19th Parliamentary Intelligence-Security Forum

Budapest, Hungary

September 6th, 2021

20 F St. NW – Suite 700
Washington, D.C. 20001
United States Of America

Mobile/WhatsApp/Signal/WeChat:
704 307 3500
Skype: live:RobertPittenger
Robert@PI-SF.con
www.PI-SF.com

CONGRESSMAN ROBERT PITTENGER
Chairman
Parliamentary Intelligence-Security Forum

Dear Parliamentarians and Distinguished Leaders:

Please note the report below from the Parliamentary Intelligence-Security Forum in Budapest, 6 September. Over 200 Parliamentarians from 54 countries heard presentations from leading experts from industry, governments and think tanks regarding critical security/technology topics including Cyber Security, 5G, AI, Blockchain/Cryptocurrencies, Central Bank Digital Currencies, Foreign Investments, Illicit Finance, Human Trafficking and other issues.

We hope this information provides helpful guidance on policy and legislative initiatives. We look forward to being with you at a future forum.

We offer special gratitude to Deputy Speaker Csaba Hende and Ms. Trixi Kese with the Hungarian National Assembly for their exceptional leadership in preparation and organization of the forum.

Sincerely,

Robert

Robert Pittenger
Chairman, Parliamentary Intelligence-Security Forum
704-307-3500

AZ ORSZÁGGYŰLÉS ELNÖKE

Dear Parliamentarian/Distinguished Leader,

Permit me on behalf of the Hungarian National Assembly to invite you to attend the Parliamentary Intelligence–Security Forum on September 6, 2021, in Budapest at the Hungarian National Assembly, what was postponed from May 2020 due to the COVID-19 pandemic.

Having regard to the significance of the issues on the agenda of the Parliamentary Intelligence-Security Forum, as well as the commitment of the Hungarian legislature and the Government to combatting human trafficking, money laundering, cybercrimes and terrorism, the Hungarian National Assembly is pleased to host this strategic and high level Conference.

By organizing this Forum with participation from experts throughout the world, we would like to raise awareness among Parliamentarians about the complex issues on the agenda of the conference, which threaten our security and the achievements of the international community in this field.

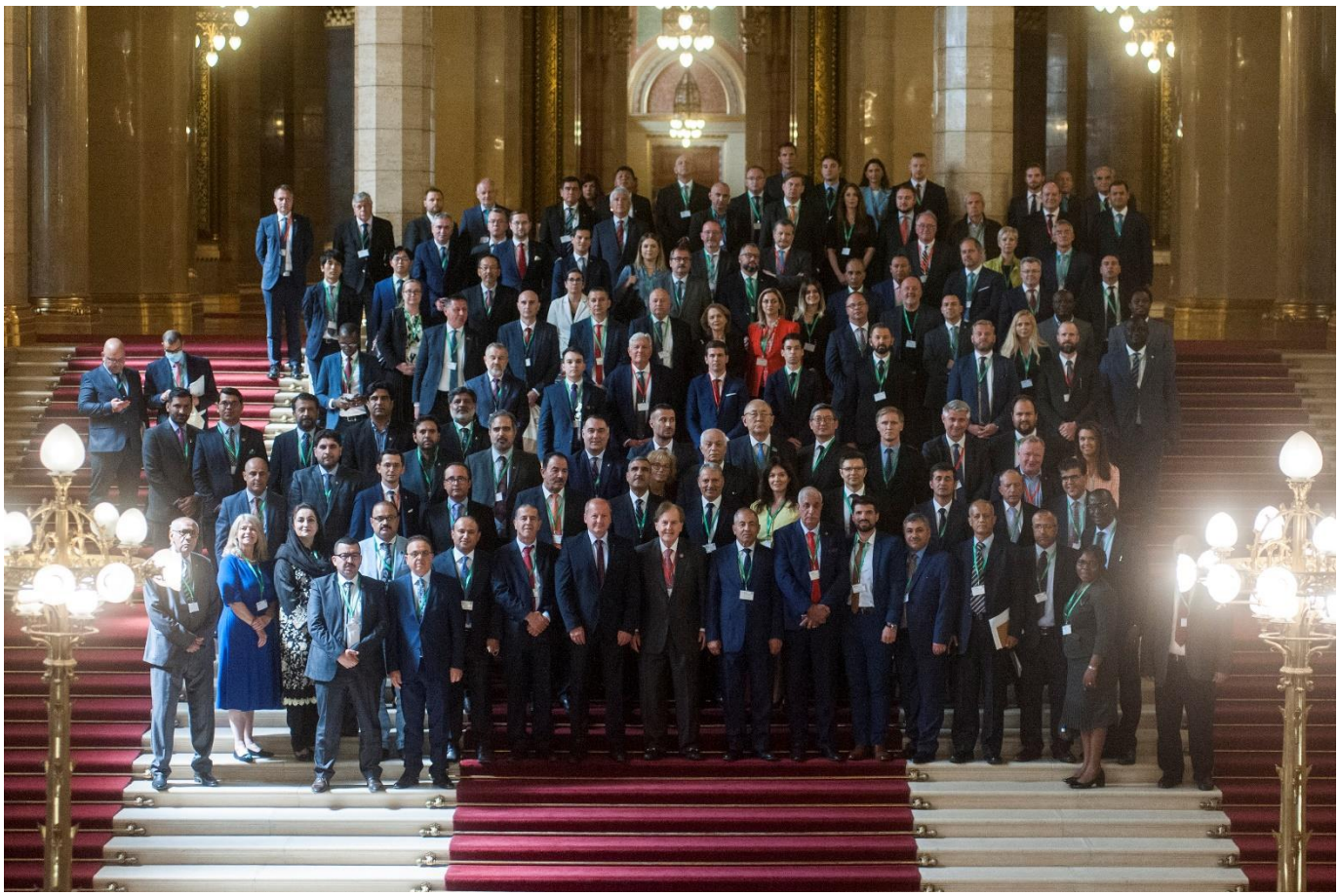
Your participation and contribution would be highly valued at this Conference, which will provide an opportunity for exchange among Parliamentarians on legislative initiatives, critical financial technology and other best practices. I send for your kind attention attached the draft programme of the Conference.

