ՆՈՅԵՄԲԵՐ • NOVEMBER 5
ԵՐԵՎԱՆ • YEREVAN 2024

# arm igf 9

## ԿԻԲԵՌԻՐԱԿԱՆՈՒԹՅՈՒՆ ԵՎ ԱՆՎՏԱՆԳ ԹՎԱՅԻՆ ԱՊԱԳԱ

## CYBER REALITY AND SECURE DIGITAL FUTURE

*Ինտերնետի կառավարման հայաստանյան համաժողով*

*Armenian Internet Governance Forum*

ԳՈՐԾԸՆԿԵՐՆԵՐ • PARTNERS »

ISOC.AM

U!com Platinum partner

Internet Society Foundation

RIPE NCC

ICANN

IGF Internet Governance Forum

Internet Society

IGFSA

» ԿԱԶՄԱԿԵՐՊԻՉՆԵՐ • ORGANIZERS

ՀՀ ԲԱՐՁՐ ՏԵԽՆՈԼՈԳԻԱԿԱՆ ԱՐԴՅՈՒՆԱԲԵՐՈՒԹՅԱՆ ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ

IGC | INTERNET GOVERNANCE COUNCIL OF THE REPUBLIC OF ARMENIA

ISOC.AM

Internet Society Armenia Chapter

#am30

#armigf2024

# *“Cyber reality and secure digital future”*
# *ArmIGF 2024*
# *REPORT*

arm igf 9

# Content

**What is IGC and ArmIGF?**
ArmIGF 2024
ArmIGF 2024 partners
Organizing committee

**ArmIGF 2024 program**

- ❑ Opening ceremony
- ❑ Armenia at a Digital Crossroad - how to build and lead the Armenian Digital Navy?
- ❑ Issues of Personal Data Protection in Newly Adopted Legal Acts: Challenges and Solutions
- ❑ Lunch
- ❑ Cybersecurity Challenges and Issues: Global Best Practices and International Collaboration
- ❑ WSIS+20 updates in the frames of events on 2024, Future of the IGF, Global Digital Compact and analysis of the Summit of the future
- ❑ National Content and ccTLDs: Strategies for Growth and Overcoming Challenges
- ❑ Closing

Session discussions
Participation
Coverage - Media, TV, Radio
Thank you

# What is IGC and ArmIGF

IGC | INTERNET GOVERNANCE COUNCIL OF THE REPUBLIC OF ARMENIA

ՀՀ ԲԱՐՁՐ ՏԵԽՆՈԼՈԳԻԱԿԱՆ ԱՐԴՅՈՒՆԱԲԵՐՈՒԹՅԱՆ ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ

arm igf 9

ISOC.AM

The Internet Governance Council (IGC) of the Republic of Armenia is a multistakeholder body comprising representatives from the government, business sector, academia, media, and non-governmental organizations.

The Council's primary objective is to address challenges by incorporating the perspectives of all relevant stakeholders into its decision-making processes. Committed to transparency, the IGC shares updates about its activities through its official website, ***igc.am***. As internet governance evolves alongside the rapidly advancing information society, innovative approaches to governance are essential.

The IGC’s success relies heavily on its Charter and active public engagement. Chaired by the Deputy Minister of High-Tech Industry, the Council is supported by the "Internet Society" NGO, which manages the **.am/.հայ ccTLD** Registry and acts as its secretariat. For more information, visit the official website at ***igc.am***.

In partnership with the **RA Ministry of High-Tech Industry**, the **IGC**, the **Internet Society NGO**, and the **Internet Society Armenia Chapter PO**, the Armenian Internet Governance Forum (**ArmIGF**) was established as a national initiative.

***Armenia joined the global Internet Governance Forum in 2015, marking the occasion with the country's inaugural internet governance conference.***
***ArmIGF serves as a transparent, inclusive, and open platform for dialogue and collaboration on internet governance matters.***

***8***
***FORUMS***

***900+***
***Participants***

***230+***
***SPEAKERS***

***105+***
***TOPICS***

# *ARMIGF 2024*

The Armenian Internet Governance Forum (IGF) 2024 took place on November 5 at the Marriott Hotel, with around 120 participants in attendance. The event also utilized Zoom and live streaming on YouTube to reach a wider audience.

Discussions focused on critical topics such as Armenia's digital development, personal data protection in light of recent legal changes, cybersecurity challenges and international collaboration, updates on WSIS+20 and the Global Digital Compact, as well as strategies for fostering national content and managing ccTLDs.

The forum concluded with a Q&A session that reflected on the discussions and highlighted key outcomes.

The **ArmIGF 2024** program was developed by the organizing committee, which included representatives from various stakeholder groups, such as the public and private sectors. Registration for the event was open on the website from October 5 to October 25.

## About ArmIGF

- It is an annual forum.
- Brings together representatives from government, civil society, and private sectors.
- Provides a platform to discuss internet governance issues, share information, and exchange best practices.
- Aims to foster the development of internet opportunities, address emerging risks and challenges, and promote a shared understanding and resolution of key issues.

# ArmIGF 2024 Partners

ISOC.AM

IGF

Internet Society

RIPE NCC

Internet Society Foundation

U!com®

IGFSA Internet Governance Forum Support Association

ICANN

# *ArmIGF 2024 Organizing and Coordinating Team*

**Internet Governance Council**

Kristina Hakobyan - IGC member, ISOC NGO board member
Aleksey Sandikov - IGC member, Parliament member of the RA
Vahan Hovsepyan - IGC member, RIPE NCC Caucasus and Central Asia External Relations Director

**Internet Society NGO**

Katarina Gevorgyan - ISOC NGO board member, Manager of external relations of NGO
Vesmira Harutyunyan - ISOC Armenia chapter PO board chair
Narine Derdzakyan - ISOC Armenia chapter PO board vice-chair

**PR and technical team members**

Lillit Galstyan – PR manager
Nana Poghosyan – Content manager
Aram Verdyan - ISOC NGO board member
Ashot Harutyunyan – Tech support

# ArmIGF 2024 program

05.11.24
YEREVAN
arm igf 9
ԿԻԲԵՌԻՐԱԿԱՆՈՒԹՅՈՒՆ
ԵՎ ԱՆՎՏԱՆԳ ԹՎԱՅԻՆ ԱՊԱԳԱ
CYBER REALITY AND SECURE DIGITAL FUTURE
Ինտերնետի կառավարման հայաստանյան համաժողով
Armenian Internet Governance Forum
IGC
ISOC.AM
ICANN
RIPE NCC
IGF
IGFSA

**09:00 - 10:00**
**Registration**

# *10:00 - 10:45* *Opening ceremony*

- ❑ **Gevorg Mantashyan** – First Deputy Minister of of High Tech Industry of the RA
- ❑ **H.E. Mr. John Gallagher** – British Ambassador to Armenia
- ❑ **Igor Mkrtumyan** – Chair of the Board, Internet Society NGO
- ❑ **Mikhail Anisimov** – Head of Global Stakeholder Engagement for Eastern Europe and Central Asia, ICANN
- ❑ **Vahan Hovsepyan** – RIPE NCC, Senior Community and Public Policy Advisor, Internet Governance Council of RA member
- ❑ **Nick Hyrka** – Community engagement manager for the European region at the Internet Society
- ❑ **Ralph Yirikian** – General Director of Ucom
- ❑ **Andrey Vorobyov** – Coordination Center for TLD .RU/.РФ, Director

# 10:45 - 12:00 *Armenia at a Digital Crossroad - how to build and lead the Armenian Digital Navy?*

- ❑ **Gevorg Mantashyan** – First Deputy Minister of High Tech Industry of the RA
- ❑ **Hrachya Arzumanian** – An expert on national security issues

**Moderator:**

**Vahan Hovsepyan –** RIPE NCC, Senior Community and Public Policy Advisor, Internet Governance Council of RA member

# *12:00 - 13:00 Issues of Personal Data Protection in Newly Adopted Legal Acts: Challenges and Solutions*

- ❑ **Samvel Martirosyan -**Director of the ArmSec foundation, co-founder of CyberHub
- ❑ **Hakob Sununu -** Director of Quality Management & Risk Control at UCOM
- ❑ **Artur Sargsyan -** Senior law adviser at ISAA

**Moderator:**
**Gevorg Hayrapetyan** – Personal data protection expert, CyberHub, dpHub

# *14:00 - 15:00 Cybersecurity Challenges and Issues: Global Best Practices and International Collaboration*

- ❑ **Nerses Yeritsyan** - Director of Information Systems Agency of Armenia
- ❑ **Karen Gasparyan -** Executive Director of “INFOSEC” LLC
- ❑ **Hayk Mkrtchyan -** Head of the Division of Combating Cybercrimes of the Main Department of the Criminal Police of the RA Ministry of Internal Affairs Police
- ❑ **Markko Kunnapu -** Ministry of Justice of Estonia, Criminal Policy Department, Adviser

**Moderator:**

- ❑ **Armine Arzumanyan -** AUA College of Science and Engineering

# *15:00 - 16:00 WSIS+20 updates in the frames of events on 2024, Future of the IGF, Global Digital Compact and analysis of the Summit of the future*

