Cybersecurity Ecosystem Report

Western Balkans: Emerging Cyber threats

March 2022

Supported by

UK Government

pwc

ISAC
CENTAR ZA MEĐUNARODNE I BEZBEDNOSNE POSLOVE
INTERNATIONAL AND SECURITY AFFAIRS CENTRE

This report has been supported by the UK Government.
The views expressed in this publication do not necessarily
represent the views of the UK Government.

Executive summary

This Cybersecurity Ecosystem Report maps cyber threats in the Western Balkans, identifying key risks, threats, incident and attack types, and, where possible, threat actors. Commissioned by the UK Government, the report has been prepared jointly by PwC, focusing on the global and regional threat landscape, and the ISAC Fund, providing the geopolitical context for each of the Western Balkan economies (Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia).

The findings are based on comprehensive desk research on existing bilateral, regional and international agreements and other forms of cooperation that Western Balkan economies have in place, as well as official reports of cyber authorities. This is supplemented by information obtained from interviews and focus groups with local stakeholders from the public and private sector, academia and civil society. Finally, insights into the activities of global threat actors are shared from PwC's Cyber Threat Intelligence (CTI) team.

The report shows that the cybersecurity threats faced by Western Balkan economies generally mirror global threats. Ongoing increases in digital activity, accelerated by the global pandemic, have led to greater numbers of incident reports received by national authorities. Increasingly, smaller actors such as small and medium enterprises, media actors and civil society organisations are also encountering cyber threats. Attacks are becoming more sophisticated, with better tailoring of malicious content to local languages and context. Currently, cybercrime is seen as the main threat, with malware, phishing, ransomware and, to an extent, Distributed Denial of Service (DDoS) as the most common attack types.

Regional stakeholders do not consider the Western Balkans a primary target for any particular threat actor. Instead, attacks and incidents are perceived as collateral damage from attacks aimed at other primary targets. Additionally, stakeholders have not identified any region-specific malicious actors, or cybersecurity developments. This does not discount the possibility of a more regional dimension to cyber threats emerging in the near future, given the pace of digitalisation and geopolitical developments.

The main risks identified fall under the headings of governance, technical, capacity and awareness. In terms of governance, national cybersecurity frameworks are either incomplete or have multiple shortcomings, including overlapping jurisdictions and limited enforcement powers. From a technical perspective, legacy systems and equipment, especially in the public sector and critical national infrastructure, bring a significant vulnerability that could be exploited by malicious actors. Capacity-wise, the global shortage of cybersecurity experts is arguably

felt even more strongly in the Western Balkans, with the ongoing trend of high emigration from the region. Finally, a general lack of awareness of cyber risks and threats, across all strands of Western Balkan societies, is one of the key obstacles to building more resilient societies in the region.

Western Balkan economies have been actively attempting to strengthen resilience of their national cybersecurity ecosystems. Often with the support of the international community, regional economies have developed relevant legislation, established new institutions, and built up technical and operational capacities. Western Balkan economies have also forged bilateral and multilateral partnerships, generally gravitating towards EU and NATO approaches but with some national differences.

Sustaining these efforts requires continued engagement of all relevant stakeholders across the region, as well as support from international partners. This report recommends the following actions to foster greater cyber resilience in the Western Balkans:

- Better communicating the mutual benefits of incident reporting and information sharing among all stakeholders;
- Developing tailored methodologies for regular monitoring of cybersecurity developments, collecting, processing and categorising data on reported incidents, and devising national threat landscape reports;
- Agile alignment of legislative and strategic frameworks to address the evolving cybersecurity threat landscape, developments in the cyber sphere, and resulting needs;
- Capacity development of additional relevant institutions and bodies, such as those in charge of investigation and prosecution of cybercrimes;
- Adopting a sectoral approach by building decentralised competences and response capacities, centrally coordinated at the national level;
- Devising joint approaches of public and private sectors and establishing partnerships with academic institutions aimed at identifying sustainable models to address workforce constraints;
- Running comprehensive cybersecurity awareness programmes, segmented, designed and delivered in a way to target specific audiences across Western Balkan societies.

Table of contents

List of abbreviations

APT	Advanced Persistent Threat
CCD CoE	(NATO) Cooperative Cyber Defence Centre of Excellence
CEEC	Central and Eastern European Countries
CERT	Computer Emergency Response Team (incl. Computer Security Incident Response Teams – CRISTs, and Computer Incident Response Teams – CIRTs for the purpose of this report)
CII	Critical Information Infrastructure
CNI	Critical National Infrastructure
CoE	Council of Europe
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
ENISA	EU Cybersecurity Agency
EU	European Union
GFCE	Global Forum on Cyber Expertise
ICT/IT	Information and Communication Technology/Information Technology
IPA	Instrument for Pre-accession Assistance (of the EU)
IPAP	Individual Partnership Action Plan (with NATO)
ISAC	Information Sharing and Analysis Centre
MoC	Memorandum of Cooperation
MoU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NIS	Network and Information Security
OSCE	Organization for Security and Co-operation in Europe
TTP	Tactics, techniques and procedures
UN GGE	United Nations Group of Governmental Experts
UNDP	United Nations Development Programme
UNICEF	United Nations Children's Fund

Introduction to the Report

The primary aim of this report is to map the existing cybersecurity threat landscape in the Western Balkans. This includes identifying known key risks, threats, incident and attack types, and, where possible, threat actors that Western Balkan economies, their competent authorities and other relevant stakeholders are faced with. Aimed at generating greater awareness on the cybersecurity ecosystem in the Western Balkans, the report provides insight into existing trends in the Western Balkan cybersecurity landscape and the perceptions thereof, as well as expectations of regional stakeholders on what the imminent cyber future may hold.

The report starts with a brief overview of global trends in cybersecurity and how these trickle down to the Western Balkans. A mapping of global threat actors whose activities have been recorded in the Western Balkans is provided, with an indication of the attack methods employed and the types of stakeholders targeted.

This is followed by a deep-dive into regional developments, covering the wider geopolitical context relevant for the purpose of this report and the cyber threat landscape itself. The geopolitical context is based on an analysis of existing international, regional and bilateral agreements and cooperation frameworks. The threat landscape encompasses existing trends, identified risks and challenges, cooperation and support patterns and anticipated future developments in cybersecurity in each respective economy, the region as a whole, and globally.

The report concludes with a list of observations derived from the research and analysis process. A set of tailored recommendations pertaining to the possible mitigation of identified risks and challenges is provided, taking into account expected future needs of Western Balkan economies in order to foster more cyber resilient societies in this region.

The report is informed by content provided by PwC's in-house threat intelligence team, who perform in-depth research into current and historical cyber threat actors from across the globe, publicly available information and data on bilateral cooperation frameworks and relations of Western Balkan economies and competent authorities' reports on recorded incidents and attacks in cyberspace. This is supplemented with information obtained through interviews with relevant stakeholders from each of the regional economies in scope. The report has been jointly produced by PwC, compiling the global and regional threat landscape analysis, and ISAC Fund, providing the geopolitical context for each of the Western Balkan economies.

Approach and methodology

For the purpose of this report, a mixed-methods approach has been employed, combining desktop research, (virtual) field work and internal resources.

Desktop research has been used as the primary method for collecting information on existing bilateral, regional and international agreements and other forms of co-operation that Western Balkan economies have in place, feeding into respective analyses of the geopolitical context. Specific sources used to this end include:

- Online databases of national gazettes, listing national legislation and cooperation mechanisms in place;
- Embassy websites to further supplement initial findings or provide information where the project team experienced limitations in terms of language and/or machine readability of existing content;
- Academic articles analysing in more detail the geopolitical context in order to provide more information on the causes and consequences of specific arrangements; and
- Public institutions' and media reports on specific statements made by public officials, bilateral meetings and official state visits, as well as relevant initiatives, projects and events.

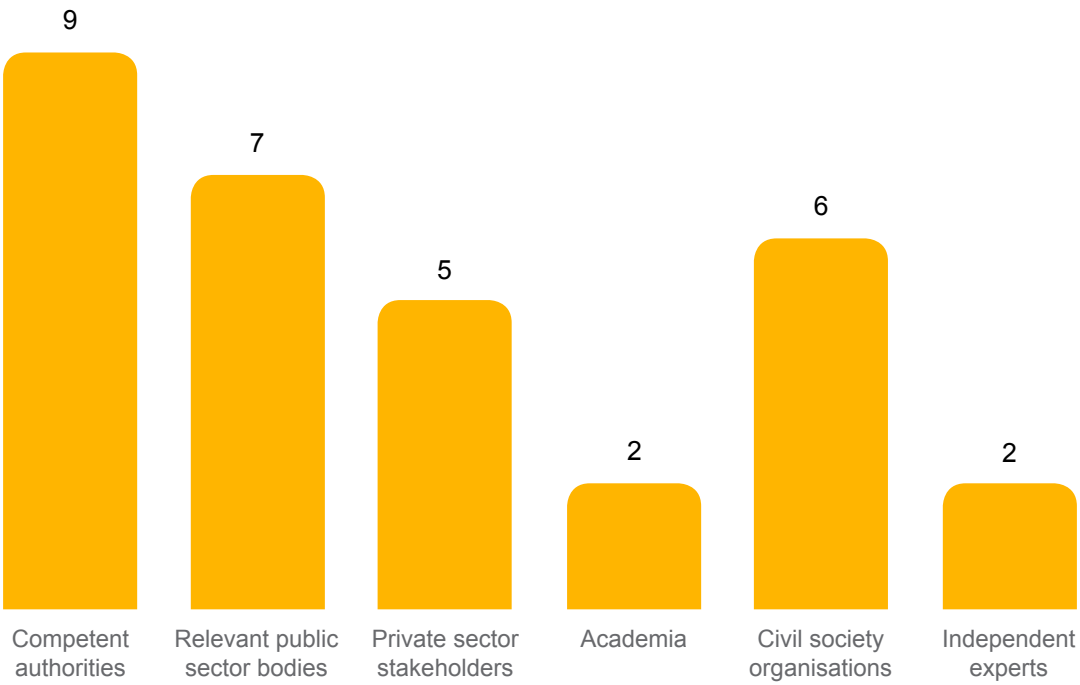
Desktop research has also been employed to collect relevant information regarding officially reported incidents in order to infer existing trends. To this end, publicly available reports of competent authorities and national CERTs have been addressed in order to map out the type and frequency of recorded incidents at the national level, for each of the Western Balkan economies. In instances where official reports were not available, information has been obtained through direct communications with relevant authorities.

The initial findings obtained through desktop research are complemented by information obtained through semi-structured interviews with relevant stakeholders from the public and private sector, academia and civil society, conducted between November 2021 and January 2022. The purpose of these interviews was to elaborate in greater detail on the data collected, and as to provide insight into the root causes of recognised existing risks, threats and challenges, as well as the perceptions of relevant stakeholders as to what the future holds.

In addition, dedicated focus groups have been conducted with civil society organisations active in the field(s) of gender, womens' and LGBTQI rights, among others, in order to provide basic insight into the extent and frequency of challenges that these and other vulnerable groups experience in cyberspace. Although not the pri-

mary focus of this report, the purpose of these focus groups has been to provide for a more comprehensive overview of the cybersecurity landscape in the Western Balkans, taking into account developments that have, to date, been commonly overlooked in official statistics of competent authorities for a number of reasons.

In total, just over 30 stakeholders have been consulted for the purpose of this report, including representatives of competent authorities (competent ministries and national CERTs), other relevant public institutions and bodies (relevant sectoral ministries and other public sector/governmental CERTs), academia and civil society, as well as independent experts. A high-level breakdown of the number of interviewees per sector is provided below.



Finally, reports produced by PwC's Cyber Threat Intelligence (CTI) team and relevant international actors have been referred to in order to identify potential regional peculiarities compared to global trends. To this end, existing CTI reports have been filtered to those where global threat actors and developments in cyberspace have been found as affecting the Western Balkans region as a whole or any one of its economies, providing details on the attack methods employed as well as the threat actors seen as likely to have been involved. Global threat landscape reports have also been used to compare the trends expected to unfold at the international level to those identified as forthcoming by the interviewed regional stakeholders.

Using qualitative analysis and data triangulation, the collected data has been processed in order to provide two key strands forming this report:

- Current state analysis and existing trends; and
- Stakeholder perceptions and expectations of the current state and future trends.

The report therefore contains information observed through three lenses, based on the level of certainty in the accuracy of the information and the possibility to verify collected data through triangulation or using official sources:

Lens	Explanation
Fact	Data or information that was scoped from official, publicly available documents (e.g. annual CERT reports), or obtained through stakeholder interviews and verified using additional sources (incl. publicly available documents and statements of other interviewees)
Statement	Data or information obtained through stakeholder interviews that has not been subject to further assessment regarding accuracy (e.g. an interviewee's recollection of an event/incident; information on existing cooperation patterns, etc.)
Perception	Data or information obtained through stakeholder interviews that relates to the interviewee's independent, subjective opinion on what could be taking place, both at present and in the future (mainly pertaining to opinions on the difference between official reports and the actual state of affairs, as well as expected future trends)

Limitations

In the process of compiling this report, the project team has faced the following limitations:

Variations in data availability across Western Balkan economies, especially when it comes to publicly available information pertaining to existing international cooperation agreements. These range from general data (un)availability, to online legal databases that do not contain a search function or have certain limitations pertaining to machine readability. In order to mitigate this challenge, the project team referred to alternative sources, such as official websites of embassies and diplomatic posts of specific Western Balkan economies in order to map existing bilateral cooperation frameworks and agreements.

Variations in available information on reported incidents across Western Balkan economies. These range from competent authorities having a track-record of officially recorded incidents dating several years back, to others who have only recently started classifying different incident types, and those who still lack sufficient data to be able to produce relevant reports on previous incidents. This impeded the possibility of comparison and generating more comprehensive national trends from a quantitative aspect. Further variations pertain to the way in which national competent authorities and CERTs present aggregated data on recorded incidents. Namely, depending on available sources of information, national CERTs cluster incidents by incident type, threat actors and/or the number of affected IP addresses. This limits the possibility of inferring more specific, aggregate trends for the region as a whole. Consequently, the project team relied on information obtained through interviews with representatives of national competent authorities and CERTs for qualitative insight, to supplement initial findings.

Lack of responsiveness of some of the public sector institutions initially identified as relevant in the context of this report. This can be attributed to the overall timing of the project itself and the planned interviews taking place at the very end of the year. Another potential cause for the relative hesitancy of some stakeholders to take part in the interviews is that this type of research is a novelty in the region, causing some of the targeted interviewees to approach discussions on the threat landscape, threat actors and recorded incidents with a higher degree of caution. For this reason, the project team has anonymised all information obtained through stakeholder interviews and focus groups.

Identified global trends

In 2021, cybersecurity has been defined as 'coming of age'[1] With ongoing processes of digitalisation, boosted by the global pandemic, cyber threats are increasingly recognised as a key element to be considered in strategic approaches to understanding risks at all societal levels worldwide. The global pandemic and the fast-paced digitalisation stemming as a direct result thereof, featured as two key trends (re)shaping the modus operandi of public institutions and the private sector. Posing as the two major drivers of venturing into the digital sphere, these effectively led to a growing number of stakeholders exposed to an expanded range of cybersecurity threats and attacks.[2]

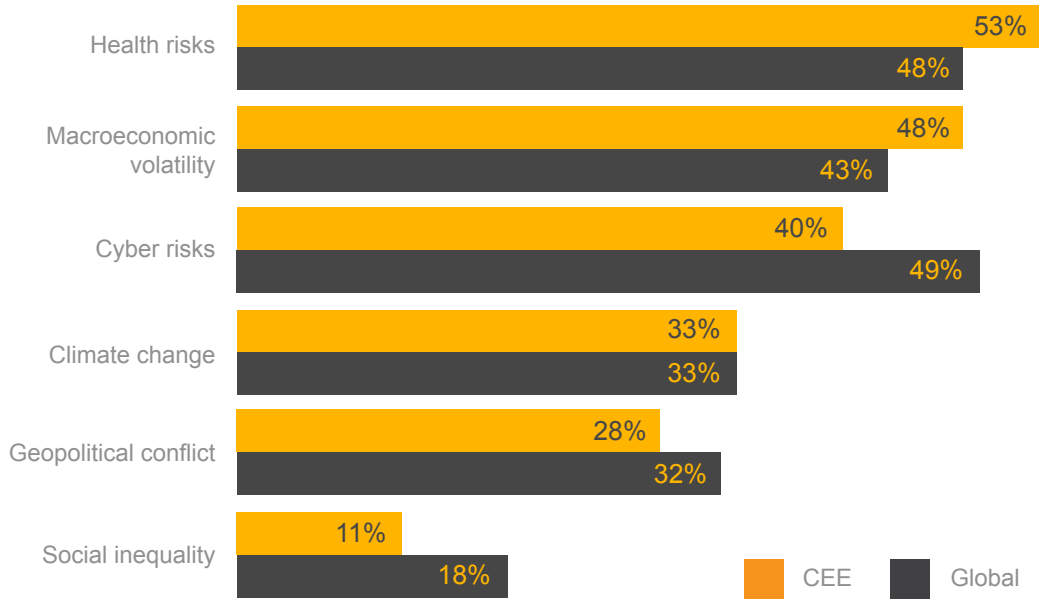


Figure 1. CEE CEO level of concern about global threats in the next 12 months[3]

Overall, 2021 has seen a general rise in global cybersecurity threats with ransomware being the most prominent one, alongside supply chain compromise, the leveraging and exploitation of zero-days[4] and commercial espionage, with a growth

1 Global Digital Trust Insights. 2021. PwC. https://www.pwc.com/jg/en/publications/digital-trust-insights.html

2 ENISA Threat Landscape. 2021. European Union Agency for Cybersecurity. Simplifying cybersecurity. 17.02.2021. PwC. https://www.pwc.com/gx/en/issues/reinventing-the-future/take-on-tomorrow/simplifying-cybersecurity.html

3 Central and Eastern Europe: The new equation for leadership in CEE. 25th Annual Global CEO Survey: Reimagining the outcomes that matter. 2022. PwC. https://www.pwc.com/c1/en/25th-ceo-survey-cee.html

4 Vulnerabilities in a piece of software that are not publicly known yet.

in targeting of civil society by espionage-motivated threat actors. Looking at a high-level regional breakdown, this shift has been strongly recognised in Central and Eastern Europe (CEE) as well. Threat perceptions have rapidly evolved in CEE, from failing to recognise cyber among the five top tier threats in 2020[5] to having cyber threats taking a prominent third place just a year later. This trend mirrors perceptions at the global level, where risks and threats stemming from cybersecurity have only strengthened their position as a priority source of concern.

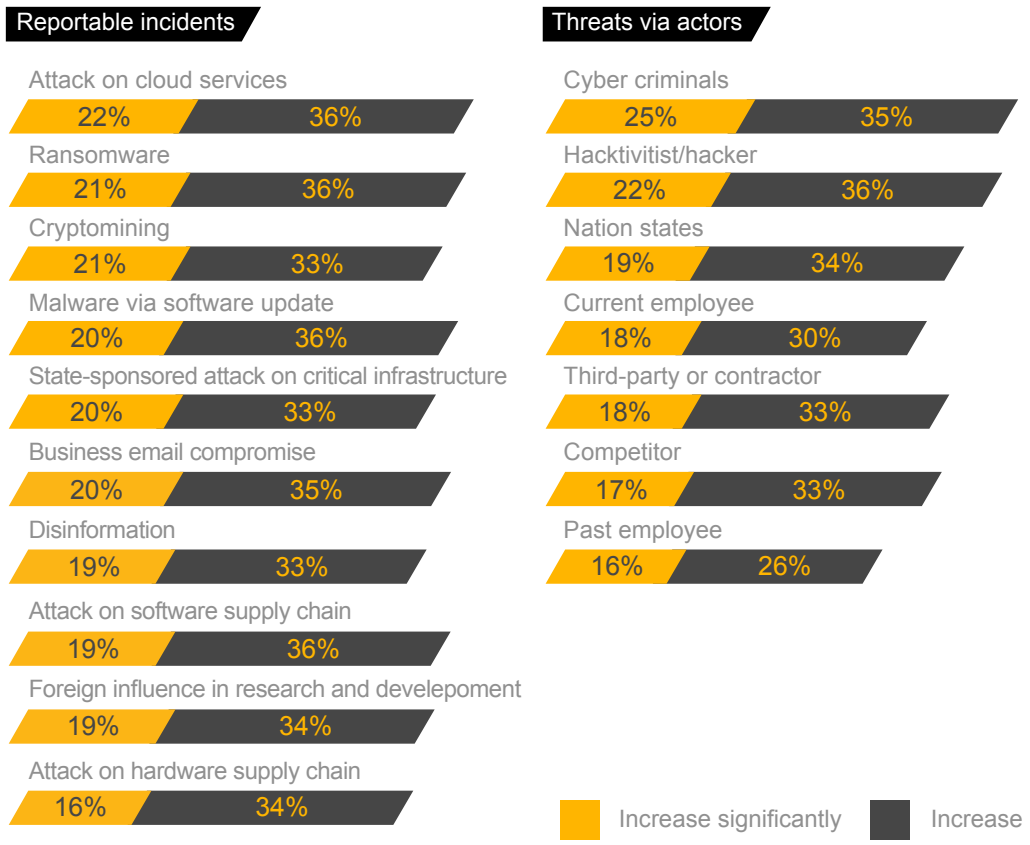


Figure 2. The 2022 threat outlook[6]

Having witnessed a tide of phishing campaigns, ransomware infections, supply-chain attacks and a general rise in cybercrime over the last year, these concerns are well-founded. As a result, expected trends in 2022 when it comes to incident types see continued presence of ransomware, malware and business email compromise, in addition to new developments fuelled by digitalisation, such as attacks on cloud services and cryptomining incidents. In terms of threat actors,

5 24th Annual Global CEO Survey: A leadership agenda to take on tomorrow. 2021. PwC. https://www.pwc.com/gx/en/ceo-survey/2021/reports/pwc-24th-global-ceo-survey.pdf

6 Global Digital Trust Insights Survey: The C-suite guide to simplifying for cyber readiness, today and tomorrow. 2022. PwC. https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html

cyber criminals are expected to remain at the top of the list, closely followed by hackers and hacktivists.

