably, in late 2020 and early 2021, the group expanded this procedure to harvesting social media credentials by spearphishing to elevate false narratives through hijacked accounts of government officials. UNC1151 uses GoPhish to disseminate their phishing lures. To imitate legitimate webmail providers, generic login pages, and legitimate websites, the threat actor initially used the anonymous DNS resolver Freenom to redirect targeted users but has migrated to Cloudflare since around 2022. The group has used a variety of custom malware (e.g., HIDDENVALUE and HALFSHELL), as well as freely available tools.

Zero-day exploits:

No use of zero-days has been publicly reported for Ghostwriter.

Malware and tools used (non-exhaustive)

Cobalt Strike	RADIOSTAR	VIDEOKILLER
HALFSHELL	HIDDENVALUE	MicroBackdoor
.NET applications	HermeticWizard	IsaacWiper
FormBook	SunSeed	Whispergate

Sources [1][3][8][9][10][11][12][13][14][15][23]

Select tactics and techniques leveraged by the group based on the MITRE ATT&CK Framework

MITRE Initial Access
Phishing

MITRE Persistence
Boot or logon autostart execution: *Registry run keys/startup folder*

MITRE Defense Evasion
Deobfuscate/decode files or information

MITRE Impact
Defacement
Data encrypted for impact
Network denial of service

Sources [22]

ATTRIBUTION

Attribution milestones

1) Mandiant report "'Ghostwriter' Influence Campaign" (2020).

2) German government attribution of Ghostwriter activity to the Russian military intelligence service GRU (6 September 2021).

3) Declaration by the High Representative on behalf of the EU (24 September 2021), highlighting EU member state reporting of Ghostwriter activity that some member states attributed to the Russian state. The statement denounced the operations and called on Russia to follow norms of responsible state behaviour endorsed by all UN member states.

4) Mandiant report "Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity" (April 2021), associating elements of the Ghostwriter campaign with the emerging threat actor UNC1151.

5) Mandiant report, "UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests" (November 2021), establishing UNC1151's connection with the Belarusian military.

6) Recorded Future report "Ghostwriter in the Shell: Expanding on Mandiant's Attribution of UNC1151 to Belarus" (2022), building upon Mandiant's 2021 report and further elaborating on the group's potential hybrid structure combining Belarusian and Russian elements.

Sources [1] [4] [5] [6] [16]

Attribution ambiguities

Ghostwriter or UNC1151? In its first comprehensive report that detailed Ghostwriter activity in July 2020, Mandiant refrained from linking the campaign to a specific actor and instead described it as emerging "activity set." In follow-up reporting from April 2021, Mandiant concluded with high confidence that at least some activity of the Ghostwriter influence campaign was executed by the suspected state-sponsored cyber espionage actor UNC1151. At the time, the firm made no further judgments about attribution related to the group.

UNC1151 – a Belarusian operation, Russian Proxy, or collaborative framework for Belarusian and Russian military actors? At the time of reporting, it remains unclear whether Russian military intelligence relies on government/military hackers from Belarus as proxies to masquerade the origins of the operations or if Russian military operatives are actively, albeit indirectly, enabling the operations. Initial attributions by Germany focused on alleged ties of Ghostwriter to the GRU, joined by statements from Poland and the EU connecting the campaign to Russia's secret services and the Russian state more broadly.

Mandiant subsequently in November 2021 deemed links between UNC1151 and the Belarusian government to be highly likely and, more specifically, concluded with moderate confidence that the group maintained connections to the Belarusian military. Publicly, to date, this assessment stands uncontested and includes activities called out by the governments of Poland and Germany. Mandiant explicitly notes that it has not dismissed the possibility of Russian contributions to UNC1151 or Ghostwriter, but as of now has not identified any evidence to this end.

Considering that Mandiant only partially attributed the Ghostwriter campaign to UNC1151, the possibility of other actors being involved remains open. Industry perceptions have evolved to assigning Belarus a leading role in directing Ghostwriter.

It is worth noting that assessments of Ghostwriter contributions have largely focused on the campaign's cyber activity. Little is known about the influence operation aspects and generation of disinformation material, as noted in a report from Cardiff University prepared under the leadership of the former head of the EU's East StratCom Task Force.

Sources [1][3][5][6][7][15][17][18][21][24][25]

Attribution and detection sensitivity

Although UNC1151's technical capabilities as observed through Ghostwriter activity have improved over the years, there is no indication that this improvement and deception strategy is a direct reaction to previous attributions and distinct from growing organisational maturity.

Sources [13]

POLITICAL/LEGAL/LAW ENFORCEMENT ACTIONS

The German government and the EU publicly blamed the Russian state for Ghostwriter's malicious cyber activities and urged the Russian government to stop the campaign. In addition, both actors said they would consider "taking further steps."