- ❑ **Aleksey Sandikov -** IGC member, Parliament member of the RA
- ❑ **Chris Buckridge -** Senior Strategy Advisor Global Forum on Cyber Expertise (GFCE) (online)
- ❑ **Veni Markovski -** ICANN, Vice-President for UN engagement (online)
- ❑ **Amrita Choudhury -** Chair IGFSA, Chair APRALO (online)

**Moderator:**

- ❑ **Mikhail Anisimov** – ICANN, Head of Global Stakeholder Engagement for Eastern Europe and Central Asia

# *16:15 - 17:00* *National Content and ccTLDs: Strategies for Growth and Overcoming Challenges*

- ❑ **Kristina Hakobyan -** Vice Chair of the board “Internet Society” NGO, .am/.հայ registry
- ❑ **Irina Danelia -** Coordination Center for .RU ccTLD/.РФ deputy director
- ❑ **Sophie Khidasheli -** Senior Specialist of .GE ccTLD Registry (online)
- ❑ **Dejan Dukic -** CEO RNIDS.RS (online)
- ❑ **Azizbek Kadirov -** .uz ccTLD administration, UZINFOCOM (online)

**Moderator:**
**Maria Kolesnikova -** Coordination Center for TLD RU, Chief Analyst

arm igf 9

## *17:00 – 17:45 Wrap up, closing*

arm igf 9

# *Opening Ceremony*

- **Gevorg Mantashyan** – First Deputy Minister of High Tech Industry of the RA
- **H.E. Mr. John Gallagher** – British Ambassador to Armenia
- **Igor Mkrtumyan** – Chair of the Board, ISOC NGO
- **Mikhail Anisimov** – Head of Global Stakeholder Engagement for Eastern Europe and Central Asia, ICANN
- **Vahan Hovsepyan** – RIPE NCC, Senior Community and Public Policy Advisor, Internet Governance Council of RA member
- **Nick Hyrka** – Community engagement manager for the European region at the Internet Society
- **Ralph Yirikian** – General Director of Ucom
- **Andrey Vorobyov** – Coordination Center for TLD .RU/.PФ, Director

arm igf 9

As the forum moderator, Nana Petrosyan, member of the PR group of ISOC NGO, warmly welcomed distinguished guests and all participants, both in-person and online, at the opening of the Armenian Internet Governance Forum 2024.

She provided a comprehensive overview of the event, detailing the structure and key aspects of ArmIGF9. Her guidance ensured that all attendees were well-informed and ready to navigate the day’s sessions smoothly.

She also shared her heartfelt wishes for a productive and dynamic forum, encouraging meaningful discussions and collaboration among all participants, regardless of their mode of attendance.

**Gevorg Mantashyan**, the First Deputy Minister of High-Tech Industry of the Republic of Armenia, opened the forum by welcoming attendees and wishing them a productive and successful session. In his remarks, he emphasized Armenia’s commitment to fostering a safe, innovative, and inclusive digital environment.

“***We believe the Internet should be a space where people can express themselves freely and feel completely safe. In our digitalization agenda, we place great emphasis on staying ahead in terms of cybersecurity and ensuring a cyber-safe environment when developing digital solutions***,” *he stated.*

The Deputy Minister also underscored the critical role of technology in addressing modern challenges. Highlighting Armenia’s efforts to combat misinformation, he shared examples of using advanced technologies such as antivirus systems, machine learning tools, and data analysis platforms to detect and neutralize online threats.

Additionally, he emphasized the importance of balancing technological advancement with ethical responsibility.

***"While we work to enhance cybersecurity, we remain deeply committed to preserving the principles of a free and open Internet,"*** he noted, calling for a unified approach to value-driven innovation.

He also touched upon the need for collaborative efforts across sectors to address the dynamic challenges of digitalization and ensure a sustainable, secure, and inclusive digital future for all.

His remarks set a strong tone for the forum, resonating with the themes of collaboration, resilience, and ethical progress that were echoed throughout the event.

**H.E. Mr. John Gallagher** – British Ambassador to Armenia highlighted the critical importance of addressing the challenges posed by the rapidly evolving digital world.
He emphasized that overcoming these challenges requires a collaborative and inclusive approach, bringing together governments, private sector leaders, civil society, and individuals.

The Ambassador underscored that harnessing the potential of digital technologies can drive societal progress, bridge divides, and create opportunities for all. By fostering partnerships, promoting innovation, and ensuring equitable access to digital tools, he noted, we can build a resilient digital future that empowers communities and strengthens global connections.

***His Excellency reaffirmed the United Kingdom's commitment to work.***

arm igf 9

In his welcoming speech at the 9th annual Armenian Internet Governance Forum (ArmIGF), **Igor Mkrtumyan**, Board Chair of the "Internet Society" NGO, reflected on the importance of this event in fostering dialogue and cooperation in Internet governance.

He emphasized that by initiating the IGF for the ninth consecutive time, Armenia had successfully established a platform that unites all stakeholders—government, civil society, academia, and the private sector—to engage in meaningful discussions and collaborations on the future of the Internet.

Mkrtumyan highlighted that this platform serves as a cornerstone for large-scale cooperation, enabling the exchange of ideas and best practices to address critical challenges and seize emerging opportunities in the digital space. He noted that the forum is particularly significant this year, as it coincides with the 30th anniversaries of the "Internet Society" NGO and the .am ccTLD, both of which have played pivotal roles in advancing Armenia’s digital development.

Over the past three decades, these efforts have created invaluable opportunities for the public, including improved access to education, the promotion of economic growth, and enhancements to societal well-being.

Over the past three decades, these efforts have created invaluable opportunities for the public, including improved access to education, the promotion of economic growth, and enhancements to societal well-being.

These accomplishments, he remarked, are a testament to the power of collaboration and the shared vision of all stakeholders involved in building Armenia’s digital ecosystem.
Looking to the future, Mkrtumyan called on participants to use this milestone as an opportunity to plan for the next decades of digital progress.

He urged stakeholders to focus on sustainable development, inclusivity, and innovation, ensuring that the digital landscape continues to evolve in ways that benefit all citizens.In conclusion, Mkrtumyan reaffirmed the commitment of the "Internet Society" NGO and the .am ccTLD to advancing Internet governance and fostering a digital environment that is secure, open, and accessible to everyone. He expressed gratitude to all those who have contributed to the success of ArmIGF and encouraged participants to actively engage in shaping the future of Armenia’s digital journey.

This is truly a wonderful gathering! - remarked **Mikhail Anisimov**, Head of Global Stakeholder Engagement for Eastern Europe and Central Asia at ICANN.

He commended ArmIGF for consistently standing out as a vital initiative for representatives of various stakeholder groups.
***Armenia has demonstrated remarkable leadership and participation in Internet governance processes, setting an example among other countries,-*** Mikhail Anisimov noted.

Anisimov also emphasized the importance of the WSIS+20 process, noting its role in shaping the future of global digital cooperation and ensuring inclusive multistakeholder engagement. He encouraged Armenia and other countries in the region to actively contribute to these discussions to help align global and regional priorities.

***"I am genuinely excited to see this ambition come to fruition and look forward to the continued contributions Armenia will make in advancing global Internet governance,"*** he added.
Anisimov concluded by expressing gratitude for the opportunity to participate in the discussions at ArmIGF 2024, emphasizing the importance of collaboration and shared vision in shaping the Internet's future.

**Vahan Hovsepyan**, RIPE NCC External Relations Officer, extended a warm welcome and expressed gratitude to the representatives of the government, the technical community, and all distinguished attendees for their presence at ArmIGF 2024.

He emphasized the importance of the RIPE NCC's initiatives in fostering Internet development and their growing significance in the region.

***Events like ArmIGF, which bring together diverse stakeholders to address policy development, Internet governance, and technical challenges, are vital for shaping the future of the digital ecosystem. These platforms not only facilitate the discussion of critical issues but also serve as incubators for innovative solutions and collaborative approaches to Internet governance.***

Hovsepyan highlighted that global challenges in Internet governance often have local implications, making forums like ArmIGF essential for addressing issues that resonate deeply within the region.

***"For landlocked countries like Armenia," he noted, "the Internet is our sea—a vast domain of opportunity that can overcome the geographical and economic limitations we face."***

He stressed that embracing the growth of the Internet offers Armenia significant prospects for development and progress.

Finally, he underscored the importance of looking toward the future: ***"The path ahead leads us to a new digital Armenia—a digital society that will define our success. It is crucial that we move boldly in this direction to unlock the full potential of our nation in the digital age."***

arm igf 9

The 9th annual ArmIGF commenced with an inspiring address by **Nick Hyrka**, the Community Engagement Manager for the European region at the Internet Society. He warmly welcomed attendees, emphasizing the significance of the event and congratulating everyone involved in making the forum a reality.

Hyrka commended the dedication of all stakeholders in advancing Internet governance in Armenia, calling their efforts both commendable and inspiring.

This year's forum also marks a milestone—the 30th anniversary of Armenia's national .am domain. Hyrka acknowledged this remarkable achievement as a testament to three decades of digital progress and Armenia's lasting presence in the global online community. He extended heartfelt congratulations to the Armenian ccTLD registry for its impressive journey.