Bringing this down to the Western Balkans, wider global campaigns and attack methods are found only laterally affecting the region. More specifically, apart from one directly targeted attack, most of the identified threat actors and malicious activities recorded at the global level have been focused on targets elsewhere or launched globally distributed attacks with Western Balkan economies merely 'falling into the net' of these. The recorded frequency, identified or assumed threat actors and attack types are also relatively equally distributed across the Western Balkan economies, providing no indication of systematic targeting of any specific regional actor. This mirrors the overall perceptions of regional stakeholders interviewed for the purpose of this report - that the cybersecurity threat landscape of the Western Balkans is quite similar to global developments in terms of risks, challenges and attack types, with no specific interest of major threat actors for targets in the region recorded to date. This is further elaborated in the chapters that follow.

Global trends in the Western Balkans

In May 2020, a **phishing campaign** assessed as likely to have been run by a threat actor tracked by PwC as Blue Athena (a.k.a. Fancy Bear, APT28, Sofacy, Strontium) was recorded. The campaign has been targeting the government departments of several countries across the world, in most cases targeting specifically ministries of foreign affairs and defence. A phishing email containing a link to a phishing page has been discovered mid-2020, which appears to have been sent from a foreign affairs ministry of a West European country. Many different phishing pages for various government departments have been subsequently identified, including one for a Western Balkan Ministry of Foreign Affairs. Each phishing page was set up in a similar way, with the genuine web resources copied from the legitimate page and used to present a realistic looking phishing form. This is a shift in approach for Blue Athena, which commonly relied on malicious documents to deliver bespoke malware, mirroring a wider trend, where some espionage-focussed threat actors are gradually moving away from attacks that rely on bespoke malware and have begun implementing more open-source or off-the-shelf penetration testing tools to achieve their goals.[7]

In March 2021, a threat actor tracked by PwC as Red Dev 3 continued its standard form of operations based on developing **phishing pages** imitating legitimate mail services of its targets. Close to seventy domains have been assessed as highly likely attributed to Red Dev 3, highly likely intended to spoof legitimate organisations, including NGOs, ministries of foreign affairs in a number of countries across the globe, as well as the Government of one Western Balkan economy.[8]

7 Ministry of Foreign Bears. PwC Threat Intelligence. CTO-TIB-20200924-01A.
8 Red Dev Redemption 3. PwC Threat Intelligence. CTO-TIB-20210401-01A

In June 2021, **phishing campaigns** attributed to a Russia-based threat actor tracked by PwC as Blue Dev 5 have been identified as affecting ministries of foreign affairs in both Eastern and Western Europe, including also two Western Balkan economies. In one case, analysed entries indicate the use of local themes in at least one spear-phishing campaign affecting one of the Western Balkan economies. Another case saw the use of common phishing TTPs in the form of a fake invitation from a West European Ministry of Foreign Affairs for a humanitarian event in that country. Acting as a simple social engineering device, the message sent to targeted stakeholders, including one Western Balkan economy, thus encouraged the potential victims to respond – that is, to open a malicious file – relatively quickly.[9]

In December 2021, a threat actor tracked by PwC as Blue Odin was found **using infrastructure** (servers) located in one Western Balkan economy, among other countries, as part of its infrastructure to upload documents. All of the identified documents were uploaded by a source located in Ukraine, and likely located in Luhansk, with one of these uploaded from a source in the Western Balkans. Its themes pertain to the Nord Stream 2 natural gas pipeline.[10]

Attacks identified as highly likely motivated by **espionage** related to defence information, have been recorded as unfolding in the cyber domain throughout 2021. The attacks, targeting government entities in general, and the ministries of defence and interior specifically, in two Western Balkan economies have seen the use of phishing campaigns, weaponised documents, website compromise and a previously unobserved backdoor. In addition to public sector institutions, the attacks also seem to have been targeted at specific companies, one at an intermediary for the import and export of defence-related equipment, another at a security research and development organisation. These have been assessed as likely associated with a threat actor tracked by PwC as White Tur, whose activities have been recorded since 2017.[11]

The use of **spyware** has also been recorded during 2021, affecting stakeholders in several Western Balkan economies. Namely, open-source reporting has identified an Israel-based cybersecurity company called Candiru, tracked by PwC as Grey Mazzikim (a.k.a. SOURGUM), selling highly sophisticated spyware to customers around the world which has been seen being used to target civil society members in an abuse of the tool's reported intentions, while also being leveraged against classical espionage targets as intended. Pivoting on Grey Mazzikim infrastructure over seventy domains have been identified as highly likely associated with the private sector company and its customers, including threat actors tracked

9 Blue Dev 5 – The Roots of Targeting. PwC Threat Intelligence. CTO-TIB-20210608-01A.

10 Hunting Blue Odin Servers. PwC Threat Intelligence. CTO-TIB-20211215-01A.

11 (Darth) Vladars under attack Part 1. PwC Threat Intelligence. CTO-TIB-20210310-01A.
(Darth) Vladars under attack Part 2. PwC Threat Intelligence. CTO-TIB-20210423-01A.
(Darth) Vladars under attack Part 3. PwC Threat Intelligence. CTO-TIB-20210903-01A.

by PwC as White Dev 87 and White Dev 88. The pivots show targeting of both civil society and organisations aligning with various state interests, along with a focus on the Middle East and Europe. The spyware is alleged to have been targeted at over 100 individuals, many of whom are human rights defenders, dissidents, journalists, activists, and politicians. Affected stakeholders include an investigative reporting organisation operating across several Western Balkan economies, but also international organisations, such as the Energy Community. Additionally, it is highly likely that both White Dev 16 (a.k.a. SandCat) and Grey Turul (a.k.a. Stealth Falcon, FruityArmor) are or at least have been customers of Grey Mazzikim. Candiru itself is almost certainly not the threat actor targeting specific victims, but the supplier of malware and exploits to governments that have been observed to abuse these capabilities for self-interest, while victimising civil society who attempt to hold these same governments accountable for their actions. Since Candiru is a primary supplier for multiple threat actors throughout the world, the complexity and scale of these attacks is quite extensive.[12]

12 Another commercial quartermaster. PwC Threat Intelligence. CTO-TIB-20210806-02A.

Regional trends in the Western Balkans

An analysis of cybersecurity ecosystems of Western Balkan regional economies finds cybercrime dominating the threat landscape, with malware, phishing, ransomware and, to an extent, Distributed Denial of Service (DDoS) as the most common attack types. Ongoing processes of digitalisation, fuelled by the global pandemic, have widened the risk perimeter and led to a steady increase in the number of incident reports received by national competent authorities. Increasingly, smaller actors such as small and medium enterprises, media actors and civil society organisations also experience challenges stemming from cyberspace. Attacks methods have grown in sophistication, with better tailoring of malicious content to local languages and context.

The following subsections provide an in-depth analysis of the current state of affairs, perceptions thereof, and expected developments in the cybersecurity ecosystems of each Western Balkan economy and the region as a whole. With the exception of the geopolitical context and trends related to officially reported incidents, all elements pertaining to the threat landscape have been developed solely on the basis of data and information obtained through interviews with relevant stakeholders from each respective regional economy and official reports of competent authorities.

Albania

Geopolitical context

Cybersecurity developments in Albania are predominantly influenced by the country's dedication to cooperation with NATO and EU integration. Namely, in 2013, USAID supported the establishment of the Albanian national CERT (at the time, ALCIRT, succeeded by AKCESK)[13]. At this nascent stage, and as a new member of the NATO Alliance, Albania also signed a Memorandum of Understanding on Enhancing Cyber Defence with the NATO Cyber Incident Response Centre (NCIRC), adopted the Enhanced Cyber Defence Policy, and committed to advance its national cyber defence capabilities in line with the Wales (2014) and Warsaw (2018) Summit conclusions. The overall cybersecurity framework is based on EU and NATO standards, and Albania is committed to continuing this trend, as stated in the 2020 National Cybersecurity Strategy which reiterates the importance of international cooperation and the central role of NATO and the EU in this sense[14]. The document also outlines Albania's ambition to be a regular partner in joint cybersecurity initiatives led by these two organisations.

Additional plans include setting up a Cyber Defence Unit at the Ministry of Defence, with the support of the US and within the NATO framework aimed at providing protection not only to government entities, but also to private companies and individuals.[15]

It should be noted that no significant changes took place between 2013 and 2020, with the above mentioned National Cybersecurity Strategy posing as the first official overarching strategic document in this field, adopted in 2020.

Other avenues of international support include cooperation of Albanian national authorities with UNICEF and the OSCE on projects focused on improving cyber hygiene and fighting cybercrime, respectively. Albania is a signatory of the Council of Europe (CoE) Budapest Convention on Cybercrime and is also engaged in the CoE iPROCEEDS project, aimed at strengthening the capacity of authorities in the IPA region[16] to search, seize and confiscate cybercrime proceeds and pre-

13 USAID completes project to support Albania's new cyber incidents response agency. 2013. USAID. https://2012-2017.usaid.gov/albania/press-releases/usaid-completes-project-support-albania%E2%80%99s-new-cyber-incident

14 Decision no. 1084, dated 24.12.2020 on adopting the National Cybersecurity Strategy and its Action Plan 2020-2025. Official Gazette of the Republic of Albania 2021(7), pp. 14-15.

15 Albania to Launch Cyber Defence Unit to Tackle Growing Online Threats. 13.07.2021. Exit News. https://exit.al/en/2021/07/13/albania-to-launch-cyber-defense-unit-to-tackle-growing-online-threats/

16 Countries in the EU enlargement region that are beneficiaries of EU financial and technical assistance through the Instrument for Pre-accession Assistance (IPA).

vent money laundering on the Internet, and is currently a member of its subsequent, iPROCEEDS2 phase. Albania is a signatory of the Clean Network initiative led by the US.[17] Finally, as stated by President Ilir Meta in 2019, Albania has an interest to join the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia.[18]

When it comes to bilateral cooperation, Albania's national CERT has formalised channels of cooperation through Memorandums of Understanding with Kosovo, North Macedonia and Romania, focused on international cooperation.[19] Its primary counterpart in the region is Kosovo, with which it has also concluded an ICT Cooperation Agreement in 2013, and has regular expert exchanges and joint initiatives[20]. The national CERT is an accredited member of the Trusted Introducer community of CERTs.

According to publicly available information, the research conducted for the purpose of this report has not identified any contacts or established cooperation channels that Albania has on cybersecurity matters with China or Russia.

Threat landscape

Existing risks and threats	Attack types	Anticipated trends
• Increased sophistication of attacks • Rise of business-oriented attacks • Legacy software • Lack of enforcement mechanism • Limited human capacity	Spam Malware Phishing Email spoofing	• Digitalisation-related risks • Identity-based attacks **Identified needs** • Cybersecurity education • Sectoral capacity-building • Better information sharing

Existing trends

Information on incidents is obtained via two channels. The first includes those officially reported by critical information infrastructures (CIIs), which account for 20-30 reports per annum. The second method refers to identifying risks and in-

17 Albania Joins US 'the Clean Network', Pledges Not to Use Huawei 5G. 13.08.2020. Exit News. https://exit.al/en/2020/08/13/albania-joins-us-the-clean-network-pledges-not-to-use-huawei-5g/

18 President of Albania Ilir Meta paid a visit to the NATO CCDCOE. 2019. NATO CCD CoE. https://ccdcoe.org/news/2019/president-of-albania-ilir-meta-paid-a-visit-to-the-nato-ccdcoe

19 A list of publicly available documents is provided in Annex A.2.

20 Albanian Cyber Academy. 2017. AKCESK. https://cesk.gov.al/publicAnglisht_html/aktivitete/acy.html

cidents from different threat intelligence sources, which results in detecting 600-700 incidents per annum.

In terms of attack types, Albania seems to mirror general global trends. Both public and private sector stakeholders interviewed for the purpose of this report cite spam, malware, phishing and social engineering as most common. Email spoofing has also been on the rise in the previous year, using a solid level of Albanian language and mimicking email signatures.

The global pandemic forced a 'blast of digitalisation', meaning that a number of stakeholders entered the digital sphere of remote work and online transactions without any prior experience in cybersecurity hygiene, knowledge of safe conduct and procedures or supporting tools. As a result, business-oriented cyber attacks, targeting companies and end-users have also increased.

In general, a higher degree of sophistication of attacks has been noticed, as the pool of attackers is no longer limited to amateurs. Consequently, this rise of professional cyber criminals means that identifying potential targets is no longer straightforward – everyone can be targeted regardless of whether they belong to the public or private sector, or how big or small they are.

Identified risks and threats

From a **governance perspective**, some interviewed stakeholders see risks in the unaddressed need for enforcement mechanisms to ensure that the legislative and strategic documents in place are actually implemented. In practice, with no compliance management in place, interviewees see this translating into a lack of responsibility of relevant actors to implement specific actions within their jurisdiction, as there are no consequences for inaction.

To a certain extent, this also affects the extent to which the potential of multi-stakeholder approaches can be utilised. Although undoubtedly recognised as a necessary element of establishing comprehensive cybersecurity ecosystems and resilient societies, interviewees highlight that someone still needs to own the process – a framework needs to be in place determining who makes the final decision, who gives out orders, and who implements agreed actions.

Capacity-wise, interviewees list emigration of skilled workforce as one of the biggest risks for Albania, and the Western Balkan region in general. This trend of losing skilled workforce is especially concerning in light of fast-paced digitalisation of Western Balkan societies, and expectations that as a result of this process, regional economies will become more interesting to malicious actors in cyberspace. Lack of capacity is also mentioned as a limitation for keeping up with processes unfolding at the higher, EU-level, most notably in terms of alignment

with the EU Network and Information Security Directive (NIS Directive)[21] and the expected NIS 2.0[22].

From a more **technical aspect**, existence of legacy software in large and complex ICT environments which are difficult to change is seen as a source of risk. The lack of necessary patches, updates and support means that large systems used in critical sectors are left vulnerable.

Although no specific large-scale incidents at the national level were highlighted by the interviewees, common listed threats include ransomware and zero-days attacks. According to media reports, several large-scale data leaks took place in the country in 2021.

Regional specificities

There is no awareness of any region-specific APTs, which interviewees attribute to the fact that operating high-scale sophisticated attacks is expensive, making larger countries a more obvious target. There is also no evidence or perception of state-sponsored attacks targeting Albania. The possibility of identifying potential region-specific cyber criminal groups in the future has been mentioned however, but this exercise is seen as necessitating some form of a (regional) malware analysis centre in order to enable proper inspection and attribution.

In terms of attack vectors and types, interviewees agree that no significant difference from global trends and developments can be identified. As highlighted by one interviewee, launching a malware attack does not require any country or region-specific tailoring, as malware will be equally efficient in attacking computers in the Western Balkans as it is anywhere else in the world.

Personal data leaks

In December 2021, prosecutors in Tirana commenced a verification process, reportedly hours after a massive data breach of citizens' private information was circulated online. The data contained the salaries, job positions, employer names and ID numbers of some 630,000 citizens, from both the public and private sectors.

Further investigation led to the conclusion that the systems were not hacked - rather, two IT technicians, working at the state tax office stole the information and sold it to two undisclosed persons. All four were afterwards arrested, without disclosure of further information.

As an immediate response, the Albanian government signed a contract with the US-based Jones Group International aimed at "strengthening the security of digital systems".

Earlier in the year, and days before the April elections, a database containing private information of around 910,000 voters in Tirana, including names, addresses, birth dates, personal ID cards, employment information and other data, was leaked to the media.

21 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

22 Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. COM/2020/823 final.

Finally, despite the tendency to explore the possibilities of developing a specific approach to the Western Balkans, one interviewee underlined that all countries in the region face the same threat actors and attack-types as found in global trends. To this end, the argument made is that instead of developing a cybersecurity path for the region, focus should be placed on supporting Western Balkan economies in becoming part of global communities of practice to be able to respond to common cyber risks and challenges.

Main cooperation and support patterns

At the regional level, Albania has operational cooperation mechanisms in the form of Memorandums of Understanding between the Albanian national CERT and the national CERTs of Kosovo and North Macedonia, with an MoU with Serbia's national CERT pending. Additional MoUs are in place with the national CERTs of Romania and Cyprus.

Formalising such cooperation is recognised as challenging sometimes for several reasons, most of which are caused by common rules of procedure and protocols in place. For example, the research team was informed that differences in the position/level of competent authorities hosting national CERTs within the overall national cybersecurity framework (e.g. competent ministry vs. regulator) have thus far prevented Albania's national CERT in concluding certain MoUs with regional peers. Nevertheless, interviewees consider Albania's technical cooperation in cybersecurity as satisfactory, reaching further than the Western Balkan region, citing positive examples of cooperation and information exchange with several EU countries.

Cooperation with dedicated European and global CERT and technical communities is also utilised by the national CERT, primarily through its membership in FiRST and Trusted Introducer, and established relations with the Shadowserver Foundation.

Anticipated trends

The process of digitalisation in Albania, as observed across Western Balkan societies, is seen as one of the greatest potential cybersecurity risks in the near future, with a rise in digitalisation-caused threats expected by interviewed stakeholders. Possible targets are numerous and primarily identity-based (i.e. focused on personal data), given the expanding presence and use of tools such as electronic IDs, vaccine certificates, prescriptions, receipts, where, for example, man-in-the-middle attacks are seen as potentially having serious consequences.

Preparing for such upcoming trends, Western Balkan countries are faced with the risk of limited capacities, especially in the public sector. Although this is a common global challenge in cybersecurity, interviewees argue that the situation is more alarming in the region compared to Western Europe, when accelerated migration flows of skillful professionals from the Western Balkans towards the open and expanding EU market are also taken into account.

In order to respond to forthcoming cyber risks, interviewees argue that Western Balkan economies need to further develop their capacities to recognise threats, and invest more into both people and technology. From a high-level, long-term perspective, this means adequate cybersecurity education needs to be offered, especially to younger generations, in order to ensure capacities for the future. Currently, interviewees cite a lack of investment into educating future, and recruiting existing, professionals to support digitalisation processes, with very limited security-focused content being taught at the academic level.

In the mid-term, this means adopting a sectoral approach to strengthening national cybersecurity capacities in Albania and across the Western Balkans alike. This is an approach that Albania is already pursuing after rightfully recognising that, even if existing limitations in terms of human capacities in competent authorities are mitigated, the pure breadth of the cybersecurity risk and threat landscape still means that no single actor can respond to all incidents at the national level. Instead, developing sectoral pockets of capabilities, coordinated and supported at the national level in terms of information and knowledge sharing is recognised as a precondition for building greater national resilience, at the same time avoiding potential bottlenecks caused by centralised frameworks.