German officials directly raised these concerns with their Russian counterparts in explicit reference to Ghostwriter during a meeting of the German-Russian High Level Working Group on Security during 2-3 September 2021.

Following partially-successful DDoS and defacement attacks against nearly 70 Ukrainian websites during 13-14 January 2022, the Security Service of Ukraine (SBU) announced an investigation into the incidents.

Sources [5][6][19]

Indicted individuals/sanctioned (associated) entities

As of early May 2023, no indictments or sanctions over suspected involvement in UNC1151 have been announced.

Landmark operations

NATO-themed influence campaign Ghostwriter: Starting in 2020, Ghostwriter operatives directed a coordinated wave of disinformation narratives at audiences in Lithuania, Latvia, and Poland, with the overriding goal to destabilise trust among NATO allies and in the reliability of the alliance overall. The campaign focused on compromising websites and disseminating fabricated content via hacked social media and email accounts. In isolated cases, the activities generated political attention and tensions, especially in Poland, culminating in the resignation of Michał Dworczyk, head of the Polish Prime Minister's Office, on 30 September 2022. Ghostwriter members are suspected of having compromised Dworczyk's personal email account that he also used for government business and started to leak internal messages in 2021. Published messages contained correspondence between government representatives and the sitting chief justice of Poland's constitutional court discussing ongoing proceedings in disregard for the separation of powers. Dworczyk linked his resignation to the impression that the scandal degraded his ability to administer his role effectively. Between 2018 and 2020, the Lithuanian news portal Kas Vyksta Kaune was compromised at least seven times in an attempt to push fabricated information from a legitimate source. When raising the lack of state support to improve the security of the organisation's systems with Lithuania's National Cyber Security Center, a former editor was told the news portal could be closed down if deemed to be a risk to Lithuania's national security. While the shutdown of a media outlet remains a hypothetical development, the encounter illustrates the power incident responses wield in shaping the outcome of cyber operations and points to potential non-cyber-related avenues of influence operations to impact public discourse.

Ghostwriter activity targeting Germany: During March 2021, seven members of the Bundestag and almost 30 members of state parliaments were targeted by spearphishing emails. German security authorities detected the incident early and contacted the politicians concerned. Officials initially linked these attempts to the Russian GRU.

Website defacements in Ukraine: In January 2022, nearly 70 Ukrainian websites became the target of DDoS and defacement attacks, warning the Ukrainian population to "expect the worst," in a possible harbinger of Russia's large-scale invasion of Ukraine on 24 February 2022. A Ukrainian government official attributed the attack to UNC1151 in a statement carried by Reuters on 16 January 2022. The same official - Serhiy Demedyuk, Deputy Secretary of Ukraine's National Security and Defense Council - noted in an interview with The Record on 18 January 2022, that some aspects of the attack displayed characteristics of other Russian APTs, namely Sandworm, APT28, and APT29, and stated further that the attack was a "demonstration of the synchronization of the cyber forces of the Russian Federation and the countries included in the so-called [Collective Security Treaty Organization] format."

Surging phishing campaigns targeting NATO countries in the context of Russia's war against Ukraine since 2022: According to a joint report in February 2023 by Google's Trust & Safety unit, its Threat Analysis Group (TAG), and Mandiant, phishing efforts have increased by over 300% compared to the 2020 baseline. The authors claimed UNC1151 (which TAG tracks as "PUSHCHA" and associates with Belarus) as mainly responsible for this upward trend.

Sources [1][4][5][7][9][15][16][20][26][27][28]

SOURCES

[1] Mandiant (2021), Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Activity, Mandiant. Available at https://web.archive.org/web/20230510190226/https://www.mandiant.com/sites/default/files/2021-09/rpt-ghostwriter-update-unc1151-000376-1.pdf [Archived on: 10.05.2023].

[2] Michael Raggi, Zydeca Cass, and the Proofpoint Threat Research Team (2022), Asylum Ambuscade: State Actor Uses Compromised Private Ukrainian Military Emails to Target European Governments and Refugee Movement, Proofpoint. Available at https://web.archive.org/web/20230220163752/https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails [Archived on: 20.02.2023].

[3] Gabriella Roncone, et al. (2021), UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests, Mandiant. Available at https://web.archive.org/web/20230503043900/https://www.mandiant.com/resources/blog/unc1151-linked-to-belarus-government [Archived on: 03.05.2023].

[4] Insikt Group (2022), Ghostwriter in the Shell: Expanding on Mandiant's Attribution of UNC1151 to Belarus, Recorded Future. Available at https://web.archive.org/web/20230514205550/https://go.recordedfuture.com/hubfs/reports/cta-2022-0318.pdf Archived on: 14.05.2023].