Also, highlighted the fruitful collaboration between the Internet Society and its Armenian Chapter, led by Igor Mkrtumyan and his team. This partnership has played a pivotal role in building a vibrant Internet community in Armenia and beyond. He also acknowledged the Armenian Chapter's critical efforts in fostering a multi-stakeholder approach to Internet governance, uniting government, civil society, academia, and the private sector.

This inclusive model enriches discussions and ensures that diverse voices are represented in shaping Armenia's digital future.

Special recognition was given to the Internet Governance Council of Armenia, which exemplifies the collaborative spirit. Comprised of representatives from various sectors, the council actively addresses emerging Internet governance challenges while promoting best practices. It serves as a platform for meaningful dialogue and decisive action, ensuring that Armenia remains at the forefront of digital innovation.

In his address, Hyrka encouraged participants to actively engage, share insights, and envision bold possibilities. He underscored the importance of discussions on issues such as connectivity, cybersecurity, and digital inclusion, emphasizing Armenia’s inspiring digital journey as a model of what can be achieved through vision and collaboration.

He also reminded attendees of the global responsibility they bear. Nearly a third of the world’s population remains unconnected or experiences poor connectivity, and  highlighted the broader impact of Internet governance forums, noting that discussions held at such events influence the global digital landscape and give a voice to the unconnected.

On behalf of the Internet Society, which envisions an open, globally connected, secure, and trustworthy Internet for everyone, Hyrka expressed gratitude for the commitment to advancing Internet governance in Armenia. He closed his remarks by encouraging all attendees to make the most of the forum and to look forward to continued digital progress and innovation in the years to come.

***At Ucom, we firmly believe that internet security is a cornerstone of the new digital era, where every individual deserves the ability to access online services with confidence***,- stated Ucom's General Director, **Ralph Yirikian**.

He further elaborated that while digitalization is a vital driver of innovation, economic growth, and social development, it also introduces complex risks that must be addressed proactively. ***"As we embrace the opportunities of a more interconnected world, we must recognize the growing challenges, such as data breaches, cyberattacks, and misinformation, that threaten user safety and trust."***

To tackle these challenges, Yirikian emphasized the importance of going beyond technological solutions. "***Technology alone cannot solve these issues. We need a collective approach that includes collaboration among stakeholders—government bodies, businesses, civil society, and individual users. At the same time, fostering a culture of digital responsibility and awareness is crucial for building a secure and trustworthy online environment***," he said.

Yirikian reaffirmed Ucom's commitment to investing in advanced technologies, educating users on safe internet practices, and working closely with partners to create a resilient digital ecosystem that benefits everyone.

***"Our goal is to ensure that digitalization becomes a force for good, empowering users while safeguarding their rights and security,"*** he concluded.

On behalf of the Coordination Center for TLD .RU/.РФ the director **Andrey Vorobyov** extended his gratitude for the invitation to this significant occasion.

***Over the years, the Coordination Center for TLD .RU/.РФ has maintained a strong and productive collaboration with the .am ccTLD registry, sharing a rich history that spans decades.***
As the .am domain celebrates its 30th anniversary, Vorobyov congratulated the registry on reaching this remarkable milestone.

He highlighted the growing importance of active participation in Internet governance processes in today's interconnected world. A key priority is creating an environment that fosters innovation, raises awareness, and promotes digital literacy among users of all ages, particularly the younger generation.
To achieve this, the Coordination Center has launched numerous educational initiatives. These include direct outreach to children and students, teaching them safe and effective ways to navigate the internet while enhancing their digital competencies.
Additionally, the Center is well-known for organizing summer Internet Governance Schools, providing young people with invaluable insights and tools to engage in critical areas such as internet governance, cybersecurity, artificial intelligence, and more. Through these efforts, the Coordination Center continues to play a pivotal role in shaping a safe, innovative, and inclusive digital ecosystem.

# *Armenia at a Digital Crossroad - how to build and lead the Armenian Digital Navy?*

- ❑ **Arshak Kerobyan –** Head of digitalisation department of the Ministry of  High Tech Industry of the RA

- ❑ **Hrachya Arzumanian –** An expert on national security issues

- ❑ **Moderator: Vahan Hovsepyan –** RIPE NCC, Senior Community and Public Policy Advisor, Internet Governance Council of RA member

***The Digital Era creates enormous opportunities for small countries to have exponential growth. However, to utilize this opportunity there is a need to create a Digital Economy, make necessary changes in the public and social infrastructures, governing structures, create a true Digital Fleet to overcome Digital Challenges and use all the opportunities of Digital Opportunities.***
***How Armenia can lead regional developments in this field,***
***what infrastructures and core reforms should be done?***

**Vahan Hovsepyan,** Senior Community and Public Policy Advisor at RIPE NCC and the member of the Internet Governance Council of RA started the panel with the key points:

## Why Armenia: Technical Feasibilities

***Presence of OVIO Tier 3 Data Center with advanced collocation capabilities:***

❑ 200 racks for collocation.
❑ Public and private cloud solutions (OVIO Cloud, gCloud) based on VMware.
❑ Thousands of CPU cores and terabytes of enterprise-grade storage.
❑ Comprehensive storage and backup capacities.

## Why Armenia: Geopolitical Implications

***Central Hub*****:** Armenia’s location at the crossroads of Europe and Asia makes it an ideal hub for digital and physical connectivity. It offers shorter, more direct data transmission routes between continents.

***Proximity to Key Markets*****:** Close to Russia, Iran, Turkey, and the broader Middle East, boosting its potential as a central digital infrastructure point.

**He emphasized Armenia's unique position and infrastructure as pivotal in the future of global digital communications.**

- Armenia's strategic position and robust infrastructure can capitalize on global data traffic growth (estimated at 25% annually).
- The country’s geographic location, technological capabilities, and economic environment position it as a key player in global digital communications.
- Armenia has the potential to bridge Europe and Asia with fiber optic connectivity, driving economic growth and enhancing global data exchanges.

Hovsepyan highlighted that, back in 2018, the Ministry of High-Tech Industry of the Republic of Armenia made a strategic decision to focus on four key areas for technological advancement: artificial intelligence (AI), blockchain technologies, semiconductor technologies, and cybersecurity.

These priorities reflect Armenia's commitment to fostering innovation and strengthening its position in the rapidly evolving global tech landscape.

**Hrachya Arzumanian**, a prominent expert on national security, shared insights into the strategic measures required to address the challenges of digital transformation and infrastructure development. He emphasized that adopting a singular strategy is insufficient for managing the complexities of today's digital landscape. Instead, he proposed a multi-faceted approach, where distinct types of strategies are developed and pursued in parallel.

According to Arzumanian, the first type of strategy should be global in nature, outlining the overarching vision and objectives for digital progress. The second is an implementation strategy, focusing on the practical steps needed to achieve this vision. He highlighted the critical importance of defining a clear roadmap for the development of critical infrastructure, ensuring that every step aligns with the broader goals of national digitalization.

Arzumanian stressed the need for the government to adopt a synchronized approach, where all strategies—whether related to infrastructure, security, or digital innovation—are harmonized.

This calls for a comprehensive, systemic framework that avoids fragmentation and ensures seamless coordination across different sectors and initiatives.

He also pointed out the rapid pace of digitalization happening on a global scale. To remain competitive and secure in this dynamic environment, Armenia must not only keep pace with these developments but also proactively position itself as a leader in innovation and resilience.

By staying agile and forward-thinking, the nation can effectively navigate the challenges of the digital era while maximizing opportunities for growth and security.

# *Issues of Personal Data Protection in Newly Adopted Legal Acts: Challenges and Solutions*

- ❑ **Samvel Martirosyan -**Director of the ArmSec foundation, co-founder of CyberHub
- ❑ **Hakob Sununu -** Director of Quality Management & Risk Control at UCOM
- ❑ **Artur Sargsyan -** Senior law adviser at ISAA

- ❑ **Moderator: Gevorg Hayrapetyan** – Personal data protection expert, CyberHub, dpHub

***The session on "Personal Data Protection in Newly Adopted Legal Acts" explored the complexities and challenges posed by recently introduced data protection laws.***

***It focused on navigating compliance with evolving regulations, ensuring effective enforcement mechanisms, and addressing the critical need to safeguard privacy in an increasingly digital world.***

**Gevorg Hayrapetyan**, the moderator of the session on "Personal Data Protection in Newly Adopted Legal Acts" at ArmIGF 2024, opened the discussion by emphasizing the relevance and urgency of the topic. He highlighted how the rapidly evolving digital landscape had brought personal data protection to the forefront of legal, technical, and societal debates.

Hayrapetyan noted that the session aimed to delve into the challenges posed by recently introduced data protection laws, particularly in the context of compliance, enforcement, and safeguarding individual privacy in the digital age. He stressed the importance of understanding how these laws impact various stakeholders, from government agencies and private sector organizations to civil society and individuals.