Finally, as a necessary measure that can be addressed in the short-term, interviewees describe information sharing pertaining to cybersecurity threats and incidents at the national and regional level as still somewhat limited for a number of reasons – mistrust, doubts regarding the balance between potential sanctions and potential benefits, reputational concerns – and highlight that having the right information in the cyber era is pivotal. Without it, wrong decisions will be made which could lead to far-reaching consequences.

Bosnia and Herzegovina

Geopolitical context

The complex political landscape in Bosnia and Herzegovina, has thus far hindered developments related to establishing an overarching cybersecurity framework. At the national level, there is no legislative or strategic framework, nor is there a national CERT, limiting also the country's potential for broader international cooperation in this field.

The situation at the entity level finds Republika Srpska with an established body – an entity CERT (CERT RS), within the Ministry of Scientific and Technological Development, Higher Education and Information Society. CERT RS is an accredited member of the Trusted Introducer community of CERTs. The entity has a Law on Information Security and a Strategy for the fight against cybercrime (for the period 2019-2023), with its Ministry of Interior also quite active in this field. The baseline structure of the current cybersecurity framework is generally in line with EU principles. As for the Federation of Bosnia and Herzegovina, the cybersecurity structure has not yet been established, although a Draft Law on Information Security has been prepared by the Federal Ministry of Transport and Communications, with additional plans to establish an entity CERT in the near future.

International support, spearheaded by the Council of Europe and the OSCE, has focused on promoting suitable cybersecurity policies and strategies. Like most countries in the region, Bosnia and Herzegovina is a signatory of the Council of Europe (CoE) Budapest Convention on Cybercrime and is engaged in the CoE iPROCEEDS project, aimed at strengthening the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet, and is currently a member of its subsequent, iPROCEEDS2 phase.

According to publicly available information, the country has only a handful of international agreements that contain cyber aspects, focused primarily on police cooperation and the fight against cybercrime. These include agreements with the Czech Republic, Saudi Arabia and Ukraine. There are also two international cooperation documents on ICT, with Croatia and Turkey.[23]

Officially a NATO aspirant country, Bosnia and Herzegovina is a member of the Partnership for Peace, and also participates in the NATO Science for Peace and Security (SPS) programme. Within the SPS programme, scientists and other experts from Bosnia and Herzegovina have engaged over the years in various cooperation programmes, including cooperation on 'exploring common solutions to security challenges in the areas of cyber defence'.[24]

---

23 A list of publicly available documents is provided in Annex A.2.

24 Bosnia and Herzegovina discusses new areas of scientific cooperation with NATO. 19.05.2017. NATO. https://www.nato.int/cps/en/natohq/news_144045.htm

The only non-Western power that is heavily involved in ICT-related projects and initiatives in Bosnia and Herzegovina is China. Given the relative weakness of central powers mentioned above, China's cooperation channels are much more focused on the entities and cantons. The only large-scale event that took place at the national level was the Third China-Central and Eastern European Countries (CEEC) Conference on Innovation Cooperation held in Sarajevo in 2018.

In terms of infrastructural support, the Ministry of Communications and Transport of Bosnia and Herzegovina signed an agreement with Huawei that includes technical support to the country's 'Smart City' and 'Safe City' projects.[25] In addition, in the sector of telecommunications, all three leading telecoms in Bosnia and Herzegovina cooperate with Huawei namely, BH Telekom, HT Eronet, and M:Tel (in majority ownership of Serbia's Telekom). All of these also consider Huawei as a potential partner in implementing the 5G network in the future.

Huawei is also active in supporting the academic sector, with Bosnia and Herzegovina taking part in its flagship corporate social responsibility programme titled 'Seeds for the future', alongside North Macedonia and Serbia. Launched in 2020, the programme is focused on providing young leaders in IT technology with new skills, knowledge about Huawei's 5G solutions, cybersecurity, AI, with a specific lens related to Chinese culture.[26] Annually, ten students are selected to take part. This is not the first time that the Chinese company has supported IT students and invested in future capacities, as Huawei has had a growing presence in Bosnia and Herzegovina since at least 2011, when it first started offering scholarship programmes for students of different universities from across the country.[27]

Federation of Bosnia and Herzegovina

At the above-mentioned 2018 China-CEEC Conference on Innovation Cooperation, representatives of Bosnia's capital Sarajevo and Huawei signed a cooperation agreement to facilitate the implementation of the 'Smart City' project in this town.[28]

In 2019, Huawei signed an Agreement on cooperation in the field of information and telecommunication technologies with the University of Mostar and included the students of this university in the mentioned 'Seeds for the Future' programme.[29]

---

25 Vladisavljev, S. June 2021. China's 'Digital Silk Road' Enters the Western Balkans. Choice. pp.14.

26 *Ibid*.

27 Huawei approves scholarships for students from BH. 24.05.2010. eKapija. *(article in BCS)* https://ba.ekapija.com/news/316339/kompanija-huawei-odobrila-stipendije-za-studente-iz-bih
Overview of activities in 2014. University in Banja Luka. *(content in BCS)* http://unibl-test.etf.rs/sr-lat/saradnja/pregled-aktivnosti-2008-2015/pregled-aktivnosti-za-2014-godinu

28 Vladisavljev, S. June 2021. China's 'Digital Silk Road' Enters the Western Balkans. Choice. pp.14.

29 Agreement on cooperation between the University of Mostar and Huawei signed 09.04.2019. Vijesti.ba. *(article in BCS)* https://vijesti.ba/clanak/442281/potpisan-ugovor-o-suradnji-izmedju-mostarskoga-sveucilista-i-huaweia; University of Mostar students participate in

Republika Srpska

Republika Srpska has employed significant resources that it has at its disposal towards international cooperation.

According to the Minister of Interior of Republika Srpska, Dragan Lukac, the interior ministries of Russia and the entity signed a Protocol on Cooperation in 2015.[30] According to publicly available information, the two police forces have had many avenues of cooperation, including cyber. At least since 2016, there have been regular meetings and training courses in which Russian experts have taken part.

The entity's cooperation with China has been unfolding since Bosnia and Herzegovina's engagement within the 16+1 framework where, alongside other Central and Eastern European countries, different forms of cooperation have been pursued based on the framework set up by the Belt and Road Initiative. In 2015, the then Prime Minister of Republika Srpska, Zeljka Cvijanovic, signed a Memorandum of Understanding with Huawei on the construction of advanced ICT for the needs of the Government and the public sector of this entity as a whole. The Memorandum was a first step towards the agreement that was supposed to 'precisely define all issues and ways of cooperation'.[31] In December the same year, the then President of Republika Srpska, Milorad Dodik, visited China as a participant of an investment forum, announcing China's interest in pursuing new projects in the entity.[32] During his subsequent visit to Beijing in 2016, Dodik signed a Strategic Partnership Agreement between Huawei and Republika Srpska, which stipulated 'establishment of systems related to safe city and security and establishment of a separate ICT and IT technologies for the functioning of the Government'.[33]

Bosnia and Herzegovina's potential accession to the US-led Clean Network initiative was blocked by Dodik, who highlighted this in an address to the Republika Srpska National Assembly in 2021[34]. To this end, after meeting the Chinese ambassador to Bosnia and Herzegovina later that year, Dodik stated that 'any pos-

---

Huawei talent program "Seeds for the future 2021". 21.05.2021. Centre for Information Technologies, University of Mostar. *(article in BCS)* https://sumit.sum.ba/novosti/studenti-sveucilista-u-mostaru-sudjelovali-na-huawei-programu-za-talente-%22seeds

30 Moscow special forces will train police officers in RS. 05.04.2016. Radio Free Europe. *(article in BCS)* https://www.slobodnaevropa.org/a/moskovski-specijalci-ce-obucavati-policajce-u-rs/27656303.htmlx

31 Memorandum of Cooperation between Srpska and the Chinese company Huawei. 24.04.2015. Radio Television of Republika Srpska. *(article in BCS)* https://lat.rtrs.tv/vijesti/vijest.php?id=146755

32 DODIK: Chinese investors interested in investing in RS. 20.12.2015. eKapija. *(article in BCS)* http://website.ekapija.com/urs/page.php?id=1315465&lng=0

33 Partnership agreement signed with Huawei. 05.11.2016. Capital. *(article in BCS)* https://www.capital.ba/potpisan-sporazum-o-partnerstvu-sa-kompanijom-huawei/

34 Dodik: I gave instructions to all our embassy staff. 10.06.2021. Radio Free Europe. *(article in BCS)* https://www.slobodnaevropa.org/a/dodik-instrukcije-ambasade-bih-/31300599.html

sibility to monopolistically or selectively approach the procurement of equipment for the 5G network is unacceptable'.[35]

Finally, Republika Srpska has also developed cooperation with Israel, encompassing ICT and cyber related aspects, with strengthened links at government, parliamentary and local community level(s). Following initial contacts established in 2019, in 2020 Dodik agreed with representatives of the Israeli company 'Elta Systems' to establish a Cyber Academy in Banja Luka[36], signing a Memorandum on its establishment in May 2021.

Threat landscape

Existing risks and threats	Attack types	Anticipated trends
Lack of a legislative framework Lack of a central governing authority Limited human capacity Lack of awareness Growth of cybercrime	Phishing Ransomware DDoS Online fraud	Digitalisation-related risks Attacks on digital services
		Identified needs
		Cybersecurity framework Update of existing legislation Awareness raising Cybersecurity education More regional cooperation

Existing trends

The complex political and institutional setup in Bosnia and Herzegovina reflects on the country's cybersecurity landscape as well, resulting in fragmented and limited information on risks, threats and incidents. Without an overarching legislative framework governing the field and no central competent authority tasked at least with compiling and aggregating data at the national, entity, district and cantonal level, reporting and information sharing remains limited, preventing any meaningful and actionable insight into existing trends.

Currently, the only operational CERT is in Republika Srpska, monitoring the threat landscape for this particular entity, as well as CERT-like capacities in several institutions, such as the Ministry of Defence and the Central Bank. Private sector entities, such as telecom operators also have their own capacities to this end. However, without a central competent authority tasked at least with compiling and

35 Dodik: I gave instructions to all our embassy staff. 10.06.2021. Radio Free Europe. *(article in BCS)* https://www.slobodnaevropa.org/a/dodik-instrukcije-ambasade-bih-/31300599.html

36 Establishment of a Cyber Academy in Banja Luka agreed: Dodik and Rajčević with representatives of Elta systems from Israel. 15.09.2020. *(article in BCS)* https://www.novosti.rs/republika-srpska/vesti/917769/dogovoreno-osnivanje-sajber-akademije-banja-luci-dodik-rajcevic-predstavnicima-elta-sistema-izraela

aggregating data at the national, entity, district and cantonal level, reporting and information sharing remains limited, preventing any meaningful and actionable insight into existing trends.

According to one interviewee, publicly available reports from the Republika Srpska entity previously indicated that the financial damages caused by cyber incidents amounted to approximately 82 million BAM (approx. £35 million). In addition to a growth in ransomware attack targeting small and medium sized enterprises, an increased level of sophistication of DDoS attacks has also been recorded, targeting media outlets, portals and web pages of healthcare facilities. The entity is also witnessing a steady increase in cybercrime, with 96 criminal acts recorded in 2019, growing to 190 in 2020. In the first couple of months of 2021, this number was already sitting at 115. As for the Federation of Bosnia and Herzegovina, unofficially, there are five cyber attacks taking place on a daily basis on average, with an estimated 2 to 3 million BAM (approx. £1 million) of cyber-caused financial losses per annum.

Based on interviewees' input and media reports, the most common types of attacks include fraud, phishing emails, ransomware and DDoS. Ransomware is found to be mainly targeting the private sector and large enterprises, with instances in which the manufacturing industry has been compromised and disabled. The technical specificities of such attacks are not publicly disclosed.

Identified risks and threats

From a **governance perspective**, the complex political and institutional setup in Bosnia and Herzegovina is one of the key risks recognised by the interviewees, with state, entity, district and cantonal divisions and authorities lacking mutual communication channels. Coupled with inadequate legislation, these shortcomings limit the extent of operational exchanges and cooperation. As such, the underdeveloped cybersecurity ecosystem is seen as a potential vulnerability at the highest level, with isolated institutional islands, such as the CERT of Republika Srpska.

Capacity-wise, a general lack of cybersecurity capacities and awareness are recognised by interviewees as root causes of existing risks, seen as inextricably connected. Namely, while a lack of awareness at the operational level is a direct functional risk, a lack of general understanding of the threats stemming from the cyber sphere from the side of higher management prevents adopting a comprehensive strategic approach to capacity development or devising any meaningful guidance on the matter. Public sector employees in Bosnia and Herzegovina rarely receive sustained cybersecurity awareness training and dedicated cybersecurity exercises or drills aimed at standardising cyber secure practices are rare. Coupled with a general lack of human resources, especially in the public

sector, interviewees believe that 'smaller' public sector stakeholders are currently running without any meaningful capacities to protect themselves, let alone their constituents. When it comes to cybercrime, interviewees highlight that prosecutors too lack the knowledge and capacity to adequately tackle cyber-related cases. A further challenge is the lack of adequate legal tools to this end, as official definitions of what constitutes a criminal act still predominantly rely on traditional understandings of crime, failing to recognise its developing manifestations in cyberspace.

On the other hand, given Bosnia and Herzegovina's lower level of digitalisation compared to other Western Balkan economies, interviewees argue that the lack of vast digital databases used for comprehensive e-services keeps the country relatively 'off the radar' of large-scale threat actors. As a result, no large-scale cyber attacks have been cited, with small and medium sized enterprises considered as the most common victims of cyber threat actors. Apart from attacks on web pages of several public institutions such as the Ministry of Finance, the banking sector, and petrol stations, several interviewees agreed that one of the largest publicly reported incidents in recent years took place in 2020, affecting one of the largest municipalities in Sarajevo.

Centar Municipality, Sarajevo

In June 2020, unknown hackers have been reported targeting the Centar Municipality in Sarajevo. The register of births and deaths in the Federation of BH was attacked and the Federal Police Directorate voiced concerns that the central civil register on the entire Federation of BH could have been deleted.

Regional specificities

Interviewed stakeholders have no awareness of any region-specific APTs, especially any targeting Bosnia and Herzegovina, which they primarily attribute to the limited scope of established e-services. The entire region is considered too small to be of specific interest for large-scale organised cyber threat actors. Instances of publicly-known malicious actors operating from the region have mainly been linked to larger-scale global campaigns, such as the group of Macedonian nationals involved in the Cambridge Analytica scandal. Nevertheless, the entire region of the Western Balkans is recognised by interviewees as sitting on the potential 'route' of malicious online activities due to its geographic position, with activities of several groups from, for example, Bulgaria, Romania and Ukraine detected in the past.

Main cooperation and support patterns

At the national level, cooperation is scarce due to objective limitations explained above. There are plans to establish a network of CERTs in the future, expecting establishment of an academic CERT in addition to those already mentioned.

However, interviewees voiced their concerns that, in case of a serious incident taking place, disagreement regarding jurisdictions could arise, resulting in a lack of engagement of some stakeholders, and a need for external support.

Although cooperation channels are not formalised at the national level, there has been meaningful interaction among relevant stakeholders in the previous years, through events, training and drills organised both at the national and regional level(s). International support to this end has also been recognised by interviewees, listing UNDP, OSCE and USAID as some of the key stakeholders, in addition to the role of the EU Delegation to Bosnia and Herzegovina in supporting efforts to transpose the NIS Directive, establish links with ENISA and strengthen existing capacities.

Anticipated trends

Given the number of commenced and ongoing processes, interviewees expect 2022 to be 'positively turbulent' year, seeing the establishment of a more comprehensive cybersecurity framework in Bosnia and Herzegovina. If no unexpected turn of events takes place, there are hopes that the initial cycle of establishing digital services in both the public and private sector could also be completed by 2024.

Precisely because of such trends however, the scope of the future threat landscape is expected to grow proportionally, with cryptoware[37] and data breaches among the key anticipated risks identified by interviewees, in addition to other types of attacks on digital services. Another concern is that, based on the current state of affairs, the process of digitalising aggregated data of a variety of public institutions and bodies is embarked from a position of extremely low cybersecurity awareness in the public sector. For this reason, development of human capacities primarily in the sense of awareness raising is seen as one of the core tenets for preparing for the future.

Education is seen as one of the long-term measures for ensuring greater future resilience. Currently, cybersecurity as a topic is seen as leaning onto security studies and/or ICT. Interviewees failed to identify any Masters or specialist programmes in the entire Western Balkans that are specifically focused on educating future cybersecurity engineers. New curricula are seen as necessary in this sense, providing long-term and multi-disciplinary education, from technology and techniques to procedures and legislation.

37 A type of ransomware designed to encrypt important data without interfering with the basic functions of a given device.

From an operational aspect, establishment of greater public-private cooperation in cybersecurity is seen as inevitable, given the limited capacities of the public sector to deal with serious cyber attacks on its own. In this sense, public-private cooperation would ensure greater national resilience, with the possible outsourcing of some cybersecurity services in the short-term to mitigate the current institutional fragmentation.

With interviewees expecting Bosnia and Herzegovina and the region as a whole will continue to experience similar threats and attack types in the future, the need for improving cooperation among regional peers is highlighted. Fostering and practising communication among all regional actors is seen as a key ingredient for generating necessary cooperation and support channels to be utilised when a serious incident takes place. Internationally, the need for higher levels of cooperation with relevant EU institutions and bodies is recognised.

From a governance perspective, in addition to processes already underway, interviewed stakeholders highlight the need to perform regular reviews of the legislative and strategic framework to ensure these provide adequate tools for responding to the challenges stemming from cyberspace. This includes developing national legislation and procedures, establishing relevant contact points, and devising an action plan for critical infrastructure. In terms of fighting cybercrime, this further includes updating the penal code to recognise the different manifestations of cyber criminal acts, such as cyber bullying or revenge porn, for example.

Finally, comprehensive awareness raising targeting all segments of society, efforts aimed at establishing baseline cyber hygiene practices and developing more preventive activities aimed at citizens and private sector stakeholders are recognised by interviewees as the core building blocks for strengthening national resilience and preparing society for what the future threat landscape may bring.

Kosovo

Geopolitical context

The development of Kosovo's cybersecurity framework has been exclusively tied to cooperation with and support from the West, and is based on EU and NATO models and best practice. In 2015, the Government adopted the National Cybersecurity Strategy and Action Plan for the period 2016-2019. The second iteration of the national strategy as well as Kosovo's first Law on Cyber Security are expected in 2022.

International cooperation is primarily focused on Western allies. Certain challenges still remain as a result of Kosovo's status at the international stage following the declaration of independence in 2008. Consequently, Kosovo is prevented from participating in some of the most important international organisations, initiatives and conventions, with its European and Euro-Atlantic integration processes also blocked due to the fact that five EU Member States (out of which four are also NATO members) do not recognise it. Over the past several years, the United States has been supporting the development of a multi-stakeholder approach to cybersecurity in Kosovo[38], whilst the United Nations Development Programme has been focused on the development of structures and capacities for fighting cybercrime[39].

Kosovo engaged in the Council of Europe iPROCEEDS project, aimed at strengthening the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet, and is currently a member of its subsequent, iPROCEEDS2 phase. In addition, several public sector CERTs are listed members of the Trusted Introducer community of CERTs, including CERTs of the Kosovo Police and the Kosovo Security Forces, while the national CERT (KOS-CERT) is a fully accredited member.

Kosovo has signed the US-led Clean Network initiative. Through its version of the so-called 2020 'Washington Agreement', Kosovo also unilaterally committed to the US that it will remove 5G equipment provided by what have been defined as 'untrusted vendors' from its mobile networks and prohibit such vendors from partaking in any future projects in Kosovo's market.

38 US Embassy grant program to improve Cyber Security and Resilience in Kosovo. 31.05.2021. Funds for NGOs. https://www2.fundsforngos.org/latest-funds-for-ngos/us-embassy-grant-program-to-improve-cyber-security-and-resilience-in-kosovo/

39 Cyber Security in Kosovo in Hands of Young People. 28.06.2021. United Nations Kosovo Team. https://kosovoteam.un.org/en/133792-cyber-security-kosovo-hands-young-people

The potential for establishing bilateral cooperation is also challenging, and agreements covering cyber aspects are limited to the sphere of police cooperation with Albania, Bulgaria, Italy, Montenegro and Switzerland. The only bilateral agreement that is out of this sphere and contains provisions directly related to cyber is with Turkey, covering military and defence cooperation, although this agreement did not result in any significant cooperation, to date.[40]

Kosovo's strongest regional partner in cybersecurity is Albania, with which it has a standing ICT Cooperation Agreement and a Memorandum of Understanding on cooperation between the two national CERTs – Albania's AKCESK (former ALCIRT) and Kosovo's KOS-CERT.