[5] Auswärtiges Amt (2021), Cyberangriffe auf Bundestagsabgeordnete und Landtagsabgeordnete durch den Cyberakteur „Ghostwriter". Available at https://web.archive.org/web/20230510192147/https://www.auswaertiges-amt.de/de/newsroom/regierungspressekonferenz/2480282#content_4 [Archived on: 10.05.2023].

[6] Council of the European Union (2021), Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes, European Council. Available at https://web.archive.org/web/20220531225957/https://www.consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/ [Archived on: 31.05.2022].

[7] Florian Flade and Hakan Tanriverdi (2021), Angriff der "Chaostruppe," Tagesschau. Available at https://web.archive.org/web/20230510193027/https://www.tagesschau.de/investigativ/wdr/hackerangriffe-105.html?_ga=2.218488081.927917024.1652362240-1118462645.1652362240 [Archived on: 10.05.2023].

[8] CERT-UA (2022), Кібератака групи UAC-0051 (unc1151) на державні організації України з використанням шкідливої програми MicroBackdoor (CERT-UA#4109). Available at https://web.archive.org/web/20220918134705/https://cert.gov.ua/article/37626 [Archived on: 18.09.2022].

[9] Catalin Cimpanu (2022), Hackers deface Ukrainian government websites, The Record. Available at https://web.archive.org/web/20230510191453/https://therecord.media/hackers-deface-ukrainian-government-websites/ [Archived on: 10.05.2023].

[10] Orange Cyber Defense (2022), Cyber war against Ukraine: Observations and recommendations. Available at https://web.archive.org/web/20230510194206/https://www.orangecyberdefense.com/de/blog/threat/cyber-war-against-ukraine-observations-and-recommendations [Archived on: 10.05.2023].

[11] Luke Richards (2022), Russian Cyber Attacks: What We Know so far, Vectra. Available at https://web.archive.org/web/20230510194828/https://www.vectra.ai/blogpost/russian-cyber-attacks-what-we-know-so-far [Archived on: 10.05.2023].

[12] NatSec News (2022), Prepare for Wiper Malware Attacks, Warns CISA. Available at https://web.archive.org/web/20230510195035/https://www.netsec.news/prepare-for-wiper-malware-attacks-warns-cisa/ [Archived on: 10.05.2023].

[13] Securin (2022), Cyberwar Bulletin 1: Russia & Ukraine. Available at https://web.archive.org/web/20230510195331/https://www.securin.io/articles/cyberwar-bulletin-1-russia-ukraine/ [Archived on: 10.05.2023].

[14] Hive Pro (2022), Ukraine government entities targeted by a destructive malware "Whispergate." Available at https://web.archive.org/web/20230510195647/https://www.hivepro.com/ukraine-government-entities-targeted-by-a-destructive-malware-whispergate/ [Archived on: 10.05.2023].

[15] Dmitry Smilyanets (2022), A top Ukrainian security official on defending the nation against cyber attacks, The Record. Available at https://web.archive.org/web/20230510191504/https://therecord.media/a-top-ukrainian-security-official-on-defending-the-nation-against-cyber-attacks/ [Archived on: 10.05.2023].

[16] Lee Foster, et al. (2020), 'Ghostwriter' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned With Russian Security Interests, Mandiant. Available at https://web.archive.org/web/20230510191505/https://www.mandiant.com/resources/blog/ghostwriter-influence-campaign [Archived on: 10.05.2023].

[17] Catalin Cimpanu (2021), EU formally blames Russia for GhostWriter influence operation, The Record. Available at https://web.archive.org/web/20230510200945/https://therecord.media/eu-formally-blames-russia-for-ghostwriter-hack-and-influence-operation [Archived on: 10.05.2023].

[18] William Thomas (2021), EMEA and APAC governments targeted in widespread credential harvesting campaign, Cyjax. Available at https://web.archive.org/web/20230510201212/https://www.cyjax.com/2021/09/16/emea-and-apac-governments-targeted-in-widespread-credential-harvesting-campaign/ [Archived on: 10.05.2023].

[19] Служба безпеки України (2022), СБУ розслідує причетність російських спецслужб до кібератаки на органи державної влади України. Available at https://web.archive.org/web/20230408212019/https://ssu.gov.ua/novyny/sbu-rozsliduie-prychetnist-rosiiskykh-spetssluzhb-do-sohodnishnoi-kiberataky-na-orhany-derzhavnoi-vlady-ukrainy [Archived on: 08.04.2023].

[20] Google Threat Analysis Group and Mandiant (2023), Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape. Available at https://web.archive.org/web/20230320202359/https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf [Archived on: 20.03.2023].