Welcoming the panelists, who represented diverse expertise in legal, technical, and policy fields, Hayrapetyan encouraged them to share their insights on the practical implications of these legal frameworks. He set the stage for a comprehensive discussion on aligning regulatory compliance with the evolving needs of digital ecosystems and exploring steps to ensure robust enforcement mechanisms that uphold privacy rights.

Throughout the session, Hayrapetyan facilitated an engaging dialogue, ensuring that the discussion remained focused on the pressing challenges and opportunities surrounding personal data protection.

He also encouraged audience participation, inviting questions and comments to enrich the conversation and address concerns relevant to both local and global contexts.

In his concluding remarks, Hayrapetyan reflected on the session's key takeaways, emphasizing the importance of collaboration among stakeholders to create effective, inclusive, and enforceable data protection frameworks. He reiterated that safeguarding privacy was not just a legal obligation but a shared responsibility in building trust in the digital age.

arm igf 9

**Samvel Martirosyan,** Director of the ArmSec foundation, addressed the critical and conceptual nature of personal data protection, emphasizing that its effectiveness depends heavily on the model a country adopts. He explained that different nations implement diverse approaches and laws, and the choice of model significantly influences the outcomes.

Martirosyan highlighted a pressing issue currently unfolding—the introduction of extensive camera systems for public surveillance. He expressed concern over the lack of public awareness regarding these systems, attributing it to societal passivity, which he described as a significant problem. He noted that the police were planning to monitor individuals who were often unaware of being observed, raising ethical and transparency concerns.

Delving deeper, Martirosyan questioned the conceptual approach being adopted in Armenia. He pointed out that policymakers often cite examples from countries with vastly different realities as positive benchmarks. However, he stressed the importance of tailoring approaches to the specific social, cultural, and legal context of Armenia rather than blindly replicating foreign models.

He underscored the need to clearly define the type of personal data to be protected and to establish its importance within the broader framework of national priorities. Striking a balance between national security and personal data protection, he argued, was critical because the two objectives often stand in tension with one another. Without careful consideration, measures aimed at protecting one could inadvertently undermine the other.

Martirosyan also raised concerns about the unintended consequences of data protection systems. He warned that small businesses, while often contributing positively to technological advancements, could inadvertently help create systems that, if misused, might compromise national security. He cautioned against building mechanisms that could be exploited for harmful purposes, highlighting the need for robust safeguards and ethical guidelines.

In conclusion, Martirosyan called for a thoughtful and context-sensitive approach to personal data protection in Armenia. He emphasized the importance of public awareness, balanced policies, and a commitment to ensuring that technology serves to enhance security and individual rights without enabling potential misuse.

**Hakob Sununu,** Director of Quality Management and Risk Control at UCOM, raised critical concerns about the potential impact of the Law on the Installation of Video Cameras, urging for a careful evaluation of whether its implementation would ultimately benefit society or harm its interests. He emphasized the need for a balanced approach to ensure that such initiatives align with the broader goals of privacy and security.

As an operator, Sununu shared firsthand challenges his company frequently encounters in the realm of personal data protection. He highlighted the prevalence of unlicensed equipment imports to Armenia, which pose significant risks to data security. Many of these products, particularly unlicensed equipment from Chinese manufacturers, allow for tracking and surveillance without the buyer's explicit understanding or consent.

Sununu underscored his company's commitment to maintaining high standards in the protection and processing of customers' personal data. He proudly noted that Ucom achieved the ISO 27001 security certification last year, a globally recognized standard that demonstrates excellence in information security management systems.

However, he expressed concern over the unintended consequences of the new law. Under its provisions, many companies are being compelled to purchase video cameras from unlicensed suppliers, a move that could exacerbate existing problems. He warned that relying on such equipment could lead to significant vulnerabilities in the protection of personal data, undermining the very purpose of the law.

Sununu concluded by emphasizing the need for stricter regulations and better oversight to prevent the proliferation of unlicensed equipment.

He stressed the importance of ensuring that data protection remains a priority, both in terms of legislation and implementation, to safeguard the rights and privacy of Armenian citizens.

**Artur Sargsyan** emphasized the pressing need for a coordinated framework in personal data protection, warning of significant risks in its absence. He explained that as methods and technologies for processing personal data evolve, the associated security risks naturally increase, creating vulnerabilities that demand immediate attention.

Sargsyan acknowledged that the newly adopted law introduces a data classification system, which represents a crucial step toward improving data protection. However, he stressed that the success of this system relies on its proper implementation. To achieve this, he called for a concerted effort involving communities and state bodies to conduct explanatory work.

This outreach is vital for ensuring a clear understanding of the system and its correct application across all levels of society.

He underlined the importance of developing comprehensive guidelines to standardize and support the system's application.
Even with certain issues addressed at the legal level, Sargsyan cautioned that practical implementation would inevitably uncover new risks and challenges.

These could include misinterpretations, operational inefficiencies, or gaps that need to be addressed to ensure the system’s effectiveness.

In conclusion, Sargsyan urged stakeholders to prioritize coordinated efforts, education, and the development of clear protocols. By doing so, he argued, Armenia can navigate the complexities of personal data protection and establish a robust, secure system that meets the needs of its citizens and institutions.

# *Cybersecurity Challenges and Issues: Global Best Practices and International Collaboration*

- □ **Karen Gasparyan -** Executive Director of “INFOSEC” LLC
- □ **Hayk Mkrtchyan -** Head of the Division of Combating Cybercrimes of the Main Department of the Criminal Police of the RA Ministry of Internal Affairs Police
- □ **Markko Kunnapu -** Ministry of Justice of Estonia, Criminal Policy Department, Adviser
- □ **Shant Kassardjian -** Cybersecurity Advisor at the Information Systems Agency of Armenia
- □ **Moderator: Armine Arzumanyan -** AUA College of Science and Engineering

***Cybersecurity challenges are vast in the digital age, ranging from safeguarding personal data to securing critical infrastructure, managing emergencies, and ensuring coordinated responses. To address these issues, various countries have implemented a wide range of legislative and regulatory measures.***

***The speakers shared their countries’ leading practices and offered insights into their approaches to tackling these challenges.***

**Armine Arzumanyan**, a lecturer in cybersecurity governance at the American University of Armenia, opened the panel with reflections on the concept of comprehensive cybersecurity, highlighting its relevance in today's rapidly evolving digital landscape.

Arzumanyan noted that humanity stands at the crossroads of technological innovation, societal transformation, and escalating cyber threats. She emphasized the necessity of navigating these complexities while safeguarding security, resilience, and democratic values.
She underscored that cybersecurity is no longer limited to the domain of IT departments or security operations centers.

The digitalization of critical infrastructure—spanning power grids, water systems, healthcare, and financial services—has brought tremendous benefits but also introduced significant vulnerabilities. Arzumanyan stressed the importance of robust cybersecurity regulations, particularly national cybersecurity policies and standardized frameworks for protecting critical infrastructure. She warned that the most sophisticated cyber tools and attacks increasingly target digitalized infrastructure, posing threats to daily life, economic stability, and national security.

The discussion extended to other pressing concerns in cyberspace, including cybercrime. Arzumanyan described cybercrime as a multifaceted issue encompassing financial fraud, identity theft, ransomware, data trafficking, and even human and narcotics trafficking. Cybercriminals exploit the anonymity and global reach of cyberspace, creating challenges for national law enforcement agencies, which often lack the jurisdiction to effectively prosecute transnational offenders. This globalized nature of cybercrime demands coordinated international efforts and robust public-private partnerships.

Arzumanyan argued for a holistic approach to cybersecurity, integrating diverse perspectives from the public sector, private industry, academia, law enforcement, and international organizations. This comprehensive cybersecurity framework, she explained, must address policy development, legal structures, cyber defense, international cooperation, and the human dimension, emphasizing awareness and digital citizenship.
She advocated for institutionalized and systemic collaboration among cybersecurity stakeholders and highlighted her role as an academic in bridging theoretical insights with practical applications.

Her efforts aim to foster dialogue, advance research, and train the next generation of cybersecurity professionals. Arzumanyan also mentioned Armenia's progress in developing its first cybersecurity law, a draft that incorporates the principles of comprehensive cybersecurity. She pointed out that the panel itself exemplifies this holistic approach, with each speaker addressing different facets of cybersecurity challenges and solutions.

**Karen Gasparyan** provided valuable insights from the frontline of cybersecurity operations within the private sector, a domain that played an essential role in the broader cybersecurity ecosystem. With the majority of critical infrastructure—such as energy grids, communication networks, healthcare systems, and financial institutions—being privately owned and operated, the private sector was uniquely positioned to address many of the most pressing cybersecurity challenges of the time.

He highlighted how the private sector’s contribution had been pivotal not only in developing advanced cyber tools and defenses but also in continuously innovating to stay ahead of ever-evolving cyber threats. Companies in this space had invested heavily in research and development, creating sophisticated technologies such as artificial intelligence-driven threat detection systems, encryption protocols, and automated incident response frameworks.

These tools were described as crucial for securing critical assets and ensuring operational continuity in the face of increasingly complex attacks. Beyond technological innovation, the private sector had played a significant role in shaping industry standards and practices that governed cybersecurity.