Threat landscape

Existing risks and threats	Attack types	Anticipated trends
Lack of a legislative framework Lack of clear jurisdiction Limited reporting Limited capacities of critical infrastructure Limited human capacity	Phishing Malware Data theft Ransomware (limited) DDoS	Digitalisation-related risks **Identified needs** Sectoral capacity-building Public-private partnerships Awareness raising

Existing trends

Officially, not many incidents are reported to the national CERT. Interviewees find one of the possible reasons for this in the existing lack of resources and capacities within relevant constituents. Another is the potential lack of tangible benefits of reporting, and affected stakeholders prefering to solve incidents by themselves. Although reports on incidents from physical entities (i.e. individuals) are growing in total numbers, these are not within the jurisdiction of the national CERT. Reports are also received from other national CERTs, and these are coordinated and communicated further to relevant entities by KOS-CERT.

On average, three to four incidents are reported per month, mostly by other national CERTs (primarily from EU Member States). Additional information is obtained from CERT and experts communities, in cases when a general widespread threat is detected, or in instances when malicious activities are identified as potentially launched/directed from Kosovo.

40 A list of publicly available documents is provided in Annex A.2.

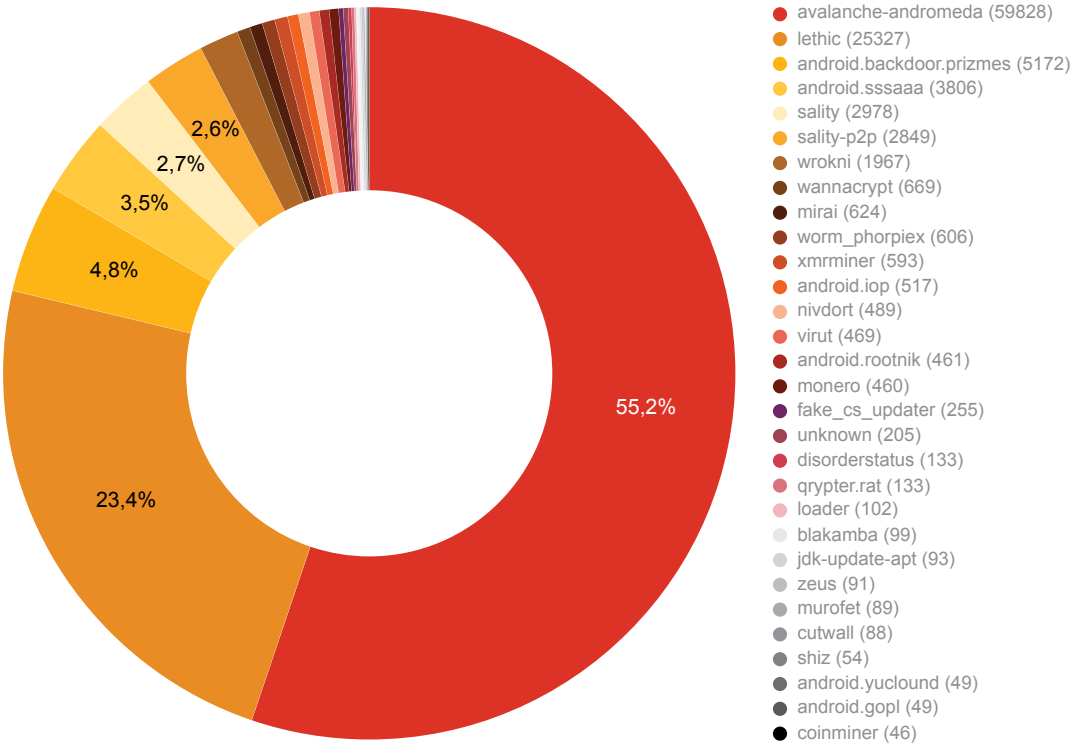


Figure 3. Number of IP addresses affected in 2020, by type of cyber infection[41]

Due to this limited number of reported incidents, the national CERT adopted a proactive approach, focusing on outreach efforts and plans to establish a public-private partnership to increase existing capacities through cooperation. Preparation of a Manual for incident prevention at the national level is also envisioned, aimed at increasing awareness and, hopefully, increasing the number of reported incidents as a result.

In terms of incident types, phishing emails, malware, data theft and, to an extent, DDoS attacks are most frequent. Phishing, which is most commonly recorded, predominantly targets private sector stakeholders and senior leadership. The financial sector is primarily targeted by ransomware although, according to interviewed stakeholders, the sector's capacity to respond to such threats is at a satisfactory level. DDoS attacks are usually directed at web pages and portals of public sector institutions.

Identified risks and threats

From a **governance perspective**, one of the key risks identified by interviewees is the lack of a comprehensive legislative framework at the national level which would clearly regulate jurisdictions of competent authorities and provide the le-

41 Annual Report 2020. National Cyber Security Unit (KOS-CERT). Regulatory Authority for Electronic and Postal Communications (RAEPC).

gal basis for imposing penalties for non-compliance (including failure to report detected incidents). Currently, existing sectoral legislation only covers Internet Service Providers (ISPs) although it also suffers from the lack of a legal basis for imposing an obligation to report incidents. The pending Law on Cybersecurity is expected to resolve some of the overlapping jurisdictions Kosovo currently suffers from, determining the overall institutional setup. The Draft Law envisions setting up a new Agency for Cybersecurity which should resolve some of these governance challenges.

From an **operational aspect**, the limited number of reports at the national level means that competent authorities are primarily dependent on international knowledge and information. Although the utilised open source feeds (such as Shadowserver, Team Cymru, etc.) provide relevant and timely information on a range of cybersecurity developments, this still means there is a general lack of grass-root information on trends, risks and incidents tailored to the national level. Consequently, efforts of competent authorities risk being mainly reactive, based on perceptions and a general awareness of existing capacities and systems nation-wide.

Banka Ekonomik

In April 2020, a variant of Bitpaymer ransomware has been reported to have hit the Ekonomik Bank in Kosovo, employing the recognised growing trend of data exfiltration in parallel. Namely, over 2GB of files with information of financial transactions and database backup files have been released by DopplePaymer, following the successful breach.

In this sense, the greatest risk identified by interviewed stakeholders lies in the limited technical and incident management capacities in critical infrastructure. Botnets, which have already been used for launching an attack on one ISP, are recognised among the key threats, commonly used for launching DDoS attacks which are most frequent at times of elections.

Regional specificities

Although the APTs detected in official reports have not been further categorised in terms of origin, interviewees highlight that there are no indications of region-specific threat actors. Kosovo, and the Western Balkan region as a whole, is generally seen as experiencing attacks coming from outside of the region, as part of greater global trends, and regional actors are not considered as the primary targets of these.

Official data confirms this, seeing attacks primarily originating from countries such as Belarus, China and Russia, with the region experiencing malicious activities of a global nature and spread. Even in instances where malicious activities have been traced back to the Western Balkans, these are not seen as large-scale campaigns of organised groups, rather as isolated actions of lone wolves, conducted by individuals.

Main cooperation and support patterns

The scope and intensity of bilateral regional cooperation from an operational standpoint varies. Kosovo's national CERT has signed Memorandums of Understanding with national CERTs of Albania and North Macedonia. The process of further formalisation of cooperation in the region is currently paused until the CERT's mandate is cleared with the mentioned legislative changes. There is also operational cooperation with Montenegro, whilst exchanges with Serbia have thus far been limited to information on detected malicious activities originating from Kosovo. Informal cooperation and exchanges have been supported through different projects implemented by international donors, fostering regional networking and communication.

Anticipated trends

Ongoing processes of digitalisation are recognised as one of the key threats in the years to come, especially when it comes to critical infrastructure. In order to mitigate these, one of the core approaches suggested by interviewees is building up sectoral capacities. No matter what the future holds, national CERTs will never be able to develop capacities that are broad enough to enable them to keep track of emerging technologies, identify existing and potential risks and threats, provide support in establishing prevention capabilities and incident mitigation capacities faced by all the different stakeholders making up the critical sectors of any one country. To this end, interviewees argue, focus should be placed on sectoral cybersecurity needs, in parallel to developing high-level national approaches. National-level competent authorities and CERTs should provide for coordination between sectoral CERTs and/or CERT-like bodies, building up their capacities and determining the overarching national framework, rules and procedures. On balance, interviewees argue, the more functional sectoral CERTs there are, the more the national cybersecurity ecosystem will be secure.

In this sense, public-private cooperation is seen as a key to success. In addition to the common reference that the majority of critical infrastructure is in private hands, this is also true in terms of technical expertise. Engaged cybersecurity expert communities have already made their mark in Kosovo, sharing knowledge, experiences as well as relevant threat intelligence when applicable.

Finally, the recurring topic of awareness raising is seen as a precondition for tackling existing and preparing for future developments in the cyber sphere. Limited capacities are acknowledged as an existing challenge globally, but are seen as an even bigger one in the Western Balkans due to the fact that senior managers and decision-makers still fail to recognise the extent of risks and threats that present-day cyber realities bring to the table.

Montenegro

Geopolitical context

Montenegro established its baseline cybersecurity framework and built initial capacities in coordination with the EU. In 2013, the country already had its first National Cybersecurity Strategy in place and fully embarked on the process of developing its cybersecurity framework. As such, Montenegro was in an excellent position to transpose the EU NIS Directive immediately after its adoption. The strategic framework was updated in 2018, with the adoption of the country's second National Cybersecurity Strategy.

On a bilateral level, Montenegro has a handful of police cooperation agreements that cover some aspects of cyber, with Bulgaria, the Czech Republic, North Macedonia, the Russian Federation and Switzerland, as well as a Memorandum of Understanding with the OSCE. All of these agreements are related to cybercrime.[42] There were also announcements regarding cooperation with Slovenia and its institutions on cybersecurity and cybercrime, and with Estonia.[43]

Like most countries in the region, Montenegro is a signatory of the Council of Europe (CoE) Budapest Convention on Cybercrime and is engaged in the CoE iPROCEEDS project, aimed at strengthening the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet, and is currently a member of its subsequent, iPROCEEDS2 phase. Montenegro's national CERT (CIRT.ME) has been a listed member of the Trusted Introducer community of CERTs since 2013, undergoing a re-enlistment process in 2019, and is also a member of the FiRST CERT community.

The pace and strategic choices related to the development of the cybersecurity ecosystem in Montenegro have primarily been influenced by geopolitical struggles in the region. Namely, Montenegro has shown a strong interest to cooperate with NATO vis-à-vis cybersecurity even before the country's membership in the Alliance, with its Membership Action Plan (MAP) including significant elements on cybersecurity. Events unfolding around the 2016 parliamentary elections, witnessing an attempted coup against the Government in power at the time which was reportedly conducted by pro-Russian elements and supported by simultaneous attacks in the cyber sphere, provided the final push for Montenegro to fully embed cybersecurity cooperation with NATO as the official national approach.[44]

---

42 A list of publicly available documents is provided in Annex A.2.

43 Krivokapić and Rataš: Estonia is a traditional friend and partner of Montenegro. 06.12.2021. Gradski portal. *(article in BCS)* https://gradski.me/krivokapic-i-ratas-estonija-tradicionalni-prijatelj-i-partner-crne-gore/

44 Montenegro targeted by cyber spies: From Russia with a virus. 05.03.2018. Balkan Insight. *(article in BCS)* https://balkaninsight.com/2018/03/05/crna-gora-na-meti-sajber-spijuna-iz-rusije-sa-virusom-03-01-2018/?lang=sr

Malicious cyber activities continued well into 2017, parallel to Montenegro's accession to NATO. Montenegro was the primary target of these coordinated cyber attacks which has been confirmed by the attack method employed. These included spear-phishing campaigns with malicious messages using weaponised documents to target civil servants, coupled with large-scale DDoS attacks targeting public institutions and civil society organisations, among others.[45] The attacks have later been attributed to the Russian-based group Fancy Bear, or APT28.[46] Since joining NATO in 2017, Montenegro has made significant steps towards developing its cybersecurity ecosystem and building up national cyber defences. Under the NATO umbrella, Montenegro has developed a schedule of long-term cooperation in ICT and cyber with the US, in line with the US Department of Defence Cyber Strategy, which foresees the pooling and sharing of resources in the cyber domain among partners and allies. In 2018, US Cyber Command Airmen, in cooperation with the US European Command, conducted Cyber Defence Security Cooperation with Montenegro, building up the country's cyber defence capabilities with an aim to 'increase interoperability, build partner capability, and deter malign influence on democratic processes'[47]. The same year, the Army of Montenegro, in cooperation with the Maine National Guard and the US Armed Forces Command in Europe (USEUCOM), hosted the international seminar 'Cyber Endeavour 3' in Podgorica.[48]

Anticipating new cyber attacks during the parliamentary elections in 2020, NATO deployed a counter hybrid team to Montenegro in late 2019/early 2020, to strengthen the country's capacities in deterring hybrid threats.[49] More recently, the United States Office of Defence Cooperation (ODC) in Montenegro has, through Foreign Military Finance (FMF) and with the use of the Countering Russian Influence Fund (CRIF), contributed to the further development of the cybersecurity apparatus.[50]

---

45 Russia's Strategy in Cyberspace. June 2021. NATO STRATCOM COE. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf

46 For the second time in a few months Montenegro suffered massive and prolonged cyberattacks against government and media websites. 22.02.2017. Security Affairs. http://securityaffairs.co/wordpress/56561/hacking/montenegro-cyber-attacks.html

47 US, Montenegro conduct groundbreaking cyber defence cooperation. 04.10.2018. Air Force. https://www.af.mil/News/Article-Display/Article/1653918/us-montenegro-conduct-groundbreaking-cyber-defense-cooperation/

48 Cyber experts from America have arrived. 02.10.2018. Mondo. *(article in BCS)* https://mondo.me/Info/Drustvo/a702442/sajber-kriminal-ekspert-USA.html

49 The Chairman of the NATO Military Committee announced that the alliance has sent a counter-hybrid team to Montenegro to face Russian hybrid attacks. 20.01.2020. Security Affairs. https://securityaffairs.co/wordpress/96627/cyber-warfare-2/montenegro-nato-hybrid-attacks.html

50 For example, Montenegro has been able to make use of two full-time cyber consultants in its Ministry of Defence for a duration of twenty months, working on cybersecurity and policy improvements. An additional USD 8 million was provided for cyber-relevant software and hardware upgrades. US and Montenegro strengthen security cooperation relationship. 22.07.2021. Defence Security Cooperation Agency. https://www.dsca.mil/news-media/news-archive/us-and-montenegro-strengthen-security-cooperation-relationship

Apart from direct cooperation with NATO, in 2019, Montenegro joined the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallin, Estonia, signing two memoranda to establish operations and functional relationships.[51] Finally, in 2019 Montenegro officially became a member of the European Centre of Excellence for countering hybrid threats, a network-based international and independent hub for practitioners and experts based in Helsinki.[52] Currently, Montenegro is the only member from the Western Balkans in both forums.

Outside of defence aspects, the US is among Montenegro's main partners in civilian matters as well. For example, the United States Embassy in Podgorica, in cooperation with Montenegro's Centre for Training of the Judiciary and the Prosecution, organised a cybercrime training for representatives of the State Prosecution and Courts and the Police in 2016.[53] In an effort to further enhance non-defence aspects of Montenegro's collaboration with the US, the acting Minister of Public Administration, Tamara Szrentic, recently held meetings with the US Digital Corps and other US companies to establish deeper cooperation on ICT and digitalization.[54]

Apart from the Western sphere, Montenegro's officials announced cooperation with the United Arab Emirates, which is to encompass cybersecurity.[55] While there is no record of concrete movements in this sense to date, the Montenegro Police and the Police of Dubai started work on a Memorandum of Understanding that should encompass cooperation against cybercrime, most notably training and education.[56] Montenegro is also a member of the Thailand-based Cybersecurity Alliance for Mutual Progress (CAMP).[57]

---

51 Montenegro to Join NATO Cyber-Defence Centre. 23.07.2018. Balkan Insight. https://balkaninsight.com/2018/07/23/montenegro-to-beef-up-cyber-defence-by-joining-nato-center-07-20-2018/

52 Montenegro and officially a member of the European Centre of Excellence for Countering Hybrid Threats. 23.05.2019. AntenaM. *(article in BCS)* https://www.antenam.net/politika/121209-crna-gora-i-zvanicno-clan-evropskog-centra-izvrsnosti-za-suprotstavljanje-hibridnim-prijetnjama

53 With US experts to better services for citizens. 27.10.2021. Radio Television of Montenegro. *(article in BCS)* http://www.rtcg.me/vijesti/drustvo/339391/sa-strucnjacima-sad-do-boljih-servisa-za-gradjane.html

54 Cyber Crime Training for representatives of State Prosecution, Courts and Police. 30.11.2016. US Embassy in Montenegro. https://me.usembassy.gov/cyber-crime-training-representatives-state-prosecution-courts-police/

55 Montenegro an important partner, ready to provide assistance to the police in the UAE. 13.10.2021. Radio Television of Montenegro. http://www.rtcg.me/vijesti/drustvo/337839/cg-znacajan-partner-u-uae-spremni-da-pruze-pomoc-policiji.html

56 Sekulovic and Brdjanin at a meeting with the director of the Dubai police. 16.11.2021. Ministry of Internal Affairs, Government of Montenegro. *(article in BCS)* https://www.gov.me/clanak/sekulovic-i-brdanin-na-sastanku-sa-direktorom-policije-dubaija

57 List of members. Cybersecurity Alliance for Mutual Progress. https://www.cybersec-alliance.org/camp/membership.do

Threat landscape

Existing risks and threats	Attack types	Anticipated trends
Frequent changes in governance structures and jurisdictions Legacy systems Limited human capacity Lack of awareness Lack of cybersecurity education	Malware Phishing Social engineering Identify theft Brute force DDoS	Digitalisation-related risks Increase in attacks on SMEs Continued growth of cybercrime
		Identified needs
		Greater engagement of international partners Capacity development Cybersecurity education Public-private partnerships

Existing trends

There is a growing trend in the total numbers of reported incidents to the national CERT (CIRT.ME). Currently, reports from citizens are most frequent, followed by public institutions, whilst reports on incidents from the private sector are still scarce, with the exception of the banking sector.

The composition of stakeholders reporting also reflects on the type of incidents officially recorded. Citizens commonly report hacked social media accounts as well as hate speech online. Such reports have grown in numbers with the Covid-19 pandemic. Malware is more common in reports coming from public institutions and bodies, in addition to a growing number of phishing campaigns targeting public and private stakeholders alike.

Private sector stakeholders generally agree with these officially identified trends, adding social engineering to the list of common attack types, alongside brute-force and DDoS attacks. When it comes to individuals, in addition to hacked accounts, identified incidents include identity and credit card theft.

Based on past experience, some of the interviewed stakeholders highlight that activities in the cyber sphere, apart from corresponding with general global trends, also reflect current political developments in the country, citing the example of the 2016-2017 malicious campaigns taking place in Montenegro's cyberspace.

There is general agreement that the actual number of incidents taking place is significantly higher, especially given the limited number of reports received from private sector stakeholders.