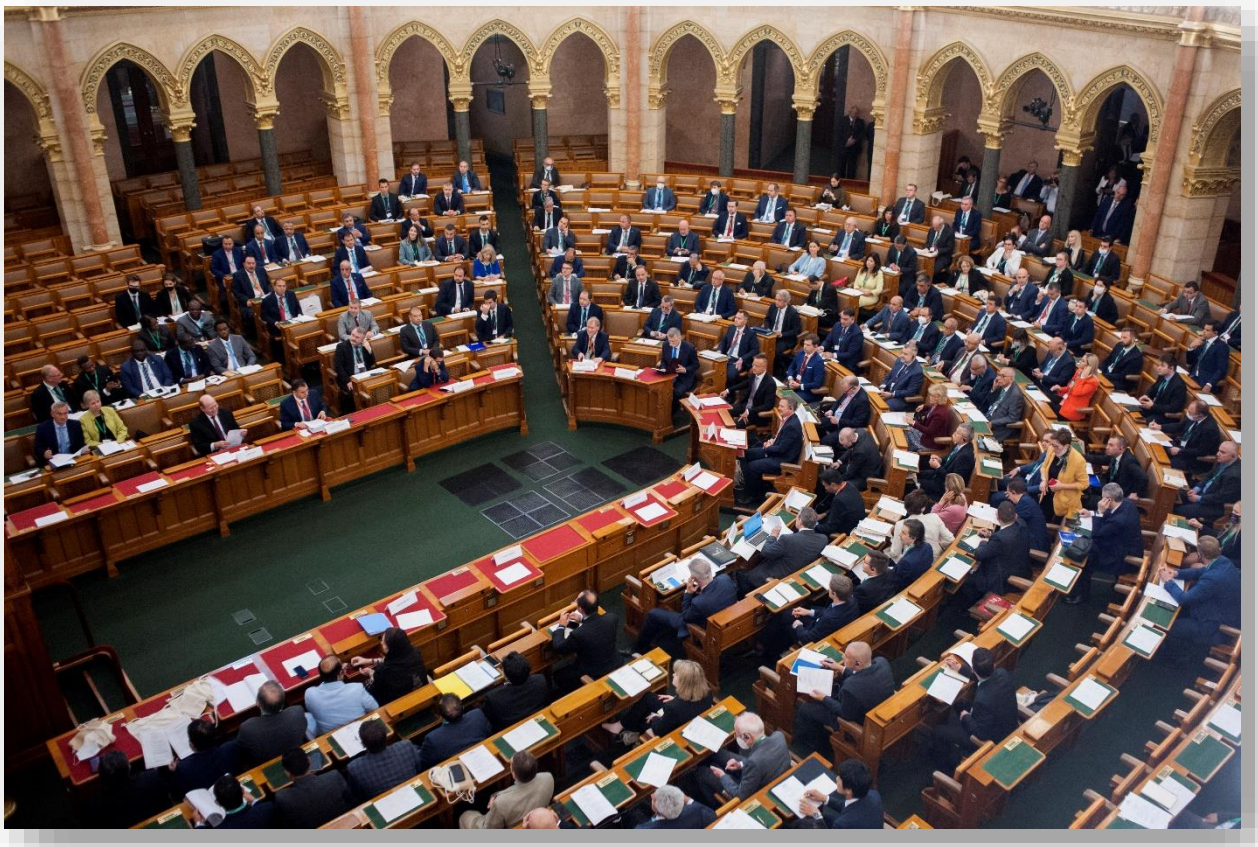
I am very much looking forward to welcoming you in Budapest in September. I strongly hope that it will be possible to have an in person meeting in our Parliament, but for those who cannot travel to Hungary, there will be a livestream of the Conference available. Please confirm your participation to the following e-mail address: lucas@pi-sf.com and PISF@parlament.hu. For questions please refer to Ms. Beatrix Kese, Tel: +36 1 441-4398, E-mail: kese.beatrix@parlament.hu.