By establishing best practices, companies had promoted consistency and resilience across industries, ensuring that cybersecurity measures were robust and universally applied. Gasparyan noted that private sector organizations had also engaged in sharing threat intelligence through platforms like Information Sharing and Analysis Centers (ISACs), which had helped improve situational awareness and preparedness across various sectors.

Additionally, he emphasized that the private sector had often acted as a bridge between government agencies and individual users. Through participation in public-private partnerships, businesses had contributed their expertise, resources, and on-the-ground experience to national and international efforts. They had played an active role in shaping cybersecurity policies, regulations, and frameworks that were both effective and feasible for implementation, also noted that the private sector had been instrumental in fostering a culture of cybersecurity awareness among its workforce and the public. Many organizations had invested in comprehensive training programs to upskill their employees, ensuring that cybersecurity best practices were deeply ingrained within their operational culture.

These insights illustrated how the private sector had not only safeguarded its own interests but also contributed to the broader effort of protecting critical infrastructure, shaping global standards, and collaborating with governments and other stakeholders to build a safer digital world. By leveraging its expertise and innovation, the private sector had made the collective cybersecurity framework more adaptive, resilient, and effective in countering current and emerging threats.

**Hayk Mkrtchyan** reflected on the vital role of national law enforcement agencies in combating cybercrime, emphasizing their central position in addressing the global and borderless nature of this growing challenge. While cybercriminals exploited the interconnected digital world to carry out illicit activities, Mkrtchyan explained that national law enforcement agencies were often the first line of defense against these threats.

He highlighted the wide range of cybercriminal activities that law enforcement agencies were tasked with addressing, including financial fraud, identity theft, ransomware attacks, and the illicit trade of sensitive data. These crimes not only harmed individuals but also posed significant risks to businesses, critical infrastructure, and public trust in digital systems.

Mkrtchyan acknowledged the unique challenges faced by law enforcement in this domain, such as the anonymity provided to cybercriminals by digital platforms, the advanced technologies they used to conceal their activities, and the cross-border nature of many cyberattacks.
Despite these hurdles, he emphasized the indispensable role of law enforcement in gathering evidence, identifying perpetrators, and ensuring they were held accountable.

He underscored the importance of international collaboration in effectively combating cybercrime. He explained how national agencies often worked closely with global organizations, private sector partners, and law enforcement counterparts in other countries. Through joint task forces, intelligence sharing, and legal agreements, these agencies overcame jurisdictional barriers and created a more unified global effort to address cyber threats.

Mkrtchyan also noted how law enforcement agencies had evolved to keep pace with the dynamic nature of cybercrime. They had adopted cutting-edge technologies such as artificial intelligence for threat detection and blockchain for tracking illicit activities. Additionally, investments in specialized training had equipped investigators with the skills needed to navigate the complexities of this ever-changing field.

He highlighted Armenia’s commitment to international efforts, noting that the country had ratified the Convention on Cybercrime, also known as the Budapest Convention, which remains the world’s foremost tool for enabling effective collaboration in this area. He praised Armenia’s active participation in international meetings and discussions related to cybercrime, acknowledging the critical importance of global cooperation.

Mkrtchyan concluded by pointing out that most cybercrimes affecting Armenia were committed from abroad, making international collaboration indispensable for successful prevention and prosecution. He reiterated that while cybercrime knows no borders, national law enforcement, supported by global partnerships, remains at the heart of efforts to ensure digital security and resilience in the modern age.

**Markko Kunnapu,** Adviser in the Criminal Policy Department of the Ministry of Justice of Estonia, provided an in-depth analysis of the transnational nature of cybercrime, underscoring the critical importance of international cooperation in addressing this growing global issue.

Kunnapu explained that cybercrime transcends national borders, exploiting the interconnected digital world to operate across jurisdictions. This inherent characteristic, he noted, renders it impossible for any single country to combat cybercrime effectively on its own, necessitating robust and coordinated international collaboration.

He emphasized the need to harmonize legal frameworks across countries to facilitate the investigation and prosecution of cybercriminals. Discrepancies in national laws, he explained, often hinder these processes, creating safe havens in jurisdictions with weaker regulations. Treaties like the Budapest Convention on Cybercrime, Kunnapu pointed out, have been instrumental in addressing these challenges by providing a common legal framework and establishing protocols for evidence sharing, extradition, and mutual legal assistance among member states.

Kunnapu also highlighted the success of joint operations in combating cybercrime. He described how collaborative efforts between national law enforcement agencies, often facilitated by organizations like INTERPOL and Europol, have led to the dismantling of criminal networks, disruption of illicit activities, and recovery of stolen assets. These examples, he noted, illustrate the effectiveness of collective action in addressing complex cyber threats.

Another key area of focus in Kunnapu's remarks was capacity-building. He emphasized that many countries, particularly those with limited resources, face significant challenges in combating cybercrime due to gaps in technical expertise and infrastructure. International partnerships, training programs, and knowledge-sharing initiatives, he said, have been vital in helping these nations build their capabilities and actively contribute to the global fight against cyber threats.

In conclusion, Kunnapu stressed that international cooperation is not an optional strategy but a necessity for combating cybercrime effectively. By leveraging legal frameworks, treaties, joint operations, and capacity-building initiatives, nations have been able to create a unified front against cybercriminals. His remarks underscored the importance of fostering a collaborative spirit to ensure that cyberspace remains secure and resilient in the face of ever-evolving transnational threats.

**Shant Kassardjian,** Cybersecurity Advisor at the Information Systems Agency of Armenia, provided a thorough analysis of the essential role government agencies play in cybersecurity governance. He stressed that national governments bear the ultimate responsibility for establishing and maintaining the pillars of comprehensive cybersecurity. The decisions and actions of government agencies, Kassardjian noted, are pivotal in determining a country's ability to resist cyber threats and safeguard its digital infrastructure.

Kassardjian outlined the efforts of the Information Systems Agency of Armenia, emphasizing its role as a central actor in the country's cybersecurity strategy. He explained that the agency has been tasked with developing and implementing policies that align with national security priorities while adhering to international best practices. The agency's initiatives encompass frameworks to protect critical infrastructure, secure sensitive government data, and ensure reliable communication channels within and between public sector institutions.

He elaborated on the agency's approach to comprehensive cybersecurity governance, which includes strengthening legislative frameworks, establishing technical standards, and enhancing institutional capabilities to detect, prevent, and respond to cyber incidents. Kassardjian underlined the importance of collaboration between government bodies and other stakeholders—such as private companies, academia, and civil society—to create a cohesive and effective cybersecurity ecosystem.

Addressing the challenges faced by government agencies, Kassardjian noted the rapidly changing nature of cyber threats, the increasing sophistication of cybercriminals, and the growing interdependence of critical infrastructure systems. To tackle these issues, the agency has focused on advancing technical capabilities, enhancing workforce skills, and fostering partnerships with international organizations.

Kassardjian highlighted key initiatives led by the Information Systems Agency, such as the development of a centralized cybersecurity framework for Armenia’s public sector and the creation of mechanisms to monitor and address cyber threats in real-time. He also pointed to the agency’s efforts to raise public awareness of cybersecurity risks and promote digital literacy among citizens, recognizing that human factors are integral to a nation’s cyber resilience.

In conclusion, Kassardjian reaffirmed the agency's commitment to strengthening Armenia’s cybersecurity posture through strategic planning, capacity-building, and collaboration. He emphasized that government agencies are not only protectors of national cybersecurity but also enablers of a secure and innovative digital future, fostering trust and resilience in the face of evolving cyber challenges.

# *WSIS+20 updates in the frames of events on 2024, Future of the IGF, Global Digital Compact and analysis of the Summit of the future*

- ❑ **Aleksey Sandikov -** IGC member, Parliament member of the RA
- ❑ **Chris Buckridge -** Senior Strategy Advisor Global Forum on Cyber Expertise (GFCE) (online)
- ❑ **Veni Markovski -** ICANN, Vice-President for UN engagement (online)
- ❑ **Amrita Choudhury -** Chair IGFSA, Chair APRALO (online)
- ❑ **Moderator: Mikhail Anisimov** – ICANN, Head of Global Stakeholder Engagement for Eastern Europe and Central Asia

***The session on WSIS+20 Updates focused on the latest developments leading up to the 2025 review of the World Summit on the Information Society. It examined the evolving role of the Internet Governance Forum (IGF), the importance of the Global Digital Compact in shaping global digital cooperation, and the key outcomes of the Summit of the Future. The discussion highlighted how these milestones were expected to influence Internet governance and digital policy strategies for 2024 and beyond.***

**Mikhail Anisimov** opened the session by acknowledging the ongoing global discussions surrounding the Internet Governance Forum (IGF) and its pivotal role in shaping the future of the digital ecosystem. He underscored the importance of these conversations in addressing the rapidly evolving digital landscape and the need to adapt to new challenges and opportunities. Anisimov emphasized that the session aimed to provide a platform for examining these global processes through the perspectives of diverse stakeholders, including representatives from international organizations, government sectors, civil society, and the private sector.