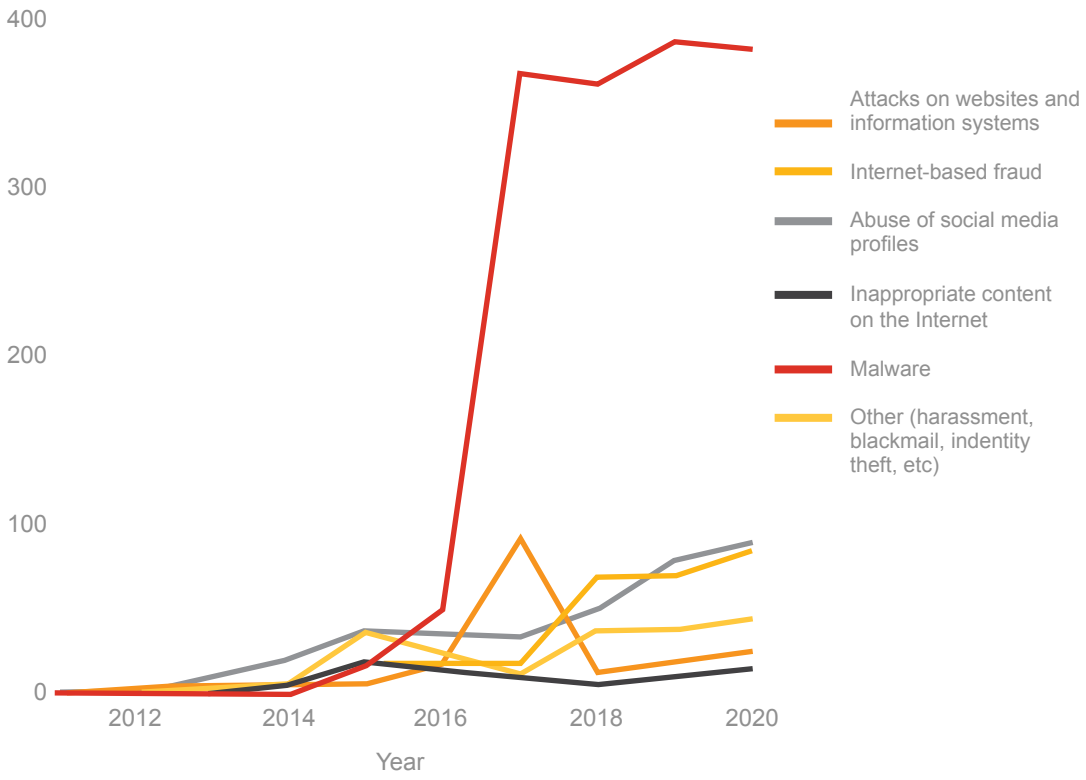


Figure 4. Incidents officially reported to CIRT.ME, by type[58]

Identified risks and threats

From a **governance perspective**, frequent changes in public institutions and bodies dealing with cybersecurity have been identified as a potential risk, with the existing framework seen as lacking continuity. Interviewees highlight that the governing structure has been downgraded from the former Ministry for Information Society to the level of a Directorate, with the national CERT displaced from the Ministry of Public Administration to the Directorate for the Protection of Classified Data following adoption of the Law on Classified Information. Some of the interviewees shared their impression that in the past several years, Montenegro has circled back to the very beginning when it comes to developing its national cybersecurity framework, shrinking its capacities from a wide array of cybersecurity mechanisms to maintaining the system at the level of mere existence.

From an **operational aspect**, legacy systems and equipment are listed as a key risk, especially in the public sector. Interviewees mentioned previously experienced difficulties when reporting incidents to the national CERT as a possible explanation for limited reporting by the private sector. In addition, limited capacities of CIRT.ME are seen as one of the root causes of the current lack of cross-sector communication at the national level. The lack of capacities is not seen as inherent

58 Data provided to the project team by CIRT.ME.

Coordinated campaigns throughout 2016-2017

October 16, 2016, the day of parliamentary elections, witnessed large-scale DDoS attacks launched against state web pages and digital infrastructure, as well as the websites of pro-NATO and pro-EU political parties, civil society webpages and electoral monitors. The same day, an attempted coup d'etat against Montenegro's government was taking place, later said to have been assisted by Russia's intelligence services. Several days later, a phishing attack was launched against the parliament of Montenegro.
The trend continued well into 2017 with an even larger DDoS attack recorded in February, compromising government and state institutions' web pages, as well as those of several pro-government media. In parallel, the Ministry of Defence reported being targeted by spear-phishing attacks. In June the same year, further cycles of similar attacks have been reported, in light of Montenegro's official accession to NATO.
Cybersecurity firms – FireEye, Trend Micro and ESET – attributed some of these attacks to APT28.

only in the public sector, as interviewees highlight that only large private sector stakeholders such as banks and telecom operators have the necessary resources to ensure adequate protection levels. Smaller businesses and those that are not directly in the ICT business, such as retail chains or construction companies, are seen as still quite vulnerable in the cyber sphere.

Further **capacity considerations** see a lack of awareness listed as one of the key weaknesses in Montenegro's cybersecurity ecosystem by interviewees, the consequences of which are manifold. With no strategic approach to resource planning, there is no continuity in human capacity development both horizontally and vertically. At the academic level, there are currently no dedicated cybersecurity programmes, despite positive examples in the past. At the expert level, events, workshops and training take place in an ad hoc manner and at irregular intervals. This means actions are of a reactive nature, resulting in limited investment in cybersecurity both in the public and private sector – until an actual incident takes place. Lack of awareness also means that in the process of digitalisation of services, both public and private, security aspects often get sidelined with an inconsistent approach to updates and patching of the systems and servers in place.

Although no specific threats or threat actors have been identified by the interviewed stakeholders, there is general agreement that although Montenegro is not a particularly interesting target on a global scale, certain malicious actors increase their activities in cyberspace at times of significant political events and developments.

Regional specificities

In general, interviewees agree that cybersecurity experiences of Western Balkan economies, Montenegro included, mirror global trends when it comes to incidents and attacks, with no particular regional specificities. The region as a whole is not considered to be of any significant interest to large-scale organised cyber criminal groups.

One regional specificity that has been highlighted however is the use of unlicensed software, which is seen as (still) common practice across the Western Balkans. In this sense, pirated software is recognised as a shared regional vulnerability.

Main cooperation and support patterns

Operational cooperation between CIRT.ME and other CERTs in the region is in place, with regular sharing of information pertaining to reports and inquiries regarding detected malicious IP addresses. CIRT.ME also has contacts with the Cypriot national CERT. Support received from the national CERT of Slovenia on several occasions when threats and incidents directed at specific sectors in the wider Western Balkan region have been detected was also highlighted by interviewed stakeholders.

Greater international support, primarily from European countries, is considered necessary. Apart from the obvious benefits of learning from peers who are more advanced in cybersecurity, some interviewees believe that guidance from, and joint projects with, external partners carry greater weight compared to local voices. This means, in their view, that greater engagement of international partners might provide a significant push for necessary developments in this field to take place more efficiently.

Anticipated trends

Interviewees anticipate a steady growth of attacks and incidents in the future. The process of digitalisation is seen as one of the primary sources of vulnerabilities that malicious actors might use to their advantage, with doubts expressed regarding current capabilities to secure digital services offered to citizens, both public sector and commercial. Small and medium-sized enterprises are considered as particularly unprepared for entering the world of e-commerce, with data theft, credit card fraud and similar challenges seen as possible risks in this domain.

Two specific near-future expectations were highlighted by interviewees:

- Fast-paced development of ICT solutions with insufficient attention paid to security aspects; and
- Continued reduction of public sector capacities in terms of human resources.

An increase in cybercrime is also anticipated, as the more ‘traditional’ criminal organisations realise the potential benefits of using the digital space for transferring and/or expanding their malicious activities into the cyber sphere. This is expected to bring a rise in blackmail and extortion, as well as purchases of illegally acquired accounts, credit card information, and other monetizable data.

In order to prepare for such developments, interviewees see the strengthening of existing capacities as a primary requirement. A step in this direction is seen in the announced establishment of a cybersecurity agency at the national level, gathering the human and technical resources of all relevant institutions in one place. In contrast to interviewees from other Western Balkan economies who see outsourcing of public sector capabilities as inevitable, stakeholders in Montenegro argued against such approaches. Namely, with cybersecurity requiring continuous engagement and monitoring, outsourcing is seen as an expensive option by some interviewees in Montenegro, who argue in favour of building up internal capacities instead.

An additional complementary approach suggested by some of the interviewees is to make greater use of academic capacities. The academic sector could support Montenegro's cybersecurity resilience by, for example, performing in-depth analysis of detected incidents based on data that was previously anonymised. This would ease the burden of the already strained competent authorities and provide more detailed information for deliberating the threat landscape.

Delving deeper into the possibilities of greater utilisation of academia, the need for a multi-disciplinary approach to developing future cybersecurity experts has been highlighted by interviewees. Close monitoring of trends and continuous adjustment is considered necessary to this end as well, given the pace of change in this field. Establishing close cooperation between private sector stakeholders and academia to this end is seen as a possible option for enabling development of wide skill sets, and putting these to practise through hands-on apprenticeships.

Finally, interviewed stakeholders mentioned recent discussions regarding the possible establishment of a regional centre for coordination in case of large-scale incidents, recognising this as a potentially good idea for the Western Balkans.

North Macedonia

Geopolitical context

North Macedonia has been developing its cybersecurity framework almost exclusively with the support of the West. Developments to this end have slightly stalled in the few years towards the end of Nikola Gruevski's VMRO-led government as a result of a bleak international perspective because of the 'name issue', including cybersecurity-related aspects. With the change of government however, and a renewed EU and NATO membership perspective following the Prespa Agreement, North Macedonia was also back on track in developing its cybersecurity ecosystem. To this end, in 2018, the first national Cybersecurity Strategy was adopted, based on the principles of the EU Cybersecurity Strategy and the NATO Cyber Defence Pledge.

Following its accession to NATO, in 2021 North Macedonia signed the new Memorandum of Understanding on Cyber Defence cooperation with NATO. This document will enable the country to be better integrated into the cybersecurity and defence framework of NATO and benefit more from its membership, as Albania and Montenegro already do.

Like most Western Balkan economies, North Macedonia is a signatory of the Council of Europe (CoE) Budapest Convention on Cybercrime and is engaged in the CoE iPROCEEDS project, aimed at strengthening the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet, and is currently a member of its subsequent, iPROCEEDS2 phase. The national CERT (MKD-CIRT) is an accredited member of the Trusted Introducer community of CERTs. In terms of direct bilateral support, North Macedonia is currently engaged with the US on projects focused on building up resilience of critical national infrastructure, previously benefitting from several USAID programmes related to cybersecurity. North Macedonia has signed the US-led Clean Network initiative.[59]

Research conducted for the purpose of this report has not identified any official cooperation arrangements between North Macedonia and Russia on cyber-related matters. The country's only indirect relation to Moscow pertains to the assumed distribution of fake news stories distributed from an organised centre in the small town of Veles in 2016. The campaign of which this centre was part of has been defined as influencing the final outcome of the 2016 US presidential elections. Despite indications that some of these fake stories had their source in

59 Bulgaria, Kosovo, North Macedonia Join U.S. Initiative To Block Chinese Equipment In 5G Network. 23.10.2020. Radio Free Europe. https://www.rferl.org/a/bulgaria-kosovo-north-macedonia-join-us-initiative-to-block-chinese-equipment-in-5g-network/30909512.html

Moscow,[60] there is no proof of any meaningful cooperation with, or influence of, Russia at the national level. Simply put, distribution of fake news was outsourced to a location in the Western Balkans.
As for China, there is no elaborated form of bilateral cooperation between Skopje and Beijing, in comparison to some other Western Balkan economies.

Threat landscape

Existing risks and threats	Attack types	Anticipated trends
Growth of cybercrime Increased sophistication of attacks Lack of clear jurisdiction and enforcement powers Limited human capacity Lack of awareness Supply chain risks	Phishing Website defacement Ransomware	Rise in attacks on critical infrastructure Digitalisation-related risks Increase in ransomware Continued capacity challenges
		Identified needs
		Stronger regional cooperation Awareness raising Sectoral capacity-building

Existing trends

The number of incidents officially reported to MKD-CIRT varies on a monthly and annual basis. Current trends show phishing as the most common type of attack, followed by website defacement and ransomware. Generally, the primary vector for gaining access is phishing, using malicious programmes that enable overtaking remote control functions and collecting data. A growing level of sophistication of phishing methods has been recorded, making it much harder to differentiate between legitimate and fake web pages, compared to previous use of poor graphics and grammar.

In 2020, the total number of incidents officially reported to MKD-CIRT was 1443. Most of these are automated reports on malicious activities detected abroad, in which Macedonian IP addresses were identified as a source of harmful activities.[61]

60 'Fake News' Sites In North Macedonia Pose As American Conservatives Ahead Of U.S. Election. 22.10.2022. Radio Free Europe. https://www.rferl.org/a/macedonia-fake-news-sites-us-election-conservatives/30906884.html

61 Statistics on the operations of MKD-CIRT in 2020. National Centre for Computer Incident Response of the Republic of Macedonia. *(report in Macedonian)* https://mkd-cirt.mk/wp-content/uploads/2021/06/Statistika_2020_vebv2.pdf

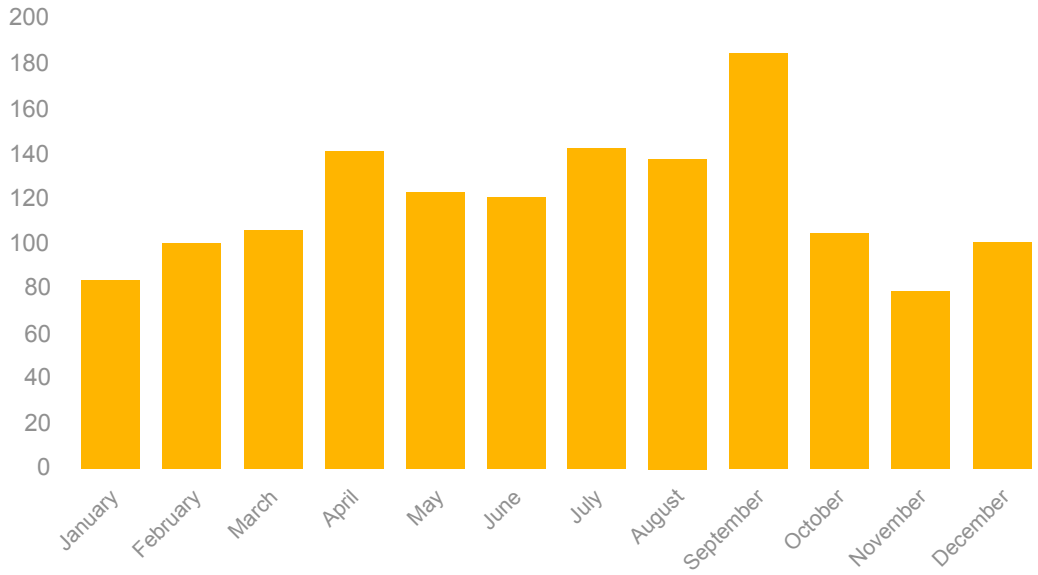


Figure 5. Incidents reported to MKD-CIRT per month in 2020[62]

This is an increase from 2019, when 1060 incidents were reported to the national CERT.[63]

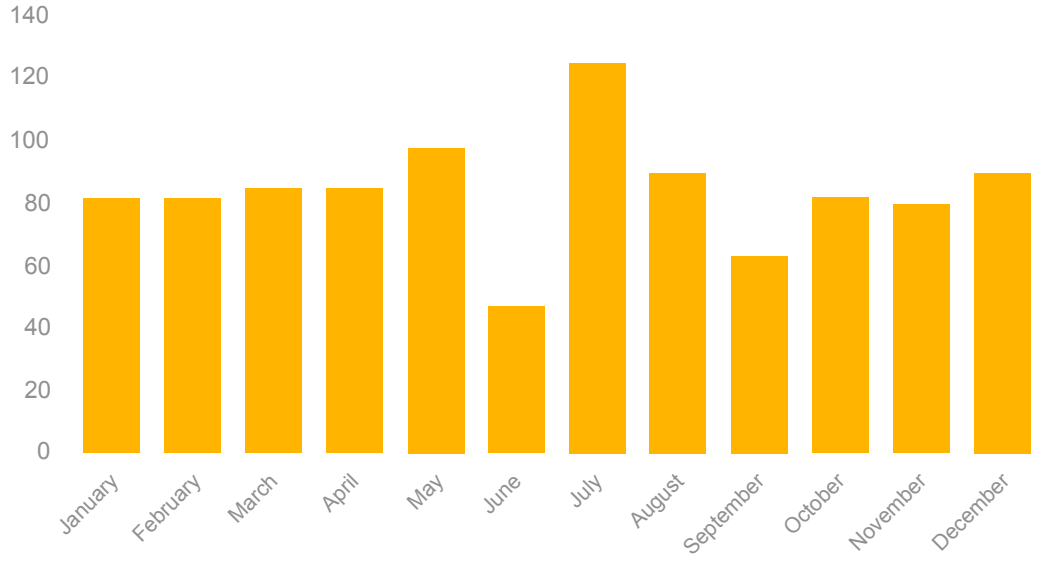


Figure 6. Incidents reported to MKD-CIRT per month in 2019[64]

62 *Ibid.*

63 Report on the work of MKD-CIRT in 2019. National Centre for Computer Incident Response of the Republic of Macedonia. *(report in Macedonian)* https://mkd-cirt.mk/wp-content/uploads/2020/12/Informacija-od-izveshtaj-MKD-CIRT-2019.pdf

64 *Ibid.*

With no legal obligation to report incidents, official numbers are still low, although this is expected to change with the adoption of the Law on Information Systems Security which should make reporting mandatory for critical national infrastructure. Consequently, interviewees believe that the actual number of incidents taking place in North Macedonia is much higher than what official figures indicate.

Follow-up analysis of reported incidents is performed, but to a limited extent. In cases of reported phishing, a wide pool of stakeholders is willing to engage, with active engagement of the banking sector, for example. When it comes to ransomware, however, reports are less frequent due to reputational concerns, predominantly coming from physical persons (i.e. individuals). In cases of ransomware, performing detailed analysis is considered challenging and generally only the attack vector is determined.

Identified risks and threats

From a **governance perspective**, interviewees recognise the lack of a central state body responsible for cybersecurity among potential risks. Although the Ministry of Information Society and Administration and the national CERT (MKD-CIRT) are formally established as competent authorities, they still lack adequate enforcement powers.

Lack of awareness is also seen as a risk, although initiatives and efforts of the national CERTs to this end have been commended by interviewed stakeholders. However, the low level of awareness among decision makers is highlighted as a limitation, hindering further development of relevant institutions.

From an **operational aspect**, in addition to awareness, lack of capacity is recognised as an existing risk. In the current state of affairs, even the smallest incident is seen as potentially having serious consequences, causing significant damage to the public and private sector alike.

In terms of specific threats, risks stemming from the monetisation of cybercrime were highlighted by interviewees. With reduced risk thresholds on the side of cyber criminals, through the use of cryptocurrencies for example, attackers are now increasingly targeting smaller actors too, asking for lower payments. This is seen as a new and growing trend in North Macedonia.

Finally, interviewees mentioned supply chain attacks as an area of concern. Reliance on foreign suppliers and vendors means reduced control which, while existing public procurement procedures do not always guarantee selection of the most appropriate vendors. To this end, the suspension of vendor blacklists, which were previously in place, was highlighted by one interviewee.

Regional specificities

Apart from self-proclaimed activist groups, interviewed stakeholders largely expressed doubts that there are any region-specific cyber criminal groups. The Western Balkan region as a whole is seen as faced with risks and threats that are compatible with general global trends. An example of companies operating in the financial sector was cited, experiencing the same type of attacks as their European peers.

What interviewees do see as a regional trend however is the increased quality in the language and form of communication used in recent attacks. This might, in their view, indicate the potential outsourcing of local individuals by foreign threat actors.

State Electoral Commission

The largest publicly known incident mentioned by interviewed stakeholders is the unavailability of the State Electoral Commission's website on election night in 2020, following a DDoS attack. The incident affected the systems presenting voting data, making them unavailable to the public. The website of the biggest news aggregator in the country was defaced at the same time. Following the incident, an anonymous Twitter profile claimed responsibility for hacking the news aggregator, whilst no one claimed responsibility for the Electoral Commission attack.
Although no significant harm came out of these incidents, they did result in general loss of citizen trust in the Government and its systems.

Main cooperation and support patterns

Interviewed stakeholders recognise established communications channels in the region at the operational level. However, the extent and frequency of information exchange is seen as insufficient, possibly explained by the lack of capacity and varying levels of cybersecurity maturity across regional economies. Outside of the region, stakeholders cite cooperation with Slovenia's national CERT.

At a higher level, information is obtained through established communication channels with NATO. In terms of support to further developing and strengthening the national cybersecurity ecosystem, interviewees highlight cooperation with the US, in the domain of increasing resilience of critical national infrastructure.

Anticipated trends

Critical infrastructure and especially the energy sector are key areas of concern when it comes to future developments in the cyber threat landscape. A successful attack on this sector is seen as potentially causing a domino effect, disrupting the normal functioning of the state and society. Interviewees expect a rise in attacks on critical national infrastructure, especially given the ongoing trend of digitalisation.

In terms of attack methods, ransomware is expected to increase in scope and frequency. Ransomware attacks combined with data exfiltration, whereby the information collected is made public is seen as the greatest threat.
Capacity-wise, existing challenges in terms of retention of trained cybersecurity staff are expected to continue.