[21] Cardiff University Security, Crime and Intelligence Innovation Institute (2023), The Ghostwriter Campaign as a Multi-Vector Information Operation: Attempts to Control its Influence & the Limitations of Current Countermeasures. Available at https://web.archive.org/web/20230510203213/https://www.cardiff.ac.uk/__data/assets/pdf_file/0005/2699483/Ghostwriter-Report-Final.pdf [Archived on: 10.05.2023].

[22] Lee Foster, et al. (2021), Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity, Mandiant. Available at https://web.archive.org/web/20230510203530/https://www.mandiant.com/resources/blog/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity [Archived on: 10.05.2023].

[23] Pierluigi Paganini (2022), GhostWriter APT targets state entities of Ukraine with Cobalt Strike Beacon, Security Affairs. Available at https://web.archive.org/web/20230510203810/https://securityaffairs.co/129527/apt/ghostwriter-apt-targets-state-entities-of-ukraine-with-cobalt-strike-beacon.html [Archived on: 10.05.2023].

[24] Agnieszka Barteczko and Tatiana Ustinova, ed. William Maclean (2021), Poland says it sees link between hacking and Russian secret services, Reuters. Available at https://web.archive.org/web/20230510204023/https://www.reuters.com/world/poland-says-it-sees-link-between-hacking-russian-secret-services-2021-06-22/ [Archived on: 10.05.2023].

[25] Zosia Wanat (2021), Leaked email scandal engulfs Poland's political elite, Politico. Available at https://web.archive.org/web/20230510204629/https://www.politico.eu/article/leaked-email-scandal-engulfs-poland-political-elite-mails-hacking/ [Archived on: 10.05.2023].

[26] Associated Press (2022), Polish PM's aide, target of email hacking, resigns. Available at https://web.archive.org/web/20230510205837/https://apnews.com/article/russia-ukraine-putin-poland-government-and-politics-6040a1a99cec0b3b0f76a7acbe52c790 [Archived on: 10.05.2023].

[27] Stacy Peterson (2022), Threat analysis of the Russia/Ukraine conflict, NTT Security. Available at https://web.archive.org/web/20230510210352/https://www.security.ntt/blog/threat-analysis-of-the-russia-ukraine-conflict [Archived on: 10.05.2023].

[28] Pavel Polityuk (2022), EXCLUSIVE Ukraine suspects group linked to Belarus intelligence over cyberattack, Reuters. Available at https://web.archive.org/web/20230510210621/https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/ [Archived on: 10.05.2023].

[29] Jakub Przetacznik (2023), Russia-Belarus military cooperation, European Parliamentary Research Service. Available at https://web.archive.org/web/20230308120134/https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739348/EPRS_ATA(2023)739348_EN.pdf [Archived on: 08.03.2023].

[30] Ministry of Foreign Affairs of the Republic of Belarus, *Belarus and Russia*. Available at https://web.archive.org/web/20230523120741/https://mfa.gov.by/en/bilateral/russia/ [Archived on: 23.05.2023].

[31] Peter Szyszlo (2003), *Countering NATO Expansion: A Case Study of Belarus-Russia Rapprochement*, NATO Research Fellowship report. Available at https://web.archive.org/web/20230427020039/https://www.nato.int/acad/fellow/01-03/szyszlo.pdf [Archived on: 23.05.2023].

[32] Office of the President of the Republic of Belarus (2023), *Meeting with Head of Russia's Foreign Intelligence Service Sergei Naryshkin*. Available at https://web.archive.org/web/20230523120649/https://president.gov.by/en/events/vstrecha-s-direktorom-sluzhby-vneshney-razvedki-rossii-sergeem-naryshkinym-1680603463 [Archived on: 23.05.2023].

[33] TASS (2020), *Russian-Belarusian intelligence cooperation unrelated to events in Belarus — Kremlin*. Available at https://web.archive.org/web/20230523120700/https://tass.com/politics/1215111 [Archived on: 23.05.2023].

[34] Information Analysis Portal of the Union State (2021), *Belarusian KGB, Russian SVR team up to counteract Western destructive actions*. Available at https://web.archive.org/web/20230523120728/https://soyuz.by/en/theme-of-the-day/belarusian-kgb-russian-svr-team-up-to-counteract-western-destructive-actions [Archived on: 23.05.2023].

About the authors

- **Kerstin Zettl-Schabath** is a researcher at the Institute of Political Science (IPW) at Heidelberg University.
- **Jakob Bund** is an Associate at the German Institute for International and Security Affairs (SWP).
- **Lena Rottinger** is a political science student at the Institute for Political Science (IPW) at Heidelberg University and a former research intern for EuRepoC.
- **Camille Borrett** is a Data Analyst at the German Institute for International and Security Affairs (SWP).

Last updated 23.05.2023