The session focused on exploring critical global developments, including the upcoming WSIS+20 review, the emerging Digital Global Compact, and the broader issues within Internet governance. Anisimov noted that these topics were not only essential for understanding the global framework but also for assessing their impact on regional and local levels. By bridging the gap between global initiatives and regional realities, the session sought to ensure that the voices of all stakeholders, particularly Internet users, were included in shaping policies and governance frameworks.

Anisimov highlighted the unique opportunity this dialogue provided to connect global ambitions with local implementation, fostering a shared understanding of the challenges and opportunities in building a digital future. He stressed that inclusivity, sustainability, and collaboration were fundamental principles that should guide these efforts. The session was intended to address how global frameworks like the WSIS+20 and the Digital Global Compact could be translated into actionable outcomes that benefit societies while addressing regional nuances and priorities.

He further emphasized the importance of fostering an open and transparent dialogue, where stakeholders could discuss the complexities of Internet governance, including issues of human rights, access, and the responsible use of emerging technologies like artificial intelligence. The session aimed to create a space for meaningful exchange, allowing participants to share insights, propose solutions, and identify areas for collaboration.

With these remarks, Anisimov set the tone for a productive and engaging discussion. He concluded his opening by introducing the first speaker, encouraging them to share their perspective and contribute to the collective effort of shaping an inclusive and resilient digital future.

**Chris Buckridge** highlighted the significance of the upcoming WSIS+20 review, marking two decades since the original World Summit on the Information Society (WSIS) shaped the foundation for Internet governance and digital cooperation.

Reflecting on the summits held in 2003 and 2005, he underscored their groundbreaking nature, as they convened stakeholders for the first time to address the governance of digital technologies and the potential of information and communication technologies (ICTs) for development.

Buckridge explained that the Geneva Plan of Action from 2003 provided a blueprint of actionable goals to achieve a people-centered, inclusive, and development-oriented information society. Two years later, the Tunis Agenda laid the groundwork for a distributed multistakeholder model of Internet governance, establishing the Internet Governance Forum (IGF) as a cornerstone of policy dialogue and setting a vision for enhanced cooperation among stakeholders.

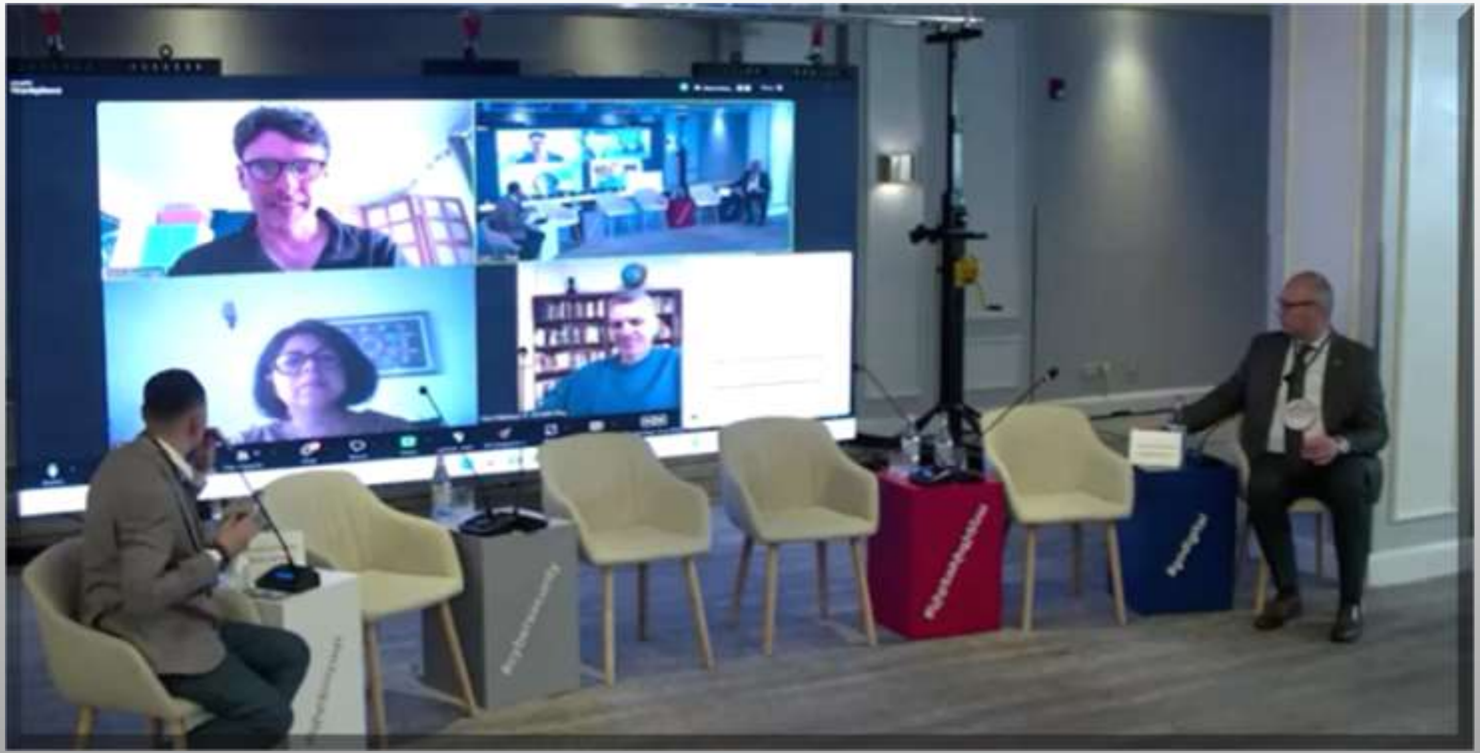
As the WSIS+20 review approaches, Buckridge framed it as a pivotal opportunity to evaluate whether the outcomes and frameworks established by WSIS remain fit for purpose in the face of today's digital challenges. He pointed to the rapid evolution of technologies, emerging global threats, and shifting geopolitical dynamics that demand an updated approach. Issues like the governance of artificial intelligence, digital public goods, and infrastructure inequalities are likely to dominate discussions, alongside critical questions about human rights, inclusivity, and the role of multistakeholderism.

Buckridge emphasized the stakes of the review, noting it would be a forum for competing visions of the Internet's future. There may be calls to revise WSIS Action Lines, such as those addressing ICT infrastructure, confidence and security, or ICT applications, to reflect new realities and priorities. At the same time, the review will need to balance these updates with the principles of technological neutrality and openness that underpin WSIS.

He expressed hope that WSIS+20 could strengthen the alignment between Internet governance frameworks and international human rights standards. He advocated for a more robust application of WSIS's multistakeholder ethos through platforms like the IGF, ensuring these processes remain open, inclusive, transparent, and accountable.

In conclusion, Buckridge underscored the importance of leveraging WSIS+20 to refine and advance the framework that has guided digital cooperation over the past two decades, ensuring it meets the needs of an increasingly complex and interconnected world. He called on all stakeholders to engage actively, as the outcomes of this review will shape the future of digital governance for years to come.

**Veni Markovski,** responsible for governmental engagement at ICANN, delivered a critical assessment of the current dynamics surrounding Internet governance processes within the United Nations framework.



He underscored the limited participation of stakeholders beyond member states in these discussions, emphasizing the constraints this imposes on achieving a truly inclusive governance model.

Markovski pointed out that negotiations at the UN are exclusively conducted between member states, leaving other stakeholders—such as civil society, the private sector, and technical communities—with minimal opportunities to influence outcomes.

Their involvement is often relegated to side meetings or limited to observing the process through updates, such as those shared in ICANN’s blog covering discussions from UN meetings.

He expressed concern that major upcoming processes, including the Digital Global Compact, the WSIS+10 review, and the anticipated WSIS+20 review, might further entrench these limitations. The WSIS+20 review, in particular, will play a pivotal role in shaping the future of Internet governance. Markovski noted that this process could potentially alter the existing governance model, making it even more critical for all stakeholders to advocate for inclusive approaches.

Highlighting the fundamental issue of representation, he reminded the audience that each country has one vote at the UN, regardless of its size, digital infrastructure, or level of engagement in global Internet governance. This structure, while ensuring equal representation among member states, often overlooks the nuanced and essential contributions of other stakeholders.

Markovski commended the Armenian Internet Governance Forum (ArmIGF) for bringing attention to these critical issues and fostering discussions on the importance of preserving and strengthening the multistakeholder model of Internet governance. He expressed hope that diplomats and decision-makers would recognize the value of this model, which has been instrumental in the Internet's growth, stability, and inclusivity.

In his closing remarks, Markovski urged all participants to remain engaged and proactive, emphasizing that the future of Internet governance depends on a balanced, collaborative approach that includes voices from all sectors. Only by safeguarding the multistakeholder model can the global Internet community ensure that governance frameworks reflect the diversity and complexity of the digital age.

**Amrita Choudhury** emphasized the critical role of civil society as a stakeholder group in Internet governance. She acknowledged that, as some of her colleagues had pointed out, the existing processes are not as open and inclusive as they need to be, limiting the ability of diverse voices to shape the digital future effectively.