In order to better prepare for these future challenges, interviewees believe that raising awareness among critical infrastructure entities is important. This should, in their view, be done through a sectoral approach. The Ministry of Information Society and Administration is currently working with regulators and privately-owned enterprises to this end, but further work on increasing internal capacities of sectoral ministries is seen as necessary. This would enable competent ministries to define sectoral laws that adequately incorporate legally binding cybersecurity aspects (cybersecurity mainstreaming).

Serbia

Geopolitical context

As an EU-candidate country, Serbia's reform processes and related international dynamics are closely connected to the West. At the same time, Serbia is often seen as a country that maintains balance and neutrality in its foreign policy, equally open to cooperation with partners from the West and the East. This neutral orientation was directly expressed in the country's first national Information Security Strategy (for the period 2017-2020). The Strategy listed the UN, OSCE, EU, and CoE as key international partners, alongside other 'political, economic, security and defence organisations and alliances with which the Republic of Serbia has concluded agreements on cooperation, as well as neighbouring countries and traditional allies'[65]. The recently published second national Strategy for the Development of an Information Society and Information Security (for the period 2021-2026) foresees three levels of international cooperation:

- Broader international: UN, ITU, OSCE, Global Forum on Cyber Expertise (GFCE);
- EU level: cooperation with EU institutions and organisations that have competencies in the field of cybersecurity such as ENISA, and the network of EU CERTs; and
- Other multilateral and bilateral cooperation based on cybersecurity cooperation agreements.

According to publicly available resources, Serbia has at least twenty-nine international cooperation documents (including agreements, Memorandums of Understanding, letters, etc.) that cover different aspects of cooperation on cyber-related matters. There are no agreements whose main topic is cybersecurity per se. Rather, these documents set the general basis for more proactive cooperation between Serbia and the other signatories. Most frequent are agreements related to police cooperation (peer cooperation, security agreements, agreements on cooperation in fighting terrorism and/or organized crime), followed by several documents related to military and defence cooperation that have references to cyber, and documents related to cooperation regarding the general development of ICT.[66] This does not mean, however, that Serbia has active cooperation in every aspect that these agreements cover on paper.

Serbia established its baseline cybersecurity framework in line with the country's EU integration process and its general cooperation patterns with the West. All of its legislative and strategic frameworks have been developed with the aim to en-

65 Strategy for the Development of Information Security in the Republic of Serbia for the period from 2017 to 2020. „Official Gazette of the Republic of Serbia", no.53/2017.

66 A list of publicly available documents is provided in Annex A.2.

sure alignment with trends in the EU, most notably the EU Cybersecurity Strategy and the EU NIS Directive.

Serbia's national CERT (SRB-CERT) has engaged in some of the critical Western initiatives, such as the ECASEC Expert Group (formerly Article 13a Expert Group – 2009/14/EU Directive) aimed at ensuring that telecom providers take appropriate security measures to protect the security and integrity of telecom networks and services. SRB-CERT and Serbia's Interior Ministry CERT (MUP-CERT) are accredited members of the Trusted Introducer, and members of the FiRST communities of CERTs. There is also standing cooperation with the George C. Marshall European Center for Security Studies and Carnegie Mellon University.

At the global level, Serbia had a representative in the 2016-17 cycle of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, and is currently a member of the UN Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security, set up in 2018. The country has also actively engaged with the OSCE pertaining to the Confidence Building Measures (CBMs) to reduce the risk of conflict stemming from the use of information and communication technologies[67]. Specifically, Serbia is contributing to CBM no.9 which is focused on reducing the risk of misunderstandings in the field of information technology, by conducting an analysis of the terminology used, and the similarities and differences in the definitions of relevant terms based on lists of national terminology voluntarily submitted by member states.[68] Finally, as the only representative of the Western Balkan economies, Serbia is a member of Global Forum on Cyber Expertise (GFCE), an initiative launched in 2015 by the Dutch Government along with forty-one ministers and other high-level representatives from business and international organisations aimed at strengthening cyber capacity building and coordinating existing international efforts more effectively.

When it comes to cyber defence, according to publicly available sources, the only programmes that Serbian defence institutions take part in are organised by NATO. Formally, Serbia's first Individual Partnership Action Plan (IPAP) with NATO, agreed in 2015, contains a reference to the country's aim to 'enhance its capabilities for protecting critical communication and information systems against cyber-attacks' concluding that 'government-level mechanisms and a coordination structure for cyber-defence need to be established'[69]. Serbia obtained a new IPAP in 2019, but the elements of the Action Plan are not publicly available.

---

67 Decision No.1202. OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of Information and Communication Technologies. 10.3.2016. Organization for Security and Co-operation in Europe. PC.DEC/1202.

68 About CBM9. Ministry of Trade Tourism and Telecommunications of the Republic of Serbia. https://cbm9.gov.rs/about

69 Quoted in Abusara, A. at al. 2016. Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities. Diplo Foundation. p.27

Nevertheless, Serbia has been utilising its participation in the NATO Partnership for Peace programme and bilateral relations with the US towards improving its cybersecurity posture. For example, since 2016 there is regular cooperation with the National Guard of Ohio, running a joint cyber drill titled 'Cyber Tesla', focused on building military capacities of Serbia's defence system to fight against high-tech attacks. In 2021, the Armed Forces of Hungary also took part in this programme, alongside a number of national stakeholders from the public and private sector, and academia.[70] Within the NATO Science for Peace and Security programme, representatives of the Government Office of the National Security Council and Classified Information Protection completed the NATO Cyber Security Training on information systems security (INFOSEC) focused on real-life situations in 2017.[71]

Regarding the cybercrime domain, Serbia is a signatory of the Council of Europe (CoE) Budapest Convention on Cybercrime and is engaged in the CoE iPROCEEDS project, aimed at strengthening the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet, and is currently a member of its subsequent, iPROCEEDS2 phase. At the bilateral level, Serbia has cooperation with several EU Member States, most notably Germany[72] and Spain[73]. Additionally, in 2013, the then State Secretary of the Interior Ministry announced plans to open a joint office for fighting hi-tech crime with the US Federal Bureau of Investigation (FBI)[74]. The Interior Ministry also works with relevant South Korean institutions, on strengthening internal capacities of its employees and officials.[75]

As for Serbia's alignment with the EU's Common Foreign and Security Policy (CFSP), Serbia has aligned with the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, which allows it to use all CFSP measures to prevent, discourage, deter and respond to malicious cyber activities directed against the Union and its Member States. In practice however, Serbia has previously failed to align with concrete restrictive measures when individuals and entities identified as perpetrators of malicious activities were of Russian or Chinese origin.[76]

---

70 Exercise Cyber Tesla 2021 successfully completed. 09.12.2021. Ministry of Defence of the Republic of Serbia. *(article in BCS)* https://www.mod.gov.rs/lat/18127/uspesno-zavrsena-vezba-sajber-tesla-2021-18127

71 Serbian Officials Complete NATO Cyber Security Training. 25.11.2017. US Embassy in Serbia. https://rs.usembassy.gov/serbian-officials-complete-nato-cyber-security-training/

72 Stefanović: Joint forces against cybercrime. 09.07.2018. Studio B. *(article in BCS)* https://studiob.rs/majer-srbija-nemackoj-najvazniji-partner-protiv-kriminala/

73 Vulin in Madrid with the Spanish Minister on cooperation and Kosovo. 22.07.2021. Danas. *(article in BCS)* https://www.danas.rs/vesti/politika/vulin-u-madridu-sa-spanskim-ministrom-o-saradnji-i-kosovu/

74 The Ministry of the Interior and the FBI are opening a centre for the fight against cybercrime in Belgrade. 26.03.2013. eKapija. *(article in BCS)* https://www.ekapija.com/news/705225/mup-i-fbi-u-beogradu-otvaraju-centar-za-borbu-protiv-sajber-kriminala

75 Stefanović: Significant cooperation between the Ministry of the Interior of the Republic of Serbia and the Korean Agency for Internet and Security in the field of cyber security. 28.03.2018. Ministry of Interior of the Republic of Serbia. https://bit.ly/3Ae872M

76 See Novakovic, I. 2020. Seven Years of Serbia's Alignment with the Common Foreign and Security Policy of the EU. ISAC Fund. pp.30-31

Only two non-Western players have thus far displayed interest in having an active role in matters pertaining to ICT and cyber at the geopolitical level. Apart from Russia and China, as the two greatest powers involved, Serbia also has standing agreements with Turkey and India. However, there is no indication that there has been any active collaboration regarding cybersecurity with the latter two, to date. Although Serbia's cooperation with Russia is seemingly primarily focused on conventional security matters, cyber has been an element of bilateral cooperation ever since the 'new relationship' was established in 2008. Although the Police Cooperation Agreement foresaw cooperation in the fight against cybercrime, there were no indications of such cooperation until a visit of the then Minister of Interior, Nebojsa Stefanovic, to Moscow, in 2017.[77] On that occasion, Stefanovic announced that he agreed with his Russian counterparts a training for the Serbian Police with Russian police experts, who will demonstrate to their Serbian counterparts 'how the Russian Police fights against organised and cybercrime, illegal migration, and drug trafficking'[78]. In 2021, Serbia's current Minister of Interior, Aleksandar Vulin, and the First Deputy Minister of Internal Affairs of Russia, Alexander Gorovoy, agreed to continue this process.[79]

In addition, the 2017 Agreement on Cooperation and Joint Action with the Federal Security Service, whose primary focus is cooperation on the security of protected persons, also contains provisions related to cyber. These are broadly defined, citing 'neutralising computer attacks against state information resources of vital importance'. According to prominent security experts in Serbia, this is a potential cause for concern as the Agreement covers all state information resources of vital importance. This implies that, in addition to the Ministry of Interior, all other institutions responsible for information security in Serbia are involved, which is not specifically mentioned in the Agreement itself.[80]

Serbia's cooperation with China is much broader, encompassing both Chinese institutions and its private sector stakeholders, most notably Huawei. Since 2009, Serbia has had a Strategic Partnership Agreement with China, which was elevated to a Comprehensive Strategic Partnership in 2016, during a visit of the Chinese president Xi Jinping. Serbia is the primary destination for the Chinese capital (loans and infrastructure projects, as well as brownfield and greenfield investments) in this part of Europe, amounting to EUR 7.5 billion, according to statements of Serbian

77 Against cybercrime with the help of Russian experts. 04.09.2017. Politika. *(article in BCS)* https://www.politika.rs/sr/clanak/388223/Hronika/Protiv-sajber-kriminala-uz-pomoc-ruskih-eksperata

78 Against cybercrime with the help of Russian experts. 04.09.2017. Politika. *(article in BCS)* https://www.politika.rs/sr/clanak/388223/Hronika/Protiv-sajber-kriminala-uz-pomoc-ruskih-eksperata

79 Vullin's two days in Moscow. 15.05.2021. Forum for Security and Democracy. https://fbd.org.rs/index.php/en/?option=com_content&view=article&id=552

80 Djordjevic, S. Security partnership between Serbia and Russia. 17.03.2018. Pescanik. *(article in BCS)* https://pescanik.net/security-partnership-between-serbia-and-russia/

politicians.[81] Cooperation on ICT and cyber has been in place even before the Digital Silk Road was announced. Initial consultations with Huawei regarding the 'improvement of the information and telecommunication system' of the Serbian Ministry of Interior took place already in 2011. Since then, Chinese companies have established cooperation agreements both at the central and local levels. In 2016, Telekom Srbija and Huawei launched a fixed network transformation project estimated to be worth EUR 150 million, which was the first large-scale cooperation effort in information and communications technology between the two countries. In 2017, Serbia and China signed a Memorandum of Understanding on Strengthening the Development of Information Silk Road for Information Connectivity, and the same year Belgrade hosted the Information Silk Road for Information Connectivity Summit. [82]

Huawei is among the commercial users of the state-owned national data centre in Kragujevac[83], and funded the completion and equipment for a second data centre in this town. In addition, Huawei signed an agreement with Serbia to start the development of an AI platform and cloud infrastructure for the data centre, also providing a grant for this project.[84] This cycle has been completed by opening Huawei's Digitalization and Innovation Centre in Belgrade.[85]

Over time, Huawei's engagement with Serbia's national telecom provider, Telekom Srbija, became increasingly complex and the company rose to be seen as a key foreign partner, especially critical for the development of Telekom's 5G network. However, the 2020 'Washington Agreement', a set of two documents containing unilateral political obligations of both Belgrade and Pristina towards the US, has abruptly ended these plans. Signing the Agreement, Serbia obliged itself to remove 5G equipment from its mobile networks provided by 'untrusted vendors' and prohibit such vendors from partaking in future projects in its market. Chinese Huawei, as well as ZTE, are seen as among these untrusted vendors. For the time being, there have been no mentions of a renewal of Serbia's engagement with Huawei, with the Serbian Prime Minister, Ana Brnabic stating in late 2020 that 'Serbia does not need 5G at this moment.'[86]

---

81 "Donations" from China will be repaid in a decade or two, with a debt of eight billion dollars. 11.12.2021. N1. *(article in BCS)* https://rs.n1info.com/biznis/donacije-iz-kine-vracacemo-deceniju-ili-dve-zaduzenje-osam-milijardi-dolara/

82 Stefan Vladisavljev. June 2021. China's 'Digital Silk Road' Enters the Western Balkans. Choice. p.15

83 National Data Centre in Kragujevac: The most modern building of that type in this part of the world, ready for the future. SmartLife Mondo. *(article in BCS)* https://smartlife.mondo.rs/e-uprava/pametni-gradovi/a26978/data-centar-kragujevac-kako-izgleda-ko-koristi-cemu-sluzi-pametni-gradovi-smart-city-huawei-ibm-foto.html

84 Huawei to use capacity at Serbia's Kragujevac data centre. 09.12.2020. SeeNews. https://seenews.com/news/huawei-to-use-capacity-at-serbias-kragujevac-data-centre-723883

85 Huawei and the Serbian Government open a 5G Tesla laboratory in Belgrade – A research centre for the entire region. SmartLife Mondo. *(article in BCS)* https://smartlife.mondo.rs/tech/uredjaji/a18635/Huawei-5G-Srbija-Huawei-centar-za-inovacije-i-digitalni-razvoj-Huawei-5G-TESLA-laboratorija-Srbija.html

86 "Stop" for 5G: Brnabić says that citizens do not need it, experts – the state has no money. 21.12.2020. N1. *(article in BCS)* https://rs.n1info.com/scitech/a686087-stop-za-5g-brnabic-

The second glitch in Serbia's relations with China pertains to Smart and Safe City projects. While the Smart City project has prompted some worries regarding citizens' privacy, the Safe City project in Serbia was met with strong opposition due to plans to introduce biometric surveillance in public spaces. Following initial contacts with Huawei in 2011, Serbia's Ministry of Interior signed the first Memorandum of Understanding on the Safe City projects in 2014, and two years later the first test phase cameras were installed in Belgrade. This was followed by the signing of a Strategic Partnership which ultimately resulted in a controversial project of installing over 1,000 state of the art technology cameras in the Serbian capital, with plans to set up more than 8,000 different cameras overall and introduce facial recognition software. The project sparked a debate between civil society in the country, led by the SHARE Foundation, and the Ministry of Interior over the usage of cameras and violations of human rights[87]. Culminating in September 2021, a Draft Law on Internal Affairs was presented, including provisions which would legalise the use of biometric surveillance in public spaces, for which there is currently no legal basis in the national legislative framework. Following prompt reaction of the civil sector in Serbia, and in Europe where several Members of the European Parliament voiced their concerns over the issue, the Draft Law has been withdrawn until the next general elections scheduled for April 2022.

Threat landscape

Existing risks and threats	Attack types	Anticipated trends
Legacy systems Digitalisation-related risks Limited human capacity Lack of awareness Increased sophistication of attacks	Phishing Online scams and fraud Ransomware	Need for outsourcing specific cybersecurity functions Growing sophistication of attacks Digitalisation-related risks Continued domination of cybercrime
		Identified needs
		Better information sharing Sectoral capacity-building Public-private partnerships Digital literacy and awareness raising

kaze-da-gradjanima-ne-treba-strucnjaci-drzava-nema-para/
Recently however, there have been announcements that an auction for the allocation of frequencies for the 5G network in Serbia can be expected in mid-2022. Auction for the installation of 5G network in Serbia, most likely in the first half of this year. 03.01.2022. eKapija *(article in BCS)* https://www.ekapija.com/news/3538858/aukcija-za-instalaciju-5g-mreze-u-srbiji-najverovatnije-u-prvoj-polovini-ove

87 Thousands of cameras. SHARE Foundation. https://hiljade.kamera.rs/en/home/

Existing trends

Official records show an increase in incidents reported in 2021 compared to the previous year. Interviewees see two possible reasons for this growing trend. The first is a general increase in the number of incidents taking place in Serbia's cyberspace. The second is increased awareness of the existence and role of the national CERT (SRB-CERT), especially following SRB-CERT's direct outreach to critical national infrastructure entities. The profiles of stakeholders reporting incidents varies from critical infrastructure entities to private sector stakeholders, including also public bodies such as posts, courts, etc. Sector-specific examples, provided by some interviewees, include financial sector entities where an increase of 40-50% in the number of attacks was recorded in 2020, followed by a 100% increase in 2021.

In terms of attack and incident type, phishing is found to be most common, especially since the start of the global pandemic. Scams on online shopping platforms are also on the rise. Reports of ransomware have been limited thus far, although interviewees believe that this can potentially be attributed to possible restraint of affected stakeholders for reputational reasons. Some of the interviewed stakeholders also mentioned the presence of DDoS attacks in early 2021, recording reduced frequency later in the year.

A total of 276 incidents have been officially reported to SRB-CERT in 2020.[88] This is an increase from 2019, when official reports accounted for 152 incidents.[89]

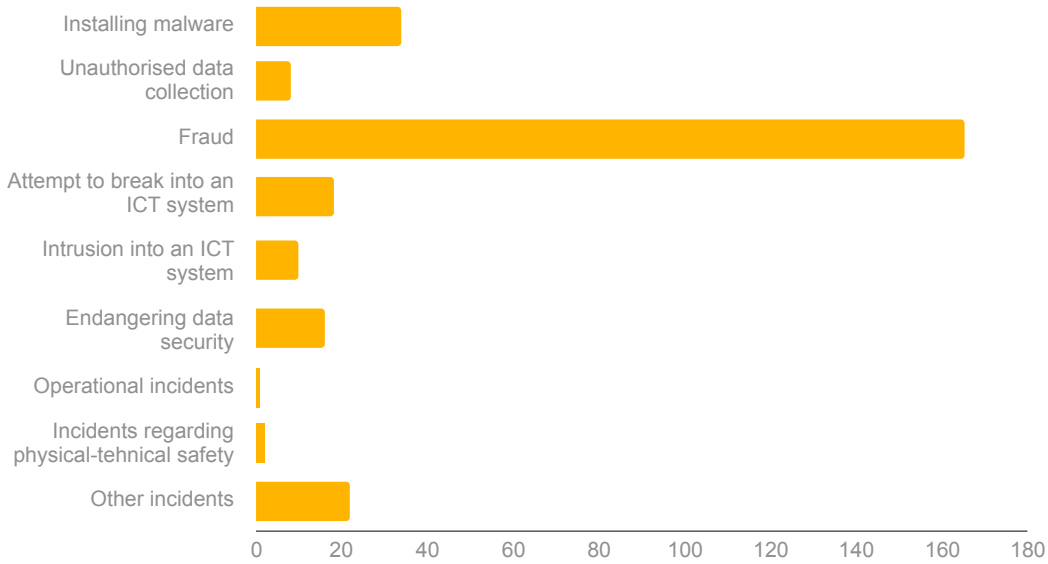


Figure 7. Reported incidents in 2020[90]

88 Chapter 10: Information security. Work report for 2020. Regulatory Agency for Electronic Communications and Postal Services.

89 Chapter 10: Information security. Annual Report 2019. Regulatory Agency for Electronic Communications and Postal Services.

90 Chapter 10: Information security. Work report for 2020. Regulatory Agency for Electronic Communications and Postal Services.

PUC Informatika

Most interviewed stakeholders cite the March 2020 ransomware attack on PUC Informatika in Novi Sad as the largest national incident. The incident saw the hacking of Informatika's servers, affecting city administrations as well as several other public services. Reportedly, the city refused to pay the ransom requested in bitcoins and was thus left without a certain part of its data. The attack also affected the unified payment system, registry offices, video surveillance system, a preschool institution and almost all public companies. The consequences of the attack included inability to pay out salaries to a number of city administration and some public companies' employees, with delays in city services as a result of the systems and equipment being taken offline for remediation.