Choudhury reflected on the Global Digital Compact (GDC), noting that while the draft document is not without merit, the broader processes surrounding it, as well as other upcoming initiatives, must adapt to the rapidly changing digital landscape.

Developing countries, in particular, are grappling with these shifts, and it is essential to recognize how the Internet affects individuals in profoundly different ways depending on their circumstances and environments.

She highlighted that regulatory frameworks introduced in various countries often perform better when they consider the perspectives of civil society and other stakeholders. Such regulations tend to be stronger, more balanced, and more effective. However, when decisions are made unilaterally or without sufficient consultation, the outcomes are frequently suboptimal and fail to address the complexities of the digital ecosystem.

Looking ahead to the upcoming GDC, Choudhury expressed hope that it would embody greater inclusivity and address critical issues such as human rights, equitable access, and digital inequalities. She stressed that transparency must be at the heart of these processes, ensuring that all voices, especially those from underrepresented communities, are heard and accounted for.

One of her key concerns was the difficulty many stakeholders from developing countries face in participating in key global discussions, such as those held in New York. The financial burden of attending such meetings often excludes civil society representatives and smaller organizations, creating an imbalance in representation. Choudhury underscored the importance of finding mechanisms to involve all communities effectively, regardless of their economic constraints, and called for solutions to enhance accessibility and participation.

In her closing remarks, Choudhury reaffirmed the need for inclusivity, transparency, and multistakeholder engagement in global Internet governance processes. Only by prioritizing these principles can the GDC and similar initiatives create a framework that reflects the diverse needs and aspirations of the global Internet community.

**Aleksey Sandikov,** IGC member and Parliament member of the Republic of Armenia, addressed the audience at ArmIGF 2024, emphasizing the significance of global processes in shaping Internet and digital governance. He highlighted the importance of the parliamentary track, which has been an integral part of the global Internet Governance Forum (IGF) for the past four years. This track, designed specifically for representatives of national assemblies, provides a platform for legislative engagement in Internet governance, and Sandikov noted Armenia's active participation in these global discussions.

Sandikov commended the Armenian IGF for its strong commitment to the multi-stakeholder model, which brings together representatives from government, civil society, academia, the private sector, and the technical community. He described this model as the most inclusive and effective approach to addressing the challenges and opportunities of the digital age. He expressed pride in Armenia's IGF, describing it as a shining example of how a multi-stakeholder framework can foster meaningful dialogue, collaboration, and innovation.

He also highlighted the parliamentary track as a successful initiative within the global IGF, noting its value in involving lawmakers in digital policy discussions. This track provides parliamentarians with opportunities to engage with experts and stakeholders, gain a deeper understanding of Internet governance issues, and contribute to the creation of balanced and inclusive policies.

Sandikov underscored Armenia’s commitment to the principles of openness, inclusivity, and collaboration in digital governance. He emphasized that addressing the challenges of the digital age requires a shared effort involving the perspectives and contributions of all stakeholders to ensure a secure, open, and equitable Internet.

In closing, Sandikov expressed his gratitude to the organizers of ArmIGF 2024 and the participants for their dedication to fostering collaboration and innovation in Internet governance. He reiterated the importance of upholding the multi-stakeholder model to address current challenges while creating opportunities for a more inclusive and prosperous digital future.

# *National Content and ccTLDs: Strategies for Growth and Overcoming Challenges*

- ❑ **Kristina Hakobyan -** Vice Chair of the board “Internet Society” NGO, .am/.հայ registry
- ❑ **Irina Danelia -** Coordination Center for .RU ccTLD/.РФ deputy director
- ❑ **Sophie Khidasheli -** Senior Specialist of .GE ccTLD Registry (online)
- ❑ **Dejan Dukic -** CEO RNIDS.RS (online)
- ❑ **Azizbek Kadirov -** .uz ccTLD administration, UZINFOCOM (online)
- ❑ **Moderator: Maria Kolesnikova -** Coordination Center for TLD RU, Chief Analyst

Panelists shared experiences from various national registries, addressing challenges such as competition with generic TLDs, security threats, and building user trust.

The discussion highlighted aligning ccTLD strategies with national priorities, including promoting local businesses, cultural identity, and digital security. Successful case studies on marketing, stakeholder partnerships, and security measures like DNSSEC were presented to inspire actionable solutions for strengthening national digital ecosystems.

**Maria Kolesnikova**, spoke about the critical role of domain names in the global digital landscape, emphasizing their importance for countries in establishing a strong and secure online presence. She highlighted how the development of resources for country-code top-level domains (ccTLDs) contributes significantly to building trust and ensuring security on the Internet at the national level.

Kolesnikova noted that this year marks a significant milestone for several ccTLD registries as they celebrate 30 years of their domain name operations. She described this anniversary as not just a reflection of past achievements but also as a stepping stone toward the next 30 years, envisioning even more developed and modern domain zones that align with the evolving needs of the digital era.

She underscored the importance of investing in and modernizing ccTLDs to ensure they continue to play a pivotal role in fostering trust, supporting local content, and strengthening national digital ecosystems.
With this she gave the flor to the registries’ representatives from different countries.

**Kristina Hakobyan** spoke about the issues and challenges surrounding the .am ccTLD, reflecting on its 30-year history. She noted that while three decades might seem lengthy, the development of policies and processes for .am has been a gradual and complex journey, shaped by the needs of the society it serves.

Hakobyan emphasized that the growth and management of a ccTLD depend on understanding the specific characteristics of the local community and applying global best practices in a way that aligns with those needs. She highlighted the ongoing efforts in policy-making, which involve creating and updating frameworks to ensure security, reliability, and inclusivity for all users.

She also spoke about initiatives aimed at engaging stakeholders through workshops and outreach activities designed to raise awareness and build a collaborative environment. Despite the relatively slow growth in .am ccTLD registrations, Hakobyan stressed the importance of continuous awareness campaigns to educate the public about the benefits of using local ccTLDs and Internationalized Domain Names (IDNs).

Hakobyan pointed out that developing local content and building trust in the national Internet space requires a collective effort.

She urged individuals and organizations to recognize the value of .am domains in fostering a robust national digital identity and contributing to the broader Internet ecosystem.
Her remarks underscored the importance of community involvement and proactive engagement in ensuring that the .am ccTLD continues to support Armenia’s cultural, economic, and technological development in the digital age.

## *Key Points*

- ❑ **The Complexity of .am ccTLD Development**
- ❑ **The Importance of Stakeholder Engagement and Awareness**
- ❑ **Promoting Local Content through .am Domains**

**Irina Danelia's** presentation focused on the strategies for growth and overcoming challenges related to national content and ccTLDs, specifically the .RU and .РФ domains. Managed by the LLC Technical Center of Internet, the registry prioritizes technical stability, security, and inclusivity for users and registrants.

The infrastructure ensures uninterrupted operations of the .RU and .РФ domains, supported by regular monitoring of critical functions such as EPP, DNS, and WHOIS. Operational stability has been a focus since 2019 when the Ministry of Telecommunications introduced additional measures. Security is addressed through comprehensive initiatives like Domain Patrol and Netoscope Services, which detect and mitigate DNS abuse. Security checks are also provided for users and government agencies to ensure a safe experience for all.

Educational efforts are a significant component, with public materials, events like "Safe Internet" lessons in schools, and the "Study the Internet – Govern It!" project, which includes specialized modules for blind users. Inclusivity is further emphasized through website features for visually impaired users and engagement activities such as the Dot-Journalism Award, promoting participation and innovation in the digital space.

The presentation highlighted the importance of the Russian language's presence on the Internet, supported by global statistics on content languages and Internet users. These efforts underline the relevance of promoting national content while addressing global challenges.

In conclusion, the presentation emphasized enhancing domain stability, ensuring security, fostering inclusivity, and promoting national content as key strategies for creating a safer, more accessible, and enriched digital ecosystem for .RU and .РФ users.

## *Key Highlights*

- ❑ **Technical Stability**
- ❑ **Inclusivity Efforts**
- ❑ **Security Measures**
- ❑ **Educational Initiatives**

**Sophie Khidasheli's** presentation provided insights into the management and growth strategies of the .GE ccTLD registry, operated by Caucasus Online under the NIC.GE Administration Unit. The registry manages over 61,000 domains with the support of 21 registrars. In 2018, it transitioned to a Registry-Registrar model, with Caucasus Online focusing solely on registry operations.

A key innovation introduced by the registry is the Search Engine for Alternative Domain Name Suggestions. This tool helps users find suitable domain alternatives by offering suggestions in Georgian and English transliterated names, as well as hyphenated words, abbreviations, and domain zones.
The system is powered by Artificial Intelligence (AI) and Natural Language Processing (NLP), enabling the digitization of Georgian language forms for enhanced functionality.

Looking ahead, the registry has outlined several initiatives to support the growth of the .GE ccTLD.

These include implementing DNSSEC to bolster domain security, engaging young innovators through support for tech startup projects, and increasing awareness of the .GE ccTLD through targeted campaigns. Additionally, the development of new SLDs tailored to specific areas is planned to enhance domain customization and adoption.

In conclusion, Khidasheli emphasized the registry's commitment to innovation, security, and community engagement, highlighting these efforts as essential for ensuring the sustained growth and modernization of the .GE domain space.

***Key Initiatives***

- ❑ **Search Engine for Alternative Domain Name Suggestions**

- ❑ **Future Projects for .GE ccTLD Growth**

**Dejan Đukić's** presentation highlighted the achievements and strategies for growth in the .rs and .срб domain zones, emphasizing steady progress, innovative business practices, active community involvement, and robust risk mitigation measures.

The .rs and .срб zones experienced significant growth in 2023, with the .rs domain growing by 5.61% year-over-year and the .срб domain by an impressive 57%. DNS availability was maintained at 100%, reflecting a commitment to operational stability and reliability.

These achievements were underpinned by fostering team collaboration and partnerships.

Business processes were invigorated with the introduction of a new registrar incentives program in early 2024 and the launch of a new registrars portal in late 2023. A more proactive market approach was adopted through continuous incentive campaigns to drive engagement and growth.

arm igf 9

Community engagement played a pivotal role, with RNIDS hosting UA Day 2024 in Belgrade, a cornerstone event. The organization also collaborated with National CERT and the Ministry for a National Cyber Security Conference in October 2024. Other supported events included IGF Serbia 2024, the 12th edition of DIDS, the 10th RSNOG Conference, the Cyber Hero project, and the ECSC 2024 competition.

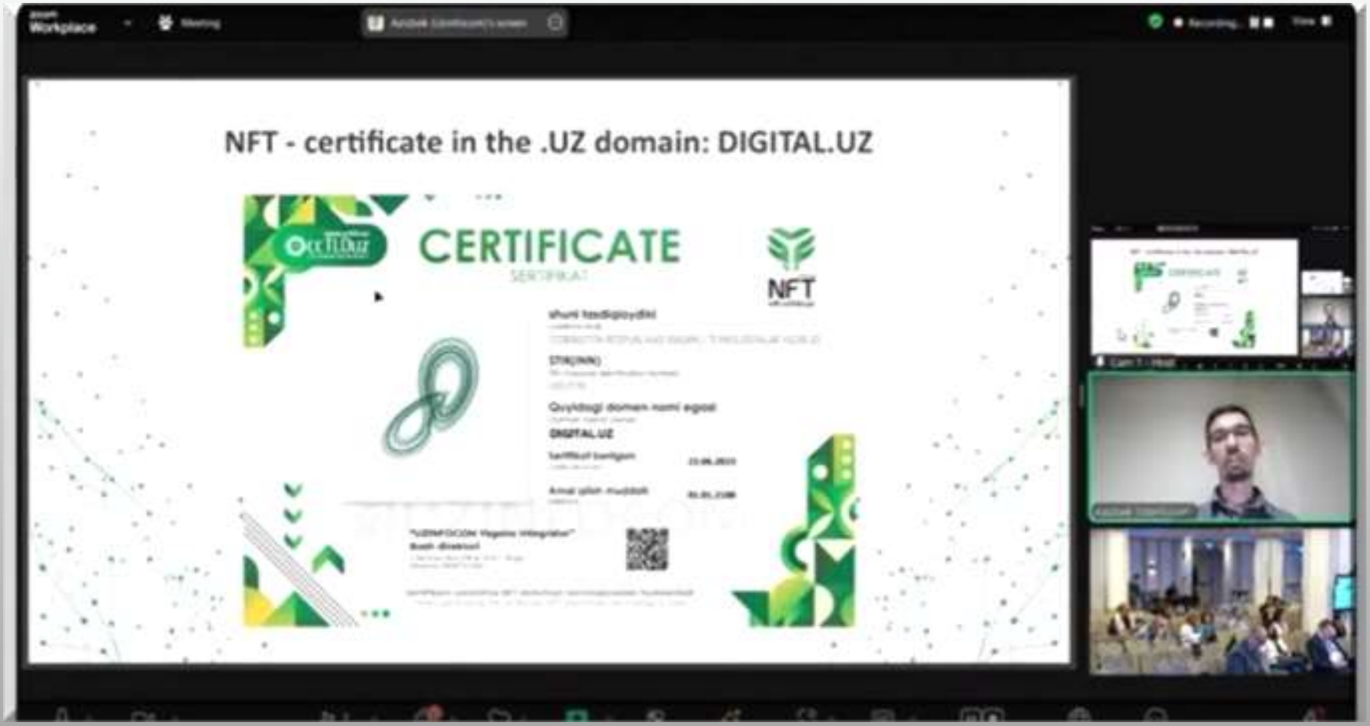
In terms of risk mitigation, system defenses were strengthened through new infrastructure, and RNIDS CERT’s incident response capacity was enhanced. Collaboration with security peers and local authorities was bolstered through training, meetings, and conferences.

The presentation concluded by underscoring the importance of steady growth, business innovation, community participation, and robust security measures in addressing challenges in the domain name system and Internet governance.

## *Key Themes and Highlights*

- ❑ **Steady Growth in the .rs and .срб Zones**
- ❑ **Vigorizing Business Processes**
- ❑ **Community Engagement Activities**
- ❑ **Threats and Risk Mitigation**

**Azizbek Kadirov** stated that blockchain technology has been integrated into the .UZ domain name registry to manage NFT certificates, introducing a transparent and immutable history of domain ownership. Certificates are issued as NFTs and include essential information such as token IDs, domain names, issuance and expiration dates, and hashed owner email addresses. These NFT certificates can be easily accessed and managed through the ccTLD .uz mobile application, ensuring convenience for users.



NFT - certificate in the .UZ domain: DIGITAL.UZ

CERTIFICATE

SERTIFIKAT

NFT

shuni tasdiqlaydiki

STIR(INN)

Quyidagi domen nomi egasi

DIGITAL.UZ

The system leverages blockchain for transparency and security by protecting data from modification, enabling transparent transactions through smart contracts, and maintaining immutable ownership records. National symmetric encryption (O'zDSt 1105:2009) is used to secure private keys, further enhancing security. Additionally, an open-source block explorer allows users to verify blockchain transactions, making the system both accessible and trustworthy.

The integration of blockchain technology has contributed to significant growth in domain registrations within the .UZ zone, creating new opportunities for monetization and simplifying processes for both registrars and users. Decentralization has ensured data integrity and preservation, positioning blockchain as a transformative solution for domain management.

While the approach offers numerous benefits, the presentation emphasized the importance of experimenting with blockchain in domain registries while being mindful of regulatory and legal considerations across different jurisdictions.

In conclusion, the adoption of blockchain and NFT technology in domain name management enhances transparency, security, and innovation, providing a robust framework for managing domain ownership and transactions. This forward-thinking approach has the potential to revolutionize how domain registries operate globally.

## *Key Features of the System*

- ❑ **Transparency and Security**
- ❑ **NFT Certificates for Domains**
- ❑ **Encryption Standards**
- ❑ **Blockchain Integration Benefits**

# *ArmIGF 2024 in numbers*

***Participants***

- ❑ In person - 137
- ❑ Online - 15
- ❑ Volunteers - 7

- ❑ Panel discussions - 5
- ❑ Presentations - 4

***Stakeholder Group***

- ❑ Government - 10%
- ❑ Intergovernmental Organization - 5%
- ❑ Civil Society (Includes academia) - 33%
- ❑ Technical Community - 22%
- ❑ Private Sector - 18%
- ❑ Press/Media - 12%

arm igf 9

# *Media coverage – hashtag #armigf2024*

The event was broadcast live on Zoom and YouTube, with coverage provided by journalists from traditional media outlets as well as social media platforms.

[https://rb.gy/1w76hu](https://rb.gy/1w76hu)
[https://shorturl.at/kJjaX](https://shorturl.at/kJjaX)
[https://shorturl.at/YEH0H](https://shorturl.at/YEH0H)

[https://shorturl.at/TU8Ho](https://shorturl.at/TU8Ho)
[https://shorturl.at/RLZRs](https://shorturl.at/RLZRs)
[https://armenpress.am/hy/article/1204126](https://armenpress.am/hy/article/1204126)
[https://hy.armradio.am/archives/610423](https://hy.armradio.am/archives/610423)

[https://shorturl.at/rmNLv](https://shorturl.at/rmNLv)
[https://rb.gy/vrdvu6](https://rb.gy/vrdvu6)
[https://rb.gy/2bwdxp](https://rb.gy/2bwdxp)
[https://rb.gy/ndeqc1](https://rb.gy/ndeqc1)
[https://rb.gy/uv6qtm](https://rb.gy/uv6qtm)

arm igf 9

# *Thank you!*

We extend our heartfelt gratitude to the regional, local, and international sponsors of the 9th Armenian Internet Governance Forum for their invaluable support and assistance in organizing the event. Their contributions made it possible to bring participants together both in person and virtually, facilitate meaningful engagement, and ensure public media coverage of the forum.

We also wish to thank all the participants, volunteers, moderators, rapporteurs, interpreters, journalists, photographers, designers, printing service providers, and other contributors whose efforts played a vital role in making ArmIGF 2024 a resounding success

arm igf 9