Attack types differ depending on the specific target. Public institutions usually experience phishing attacks targeting officials and their cabinets. Small and medium sized enterprises commonly face 'man in the middle' campaigns. A general perception highlighted by some of the interviewed stakeholders is that public institutions experience a higher volume of attacks compared to other types of stakeholders. Finally, with the onset of the pandemic, the health sector experienced an increase in attacks, as did the financial sector, which mirrors general global trends.

At the moment, no detailed analysis of reported incidents is officially conducted, apart from general classification in terms of incident type and the nature of targeted entities.

Identified risks and threats

From a **technical aspect**, legacy systems and outdated equipment are recognised among potential risks, as updates and patches are no longer available for some of these. Interviewees also mentioned the lack of anti-virus protection.

In addition, in the context of digitalisation, concerns are expressed regarding the speed at which innovations are currently taking place, without the necessary security verifications conducted.

Capacity-wise, interviewed stakeholders highlight the lack of appropriate staff, especially in the public sector. The perception of some of the interviewed stakeholders is that it is easier to secure resources for procuring equipment and maintenance services than for retaining vital staff. Public institutions are faced with the challenge of having trained staff leave for better paid positions in the private sector, or leave the country overall. Private sector stakeholders also report significant staff turnover, with a limited number of trained professionals on the market. Consequently, interviewed stakeholders see outsourcing as a possible mitigation strategy, having private companies gradually overtake some functions that the state should provide. In turn however, this is also seen as a further potential risk.

A key risk that all interviewees agree upon is the **human factor** resulting from the overall lack of awareness, with the common mantra of 'it will not happen to me'. The challenge of maintaining a high level of awareness of decision makers is particularly highlighted, as busy schedules prevent regular briefing sessions

to convey relevant information on developing trends and resulting needs. Consequently, interviewees argue, this affects decisions pertaining to investment in cybersecurity matters, feeding into the risks and challenges listed above.

Based on the characteristics of the attacks recorded, interviewed stakeholders agree that attack methods have definitely evolved, listing the example of phishing. Previously, the content of phishing emails did not make much sense, indicating the use of direct translations of poor quality and bad grammar. Present-day phishing emails however seem to be planned much better, with the content used, language-wise, close to perfection. Interviewees recognise that this might indicate the use of local resources in the preparation of materials used in phishing campaigns.

Regional specificities

Interviewed stakeholders share the opinion that there are no region-specific malicious actors operating in Serbia, or the Western Balkans. Recorded incidents are not seen as specifically targeted, and globally distributed malicious activities are seen as affecting the region as part of a general trend.

What is obvious however is that certain attacks have been launched using content developed by, or with the support of, individuals who are fluent in Serbian. Interviewees expect that this is a trend common to all Western Balkan economies.

Main cooperation and support patterns

At the national level, cooperation among competent authorities and other relevant institutions that have the necessary capacities is seen as efficient. These include, among others, the Ministry of Trade, Tourism and Telecommunications, the national CERT, the Ministry of Interior CERT and the Prosecutor's Office for High-Tech Crime. A lack of adequate capacities in the Ministry of Foreign Affairs has been recognised by interviewees, despite the fact that Serbia is engaged in a number of global processes and initiatives pertaining to cybersecurity. The gen-

In addition to the case of PUC Informatika, civil society stakeholders cited further large-scale national-level incidents:

COVID-19 database
The username and password to access the COVID-19 Information System, Serbia's national system for tracking the pandemic, was available on a public page on the website of a health institution in Belgrade for 8 days during April 2020, long enough to be indexed by Google and easily accessible with a simple search. The system is the most comprehensive citizen health database established by the Government of Serbia at the outset of the pandemic. Access to the page with credentials was disabled promptly after the authorities had been notified.

Chamber of Commerce
IT researchers discovered that an application of the Serbian Chamber of Commerce has left exposed large amounts of personal data, as its web server had the directory listing option enabled, which practically opens access to all files stored on the server. The files contained scanned ID cards, university diplomas, as well as contracts. As the researchers found, all the data was accessible without any authentication, meaning that anyone could freely access them at any time.

eral perception among interviewed stakeholders is that, in case of a major incident, they would know who to turn to as a result of previously established formal and informal connections.

Regional cooperation is also assessed positively. Interviewees highlight that relevant peers in the region know each other personally, but recognise certain challenges in cooperation with stakeholders operating in environments where no formal institutional frameworks are in place. When it comes to the wider region and globally, operational cooperation is seen as limited to information exchanges when there is awareness on a specific target in the given country, in which case communication is conducted vis-a-vis the national CERT. The only exception listed in this sense is Slovenia, where cooperation with Slovenia's national CERT is seen as much broader.

At the international level, operational information is obtained by the national and other government CERTs through membership in international CERT communities such as Trusted Introducer and FiRST.

Finally, interviewed stakeholders explain that private sector actors have additional avenues for obtaining relevant information, primarily in cases where local entities are members of wider international groups with headquarters abroad. This is the case, for example, in the telecoms and financial sector.

Anticipated trends

Interviewed stakeholders generally agree that the sophistication and frequency of attacks is growing. This trend is not expected to change. In this sense, critical infrastructure is seen as most vulnerable, especially in the energy, transport and healthcare sectors.

Given the ongoing process of digitalisation, and based on trends recorded in the previous year, e-commerce users are also expected to experience a growing number of threats, as this is still a developing field. In addition, the expected continuation of a hybrid model of work is expected to irreversibly change approaches to security.

Interviewees also anticipate continued domination of cybercrime as technology and techniques become increasingly available, enabling even 'smaller' criminals to achieve financial gains with significantly reduced risk thresholds.

Finally, some interviewees list cyber terrorism as an area to watch and prepare for, in combination with cyber warfare. At the global level, state-sponsored attacks are seen as potentially expanding in scope and frequency, conducted by different cyber criminal groups, making it difficult to determine who is the primary sponsor of specific actions.

In order to respond to these anticipated developments, interviewed stakeholders argue that the current practice of limited information sharing needs to change, highlighting that timely and appropriate information is key in cybersecurity.

From an operational aspect, due to the currently limited capacities nation-wide, interviewees proposed two possible approaches:

- Supporting sectoral capacity development in order to ensure greater national resilience in the face of upcoming cybersecurity trends; and
- Strengthening public-private cooperation and outsourcing, with the exception of military and security agency systems.

Finally, investing in the development of digital literacy and general cybersecurity awareness at all levels is seen as key for building cyber resilience nation-wide.. Such efforts, interviewees argue, should be implemented in a continuous manner, repeatedly communicated to the same audiences, rather than posing as a one-off, ad hoc activity.

Vulnerable groups lens

In order to foster truly resilient societies, the challenges faced by, and resulting need of all societal groups need to be taken into account. This necessitates adopting a vulnerable groups lens as minority and marginalised groups commonly rely on the digital sphere much more than the rest of the population for everyday social activities such as education, health information and advice, or establishing contacts. Many vulnerable groups facing stigma and discrimination turn to the digital sphere seeing it as a safe(r) environment, only to be exposed to the same risks and threats they face in the physical world.

As highlighted by interviewees, vulnerable groups are far from homogenous. The different characteristics and particular vulnerabilities of different societal clusters determine the type of risks individuals falling into one or several vulnerable groups face. From a high-level perspective, there are conceptual differences in how women and men are targeted in cyberspace, with women more prone to be subjected to specific forms of violence in the digital environment, as they are in the physical world. According to interviewees, the most common types of attacks on women across the Western Balkan region generally mirror global trends and include discrediting, stalking, shaming and publicly attacking the image of a woman (smear campaigns), sexual harassment, intimidation, as well as the publication of private content by current or former partners or the threat to do so .

In terms of specific **gender-related trends**, examples of threats and incidents provided by interviewees are similar across the Western Balkans. These range from misogynist campaigns, aimed at diminishing the integrity of public female figures, to online platforms for sharing explicit images of women and young girls, and online sexual exploitation of increasingly younger women and girls.

Delving deeper into the cyber risks and challenges experienced on the basis of **gender identities and sexual orientation**, matters become even more complex. Interviewees explain that individuals and organisations dealing with human rights, gender, LGBTQI and marginalised groups' rights experience DDoS attacks, cyber bullying, threats and attempts of hacking personal online accounts. These are followed by alarmingly growing trends in online hate speech and smear campaigns against activists, especially around Pride parades, increasingly posing as direct calls for physical violence. With the outset of the global pandemic, online dating applications have also become a source of potential risk, with malicious actors falsely representing themselves in order to collect enough information which can later be used for blackmail and extortion.

Specific risks and threats experienced by vulnerable groups in the cyber sphere vary depending on a number of characteristics such as age, gender, sexual identity, socioeconomic status, level of education, belonging to a national minority or

having a disability. For this reason, interviewees highlight that devising adequate approaches to support greater resilience requires an intersectional perspective.

Another challenge, as also recognised by interviewees coming from some of the relevant competent authorities of Western Balkan economies, is that awareness of the diversity of vulnerable groups, and the spectrum of attack types these groups face in cyberspace, is still extremely limited. This is reflected in national legislation, where in some cases actions such as cyber bullying or revenge porn are not recognised as criminal offences. Civil servants are also seen as lacking the knowledge and capacity to approach cases of such violations, collect evidence, protect the identity of the victims and take further actions such as removal of the sensitive content.

This also reflects on the number of reported cases of cyber attacks experienced by vulnerable groups. On the one hand, there are doubts as to whether reporting an incident will actually result in having the perpetrators caught or the sensitive material removed. There is also a risk that victims will be subjected to unwanted public attention, revictimised by the media reporting on the topic. As a result, victims rarely report online incidents. More often, only once something happens in the physical world does it become clear that it was preceded by a period in which the victim has been targeted in the digital sphere. As a result, interviewees argue, a dangerous trend is developing in which targeted individuals and groups have become accustomed to receiving online threats left with no other solution than to ignore them, despite the fact that these threats often materialise in some form in the physical world.

Additionally, interviewed stakeholders explain that, in most cases, even reported incidents rarely lead to necessary actions being taken by the police or the prosecution. In their experience, lack of evidence of actual physical danger stemming from threats made online is commonly cited as a justification for inaction.

Consequently, relevant competent authorities have very limited insight into cybersecurity trends and developments affecting vulnerable groups due to a lack

Security of the individual = Security of the community

Activists and organisations working with vulnerable groups are extremely wary of the fact that if they get compromised in the digital sphere, the entire community they engage with may be endangered. For example, individuals active in the LGBT community have direct contact with persons who might face further discrimination, targeting, or actual physical harm if their identities are revealed by a potential hack of just one personal account of a member of the community. This risk is applicable to a variety of vulnerable groups, from women who experience domestic violence, to investigative journalists who have contacts with different sources who do not want their identities to be made public, and many more. As a result, introducing and sustaining measures aimed at increasing personal and organisational resilience takes up a significant portion of efforts, capacities and budgets which are already limited, and without a comprehensive, systematic approach the possibility of developing greater societal resilience will remain extremely limited.

of official data. In contrast, civil society organisations active in the field (and on the ground) indicate having significantly higher levels of awareness of both trends and specific instances of violations. Even where reports are recorded for statistical purposes, the methodology for classification differs between and across institutions making it extremely difficult to have aggregated data for cross-referencing at the national level.

To this end, interviewed stakeholders agree that in order to raise capacities to face current challenges and prepare for future trends, awareness raising on these matters needs to be approached in a comprehensive manner. Community members, activists and human rights organisations would, in their view, benefit from awareness raising campaigns on cyber threats, definition and implementation of security protocols, and tailored training in cybersecurity.

This should be followed by adequate amendments of national frameworks to recognise specific types of cyber violence and harm and address these appropriately. In addition, development of fast-track mechanisms for dealing with reported incidents is also seen as a necessary measure, in order to enable prompt removal of sensitive content from the internet in order to protect the victim. This is especially relevant given the fact that only public authorities have the benefit of direct communication with specific social media platforms, and are in a position to request such removal.

Finally, interviewed stakeholders highlight that even seemingly neutral events can have significantly different consequences for vulnerable groups compared to the rest of the population. This requires every incident in cyberspace to be approached by including a vulnerable groups lens.

Conclusions

From a geopolitical perspective, a number of global actors are engaged in the Western Balkans, albeit adopting different approaches and focusing on different aspects of cybersecurity. These variations can be illustrated using the common breakdown into the people, processes and technology dimensions of cybersecurity. Specifically, the majority of Western partners, both at the bilateral and multilateral level(s), are focused on providing support and capacity building in the people and processes dimensions. These are implemented through institutional capacity building efforts and initiatives (training, workshops, exercises and drills), assisting processes of establishment of competent authorities and relevant institutions, and development of respective legislative and strategic frameworks. To a certain extent, engagement is also found in the technology dimension, although relatively limited compared to the other two. These forms of engagement are primarily spearheaded by international and regional organisations such as the UN, EU, NATO, OSCE, as well as through bilateral cooperation with Western allies such as the United States and the United Kingdom, among others. The technology dimension on the other hand showcases greater presence of China, for example, through procurement of equipment and tools. To a limited extent, certain Chinese companies have also entered the people dimension, mainly through scholarship programmes for future generations of cybersecurity experts. Finally, there are instances of existing security cooperation agreements that do include provisions related to cyber aspects although these have not been officially employed to date. Such examples include bilateral agreements that certain Western Balkan economies have with Russia and Turkey.

The process of collecting information for the purpose of this report indicates that this type of research is still extremely novel for the Western Balkan region. Specifically, input obtained through interviews conducted with relevant stakeholders demonstrates that, when considering risks and threats in cyberspace, focus is still mainly placed on aspects related to internal governance and capacities. External risks and threats are predominantly discussed in the context of anticipated future trends, at a very general level, and mainly in terms of threat types. Although internal structures and capacities are still being established in some parts of the region, undoubtedly requiring due attention, without stronger monitoring of global trends and developments, relevant stakeholders in the Western Balkans risk approaching their respective cybersecurity ecosystems in a re-

> “
>
> Cybersecurity is a matter of national security and should be treated as such. This means approaching cybersecurity matters with due attention, making strategic decisions on what needs to be protected and how and ensuring continuity of operations and planning processes.

active, inward-looking manner. Without more concrete insight into novel tactics, techniques and procedures of new and emerging threat actors, the possibility of fully understanding the developing interests and movement of malicious cyber actors - and what these mean for the local ecosystem - is limited. This ultimately hinders the possibility for a proactive approach which would ensure greater national resilience in the near future.

Limitations pertaining to trend monitoring are present at the national level as well. Incident reporting practices are still at a relatively nascent stage, leaving national CERTs with scarce amounts of data upon which to analyse and determine national cybersecurity trends and threat landscapes. Consequently, reports produced by national CERTs and relevant competent authorities portray only a fragment of the actual scope of developments in national cyberspace, with a significantly higher frequency of attacks and incidents considered to be taking place in reality. Observed reasons for this lack of incident reporting are multifold. In some instances, this is the result of a lack of reporting obligations in national cybersecurity legislative frameworks, or the lack of a national legislative framework regulating the field overall. Private sector entities are often wary of potential reputational damage if a breach is made public as a result of reporting, whilst other private stakeholders, such as small and medium-sized enterprises, may lack awareness or the capacity to understand that an incident took place and know who to report to. Regardless of the specific reasons, current practice enables only a restricted insight into national developments in this sense. This blurs the overall threat landscape, as CERTs rely on different data and information sources that they have at hand, which depends on their respective constituents' willingness to report, the categorisation methodologies employed, as well as the use of global activity monitoring through open source feeds and information obtained through membership in different CERT communities. These national variations also make inferring greater, regional trends challenging, as cross-referencing of available data is extremely difficult across all six Western Balkan economies based on current publicly available data.

Despite this **lack of comprehensive official data and tailored threat landscape reports at the national level**, the 'coming of age' of cybersecurity is recognised across all Western Balkan economies. Unfolding global trends of rapid digitalisation of services and production, fuelled by the global pandemic, have by no means bypassed the region. As a result, the cyber sphere is undoubtedly recognised as a potential source of risks and threats that are here to stay. To this end, greater insight into the often neglected cybersecurity aspects of digitalisation is seen as one of the key ingredients for supporting a number of processes to be developed and implemented in an appropriate manner.
Specifically, insight into cybersecurity trends and developments enables and contributes to:

- **Introducing necessary procedures, practices and tools** for increasing preparedness and resilience for responding to the evolving risks and threat landscape;
- **Strategically approaching capacity development** efforts based on expected trends in cybersecurity;
- **Targeting awareness raising campaigns** based on identified attack tactics, techniques, and procedures employed by threat actors, and the observed common targets of these attacks; and
- **Reviewing and (where necessary) amending the existing legislation** in order to take into account new developments in the cyber sphere, ensuring continued relevance and effectiveness of the frameworks in place.

At the operational level, a **lack of adequate enforcement mechanisms** to implement existing legislative and strategic frameworks across the region is a further limitation. Although the majority of Western Balkan economies have gradually progressed in rounding up their national frameworks, actual implementation is seen as lagging behind in certain aspects, which is seen as a potential source of risks and vulnerabilities.

The globally-present challenge of a **lack of skilled workforce** has an even stronger impact on Western Balkan economies due to the additional burden of fast-paced emmigration present across the region, affecting the public and private sector alike. Although greater involvement of the academic sector is recognised as a necessary mitigation measure to this end, the **limited number of multi-disciplinary cyber-specific programmes**, with no strategic approach to establishing coordinated and sustainable cooperation between relevant public sector institutions and academia means these challenges are expected to persist, at least in the near future. A possible short-term solution for bridging this gap is found in outsourcing certain public-sector responsibilities (with the notable exception of security and defence functions), although certain doubts pertaining to the cost-effectiveness of such an approach do exist.

Limited financial and human capacities leave national **competent authorities simply incapable of covering all aspects of the ever-expanding cybersecurity threat landscape**. Empowering different sectors to support the central cybersecurity function at national level, through the establishment of sectoral capacities coordinated by a leading competent authority, is seen as a possible mitigation strategy across Western Balkan economies. This coincides with the expected trend whereby different critical sectors in the region are expected to become an interesting target of cyber criminal groups in the near future, including healthcare, transport and energy and their respective supply chains.

Ultimately, end-users, equally encompassing civil servants, private sector employees and citizens in their various social roles, are currently considered as the most vulnerable target of potential attacks in cyberspace. At the same time, they also pose as the likely root cause of materialised cyber incidents, due to a general lack of awareness and appropriate support mechanisms. The **lack of proactive, comprehensive cybersecurity culture and awareness programmes** across the Western Balkans currently leaves individuals in all regional economies without the basic skills to recognise malicious content and activities, knowledge of how to report and to whom and, ultimately, what to do in case an attack is successful. Despite some notable examples targeting specific societal groups and stakeholders, efforts aimed at awareness raising and basic cyber hygiene capacity building have thus far been of limited scope and outreach, implemented mainly in an ad-hoc, unsustainable manner.

Recommendations

- National competent authorities and CERTs should be supported in outreach activities towards their constituencies in order to properly **communicate the benefits of incident reporting**, based on existing mandates and institutional setup. This entails communicating that, although national CERT capacities to provide incident management support and mitigation is still limited across the region, having comprehensive and accurate data on incidents and near misses in national cyberspace is nevertheless useful for all constituents. It would enable them to better prepare for future challenges based on insights into the developing threat landscape and lessons learnt from past incidents reported by industry peers.
- National competent authorities and CERTs should be supported in developing tailored **methodologies for regular monitoring of cybersecurity developments, collecting, processing and categorising data on reported incidents, and devising national threat landscape reports**. These should be based on a standardised approach and industry best practice. Development of such reports should entail in-depth scoping and detailed consultations with all relevant stakeholders, ensuring wide public sector engagement, industry insights and input from academia and relevant civil society organisations. Only such a comprehensive approach will provide for a mapping of all aspects of the cybersecurity landscape, to the highest extent possible. Capacity building aimed at employing tools and techniques for aggregation of such reports and strengthening skills for management and implementation of effective reporting should be provided to this end.
- At the regulatory level, Western Balkan economies should be supported in better **aligning their legislative and strategic frameworks to developing trends in cybersecurity**. This includes several aspects, amongst which the following are key:
    - **Updating existing legislation** to ensure criminal law(s) keep pace with technological developments and trends related to cybercrime establishing parity of treatment between offences in the physical world and those conducted in the digital sphere.
    - **Establishing a meaningful governance system** for protection of critical information infrastructure, essential and important services and industries against existing and future cyber threats.
    - Introducing **cybersecurity standards and procedures** in the process of digitalisation of public administration operations and services.
    - Developing **regulatory and operational frameworks for procurement and verification** of services, products and technologies in line with internationally recognised cybersecurity standards and industry best practice.

In order to assess the level(s) of impact of relevant legislative and strategic frameworks, a **methodology for measuring impact assessment** should be devised, specifying regular review intervals in order to monitor progress and intervene with necessary updates and amendments when necessary, based on the evolving cybersecurity landscape.

- Capacity-wise, in addition to the continued need for supporting operational capacity building of national competent authorities and CERTs, further support should be directed towards **capacity development of additional relevant institutions and bodies**, such as those in charge of investigation and prosecution of cybercrimes committed against individuals and organisations.
- To strengthen cybersecurity resilience, support should be provided in developing a **comprehensive, sustainable sectoral approach**, by building decentralised competences and response capacities (sectoral CERTs and/or CERT-like bodies) that are centrally coordinated at the national level in terms of information and knowledge sharing. Where applicable, support capacities for incident management and mitigation should also be included. A sectoral approach will ensure that the necessary level of expertise and knowledge of the operating environment, with all of its potential and limitations is considered when devising approaches to detering, responding to, and mitigating cyber attacks. A first step to this end could see the establishment of sectoral communities focused primarily on information, knowledge and best-practice exchanges, mirroring Information Sharing and Analysis Centres (ISACs) present in the United States and across Europe. Once an appropriate level of trust is established among peers, and if operational capacities allow, these communities may evolve into full-scale sectoral CERTs in the long(er)-term.
- Addressing the lack of strategic approaches to human capital development, **joint efforts of the public and private sector in partnerships with academic institutions** should be supported in:
    - Developing new and innovative **vocational training programmes** to fill existing gaps and address the lack of technical personnel in the short-term, offering cutting-edge knowledge and certified courses in order to attract prospective cybersecurity professionals.
    - Establishing **national competence centres** in the mid-term, to serve as knowledge sharing hubs for technical analysis, training and skills development, used by private and public sector stakeholders and academia.
    - Establishing **multilevel and multidisciplinary cybersecurity education curricula** in the long-term, to ensure sustainable supply of the necessary workforce. A multi-disciplinary approach would offer a combination of skills including system design and system organisation and governance, developing future experts who will have knowledge of the entire process cycle.

Having timely insight into cyber-related trends would prove beneficial in this sense as well, enabling continuous adjustment of the curriculum to meet the demands and needs of the cybersecurity human capital market.

- Comprehensive support is required across the region for developing **sustainable cybersecurity awareness programmes**, segmented, designed and delivered in a way to ensure tailored targeting and outreach to various audiences across Western Balkan societies. This includes, among other:
    - Introducing mandatory **baseline cyber hygiene programs** for all public sector employees.
    - Having national cybersecurity authorities leading by example, initiating **nation-wide awareness raising and outreach campaigns** applying a whole of society approach. This entails spearheading a sustainable, comprehensive campaign, engaging all relevant actors in society across different sectors, under a common recognisable visual identity. The campaign itself should be designed paying close attention to relevant information sources and topics targeting different societal groups, using appropriate means and communicating key messages in a clear and relatable manner.
    - Developing **region-wide educational and awareness programmes** on how to apply effective cybersecurity measures for individual protection and cyber hygiene practices of organisations working with vulnerable groups.

Further **support to vulnerable groups** can be provided in the form of developing dedicated monitoring tools and reporting procedures to be employed by relevant civil society organisations and activists, allowing for better and secure data collection on online attacks and incidents targeting specific communities. With the limited scope of data collected by authorities in this sense, such databases would serve as valuable additional input to be taken into account when potentially devising national threat landscape reports in the future.

Overall, the conclusions and recommendations stemming from this report can be translated into specific workstreams that Western Balkan economies should embrace and implement in order to strengthen their cyber resilience. Once translated into specific actionable items, these workstreams may serve as a path towards continued investment into strengthening the cybersecurity posture of the region. Given the number of intersections between these envisioned workstreams, devising any potential support programmes, projects or initiatives to this end should be based on comprehensive consultation and coordination within the stakeholder community, in order to avoid overlaps and duplication of efforts, but also to map out possible avenues for joint ventures and synergies, based on specific strategic objectives.

Annex

Annex 1: Stakeholder interview questionnaire

No.	Question	Rationale
1	What is the number of reported incidents on an annual basis? What is the most frequent type of these (e.g. DDoS, ransomware, etc.)?	To understand the existing scope of reporting and officially recognised trends in terms of attack and incident types.
2	Do you conduct any further analysis based on these reports in order to develop insights into the existing threat landscape based on which you can identify future expected trends, needs, etc.?	To understand whether relevant stakeholders (aim to) have a high-level understanding of the existing threat landscape based on which needs can be identified and possible future actions planned (human and financial resources, capacity, equipment and tools, cooperation channels and partnerships, outreach, etc.) .
3	To the best of your knowledge, how did threat actors successfully performing the reported incident gain a foothold into the victim's system or network (phishing, smishing, etc.). Do you have any statistical data on this?	To understand the methods employed for launching attacks. To understand whether these are investigated in order to harden the perimeters seen as vulnerable.
4	Who is the most common target and/ or victim of the recorded attacks (public institutions, private sector, etc.)?	To understand trends pertaining to targets (e.g. public or private sector; if public, what types of institutions; if private, what sector, size, etc.).
5	What do you see as the greatest incidents that took place at the national level? What were the effects/consequences? Any track record of costs and damage caused by these?	To map the greatest national-level incidents in order to compare these to national, regional and/or global trends. To collect material for sample cases to be highlighted in the report.
6	Did you notice any shifts in trends based on the recorded incidents (frequency, threat actors, targets)? Have stakeholders from your constituency express any specific needs or expectations they would want you to address/help them with?	To understand whether threat and attack patterns have evolved over time and how these are perceived in terms of possible shifts in needs, necessary approaches, etc.
7	Do you see any country or region-specific types of incidents taking place (i.e. as opposed to general global trends)?	To understand whether there are recorded (or perceived) national/regional outliers, specific to the Western Balkans, compared to general trends.

No.	Question	Rationale
8	How different do you think the situation is in reality (in terms of incident and attack frequency and number of actors) as opposed to official reports? What do you think the extent of this difference is (e.g. two times more, five times more?)?	To understand perceptions regarding the real-life state of affairs, based on general knowledge, experience and global trends, compared to the information officially available, which is based on the number of reports received (addressing thus one of the listed limitations as well).
9	What do you consider as the weakest links in the national cybersecurity ecosystem (specific actors, sectors, etc.)?	To understand perceptions regarding possible targets and compare these to existing instances of reported incidents (where applicable) and/or highlighted greatest incidents.
10	What do you see as the bigger risk: ● The level of sophistication of threats? ● Lack of awareness? ● Lack of capacity? ● Other?	To understand perceptions regarding existing risks, whether these are external or internal, which is indirectly linked also to the previous question.
11	Do you perform any type of attribution? If yes, do you have a specified methodology for assessing the probability/ certainty for such conclusions?	To understand the depth to which post-incident analysis is performed. If a methodology is employed, to understand whether there are defined levels of certainty for the attribution made (and the logic, methodology and approach behind these).
12	What do you see as the bigger threat: ● Large-scale APTs? ● Targeted attacks? ● Other?	To understand perceptions regarding the existing threat landscape and/or threat actors.
13	Are you aware of any cyber criminal group or APT originating from the Western Balkan region?	To understand whether there are any known (or assumed) threat actors specific to the region.
14	To the best of your knowledge, out of the identified threats and incidents, were any of these potentially state-sponsored?	To understand perceptions regarding the existence of state-sponsored attacks and/ or threat actors active in the region.
15	How do you assess your institution's/ organisation's capacity, or that of other relevant institutions/organisations at the national level to detect attacks independently and/or attribute these to specific threat actors? If limited or none, where do you get information, feeds and alerts from?	To understand perceptions regarding existing capacities to scope and analyse the existing threat landscape at the national level, and identify relevant actors and/or sources of information in this process.

No.	Question	Rationale
16	Do you have standing cooperation channels with peers or other relevant institutions/organisations at the regional level, or beyond? Which ones?	To understand existing cooperation channels at the bilateral, regional and/or global level.
17	Is this cooperation based on regular information exchange (e.g. tips, alerts, feeds) or does it also involve potential support in case of an incident (e.g. help in resolving, mitigation, recovery, etc.)?	To understand the nature of listed cooperation channels – whether these are solely for information exchange or are any recognised peers seen as having sufficient capacity to provide more concrete, operational support.
18	How do you see the cybersecurity threat landscape evolving in the short, medium and long term, both at the national level and regionally/globally?	To understand perceptions regarding upcoming, future developments in the cyber threat landscape at the national and regional level, based on general knowledge, experience and global trends.
19	What would be the consequences of such developments, and what future needs might it raise?	To understand perceptions regarding the effects of expected future developments in the cyber threat landscape at the national and regional level.

Annex 2: Mapped cooperation frameworks

A 2.1 Albania

Due to limited availability of publicly available documents in English, the list of cooperation frameworks identified for the purpose of this report is reduced to the MoUs listed below:

A 2.1.1 National CERT Memoranda of Understanding

No.	Year	Document	Counterpart	Content related to Cyber
1	2016	MoU between ALCIRT and KOS-CERT	Kosovo	The whole MoU defines the scope of cooperation between the national CERTs
2	2018	MoU between NAECCS, NAIS, and CERT-RO	Romania	The whole MoU defines the scope of cooperation between the national CERTs
3	2018	MoU between NAECCS, NAIS, and MKD-CIRT	North Macedonia	The whole MoU defines the scope of cooperation between the national CERTs

A 2.2 Bosnia and Herzegovina

A 2.2.1 Relevant international cooperation documents

No.	Year	Document	Counterpart	Content related to Cyber
1	2011	Agreement in Cooperation in the Field of Information Society and Electronic Communication	Croatia	The whole agreement serves as a basis for ICT cooperation
2	2011	Agreement on Fight against Criminal, in Particular Terrorism	Spain	Not possible to find online, but it probably has the provision related to cyber, as Serbia has a similar agreement from the same year.
3	2014	Agreement on Fight Against Criminal, in Particular Terrorism	Czech Republic	Art. 2 (scope of the agreement) mentions computer crime

No.	Year	Document	Counterpart	Content related to Cyber
4	2014	Agreement with OSCE on Security and Defence	OSCE	Not online. But cybersecurity is mentioned in annual cooperation plans determined on an annual basis: http://mod.gov.ba/aktuelnosti/vijesti/?id=61381
5	2016	Memorandum of Understanding in the Area of Information Technologies between Ministries of Foreign Affairs	Turkey	Not available online
6	2016	Agreement on Fighting Crime	Ukraine	Art. 2 (scope of the agreement) mentions cybercrime
7	2016	Agreement on Cooperation in Fighting Crime	Saudi Arabia	Art. 1 (scope of the agreement) mentions computer crime
8	2017	Agreement on Military Cooperation	Poland	Not available online. It likely contains provisions on cyber

A 2.3 Kosovo

A 2.3.1 Relevant international cooperation documents related to police cooperation, military defence cooperation, or ICT that are related to cyber

No.	Year	Document	Counterpart	Content related to Cyber
1	2010	Agreement on Cooperation In The Fields Of Military Training, Technique, Science	Turkey	Art. 4 (scope of the agreement) mentions cooperation on communication, electronics, and information systems.
2	2012	Agreement on Police Cooperation	Bulgaria	Art. 2 (scope of the agreement) mentions computer crime
3	2013	Agreement on cooperation on ICT	Albania	The whole agreement serves as a basis for cyber cooperation
4	2014	Agreement on Police Cooperation in Combating Crime	Switzerland	Art. 3 (scope of the agreement) mentions cybercrime

No.	Year	Document	Counterpart	Content related to Cyber
5	2014	Agreement on Police Cooperation	Montenegro	Art. 4 (scope of the agreement) mentions information technologies
6	2015	Security Cooperation Agreement	Albania	Art. 1 (scope of the agreement) mentions cybercrime
7	2021	Agreement on Police Cooperation	Italy	Art. 4 (scope of the agreement) mentions cybercrime

A 2.4 Montenegro

A 2.4.1 Relevant international cooperation documents related to security, police, cooperation in fighting organized crime, terrorism

No.	Year	Document	Counterpart	Content related to Cyber
1	2010	Agreement on Police Cooperation	Bulgaria	Art. 3 (scope of the agreement) mentions cybercrime.
2	2013	Agreement on Cooperation and Fight Against the Organized Crime	Czech Republic	Art. 3 (scope of the agreement) mentions computer crime
3	2013	Police cooperation Agreement	North Macedonia	Art. 2 (scope of the agreement) mentions computer crime
4	2013	Agreement on Cooperation in the Field of Information and Communication Technologies	Montenegro and Serbia	The whole agreement serves as a basis for tripartite cooperation in ICT
5	2014	Agreement on Police Cooperation	Kosovo	Art. 4 (scope of the agreement) mentions information technologies
6	2014	Agreement of Cooperation between Ministries of Interior	Russian Federation	Art. 2 (scope of the agreement) mentions Hi-Tech crime
7	2014	Memorandum of Understanding between the Ministry of Interior and OSCE Mission to Montenegro	OSCE	Art. 4 (scope of the agreement) mentions information technologies
8	2016	Agreement on Police Cooperation in Fight Against Crime	Switzerland	Art.3 (scope of the agreement) mentions computer crime

A 2.5 North Macedonia

Due to limited searchability of existing legal databases, a number of possibly relevant agreements have been identified but could not be verified for directly including cyber or ICT-related aspects within their scope. The list of cooperation frameworks identified for the purpose of this report is therefore reduced to the following:

A 2.5.1 Indicative list of recent agreements relevant to cyber, trust services or other tech-related areas

No.	Year	Document	Counterpart	Content related to Cyber
1	2021	Memorandum of understanding on cyber defence	NATO	The MoU facilitates information-sharing on cyber threats and best practices, helps prevent cyber incidents and will enable North Macedonia to increase its resilience to cyber threats

A 2.5.1 National CSIRT Memoranda of Understanding

No.	Year	Document	Counterpart	Content related to Cyber
1	2016	Memorandum of Cooperation between MKD-CIRT the national CERT of Moldova	Moldova	The whole MoC defines the scope of cooperation between the national CERTs
2	2017	Memorandum of Cooperation between MKD-CIRT and the national CERT of Slovenia (SI-CERT)	Slovenia	The whole MoC defines the scope of cooperation between the national CERTs
3	2018	Memorandum of Understanding between the National Authority on Electronic Certification and Cyber Security (NAECCS), National Agency for Information Society (NAIS) and the Agency for Electronic Communications (AEC) of the Republic of Macedonia, National Centre for Computer Incident Response (MKD-CIRT)	Albania	The whole MoU defines the scope of cooperation between the national CERTs

No.	Year	Document	Counterpart	Content related to Cyber
4	2018	Memorandum of Cooperation between the National Centre for Computer Incident Response (MKD-CIRT) and the National Cyber Security Unit (KOS-CERT) as part of the Regulatory Authority for Electronic and Postal Communications of the Republic of Kosovo (RAEPC)	Kosovo	The whole MoC defines the scope of cooperation between the national CERTs
5	2018	Protocol for cooperation between MKD-CIRT and SRB-CERT	Serbia	The Protocol defines the scope of cooperation between the national CERTs

A 2.6 Serbia

A 2.6.1 Relevant international cooperation documents related to security, police, cooperation in fighting organized crime, terrorism

No.	Year	Document	Counterpart	Content related to Cyber
1	2007	Agreement on Cooperation in the Fight against Organized Crime, International Illegal Drug Trade, and international Terrorism	Romania	Art. 1 (scope of the agreement) covers crimes against the security of computer data, information systems, and methods, as well as communication networks
2	2007	Agreement on Cooperation in the Fight Against Crime	Slovakia	Art. 1 (scope of the agreement) mentions computer crime
3	2008	Cooperation Agreement in the Fight Against Organized Crime, Drug Trafficking, and International Terrorism	Italy	Art. 2 (scope of the agreement) mentions computer crime
4	2009	Agreement on Cooperation in the Fight Against Terrorism, Organized Crime, Illicit Trafficking in Narcotic Drugs, Psychotropic Substances and their Precursors, Illegal Migration, and Other Criminal Offenses	Cyprus	Art. 3 (scope of the agreement) mentions cybercrime

No.	Year	Document	Counterpart	Content related to Cyber
5	2009	Agreement on Cooperation of Ministries of Interior	Russian Federation	Art. 3 (scope of the agreement) mentions cybercrime
6	2009	Agreement on Police Cooperation	France	Art. 2 (scope of the agreement) mentions Hi-Tech crime
7	2010	Agreement on Police Cooperation in Fight Against Crime	Czech Republic	Art. 2 (scope of the agreement) mentions cybercrime
8	2011	Agreement on Cooperation in the Fight Against Crime	Spain	Art. 1 (scope of the agreement) Mentions criminal acts committed through information systems
9	2011	Agreement on Cooperation in the Fight Against Organized and other Types of Crime	Poland	Art. 1 (scope of the agreement) mentions cybercrime
10	2013	Agreement on Cooperation in the Fight Against Crime	Lithuania	Art. 2 (scope of the agreement) mentions Crimes against the security of electronic data and information systems
11	2014	Memorandum of Understanding on Cooperation in the Fight against Organized Crime	UK	Art. 1 (scope of the document) mentions Hi-Tech Crime
12	2016	Agreement on Security Cooperation	Germany	Art. 1 (scope of the agreement) mentions Hi-Tech Crime
13	2017	Agreement on Cooperation and Joint Action with the Federal Security Service	Russia	Art. 2 (scope of the agreement) mentions “development and implementation of joint activities for neutralization computer attacks on vital state information resources.”
14	2017	Agreement on Cooperation in the Field of Law Enforcement	Sweden	Art. 1 (scope of the agreement) mentions Hi-Tech Crime
15	2018	Agreement about Cooperation in the Field of Information and Communication Technologies	Republika Srpska	The whole agreement on modalities of ICT cooperation between the two polices

No.	Year	Document	Counterpart	Content related to Cyber
16	2020	Agreement on Security Cooperation	Turkey	Art. 2 (scope of the agreement) mentions computer crime
17	2020	Agreement on Security Cooperation	Palestine	Art. 1 (scope of the agreement) mentions Hi-Tech Crime

A 2.6.2 Relevant international cooperation documents related to military and defence cooperation with other countries that have references to cyber

No.	Year	Document	Counterpart	Content related to Cyber
1	2017	Defence Cooperation Agreement	Romania	Art. 2 (scope of the agreement) mentions data, information, and communication technologies;
2	2020	Military Framework Agreement	Turkey	Art. 4 (scope of the agreement) mentions Communication, electronic means, information systems, and defence against attacks in the information space
3	2020	Defence Cooperation Agreement	Morocco	Art. 2 (scope of the agreement) mentions Information security and cyber defence

A 2.6.2 Relevant international cooperation documents related to ICT

No.	Year	Document	Counterpart	Content related to Cyber
1	2009	Memorandum of Understanding on Cooperation in Telecommunications and Information Technology	China	
2	2010	Memorandum on Understanding of Cooperation in the Field of Telecommunications	South Korea	Paragraph 2 mentions “Cooperation on Information Security.”

No.	Year	Document	Counterpart	Content related to Cyber
3	2012	Memorandum on Understanding of Cooperation in Information and Communication Technologies	USA	
4	2013	Agreement on Cooperation in the Field of Information and Communication Technologies	Montenegro and North Macedonia	The whole agreement serves as a basis for tripartite cooperation in ICT
5	2016	Memorandum of Understanding in the Field of E-Government	South Korea	
6	2016	A Memorandum of Understanding on the Cooperation in the field of Information Technology & Electronics	India	
7	2017	Memorandum on Understanding in the Field of Digitalization of Public Administration	Slovenia	Art. 1 mentions cooperation on “secure networking and data security (cyber security)”
8	2017	Strategic Partnership Agreement on the Development of Broadband Infrastructure between the Ministry of Trade, Tourism and Telecommunications and Huawei	Huawei (China)	
9	2018	Memorandum of Understanding Regarding Cooperation in Activities Related to Research and Development in Information and Communication Technologies	Turkey