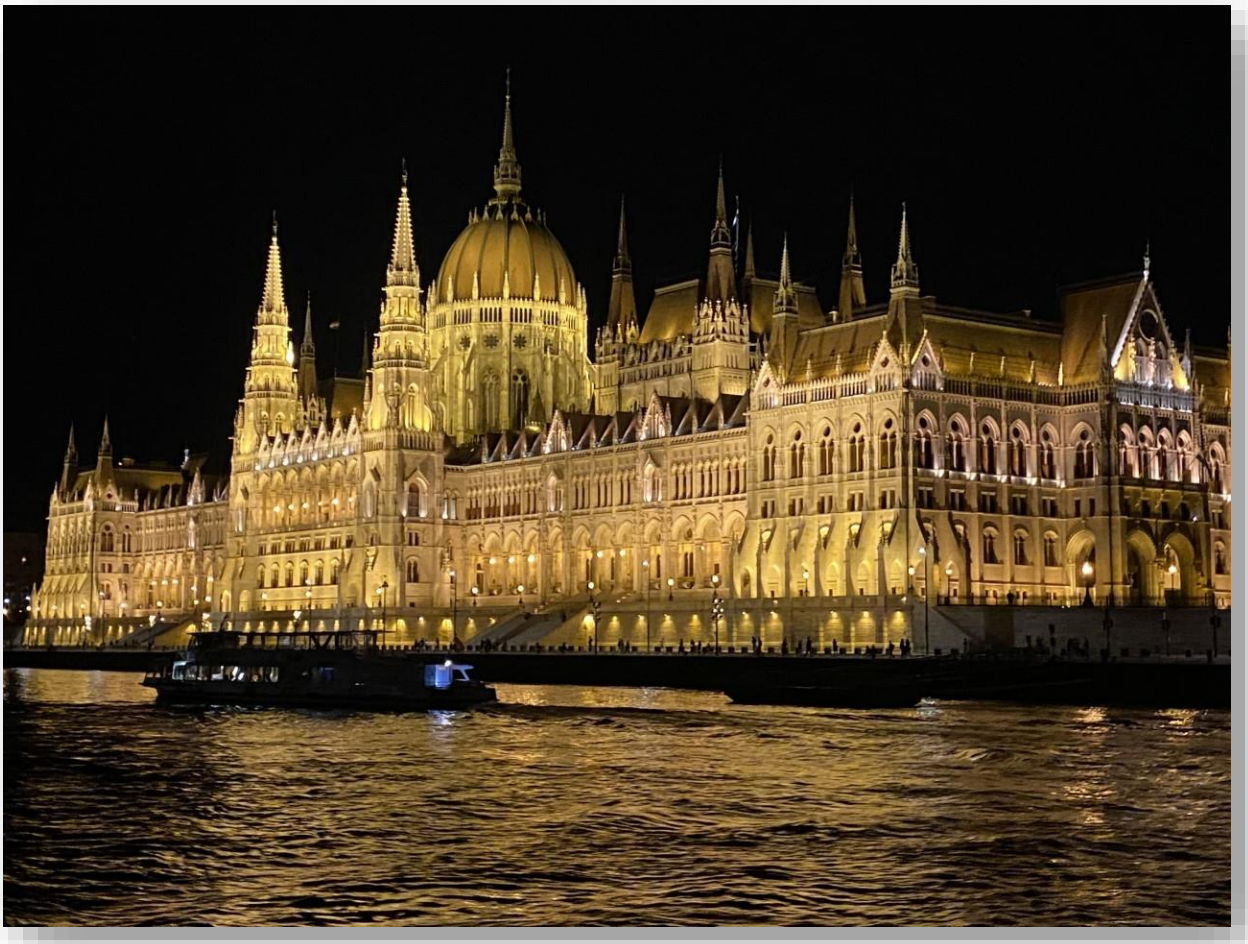
Yours sincerely,

KÖVÉR László

Family photo with all people at the Forum.





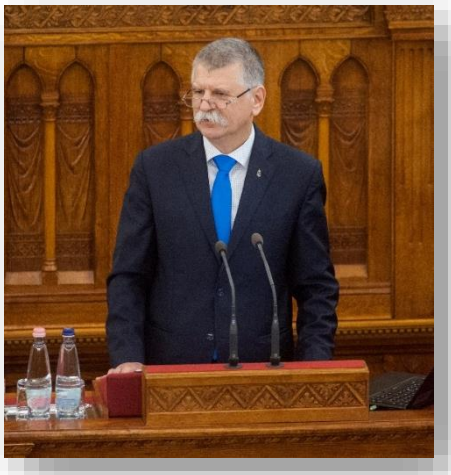


Summary of Presentations

Opening of the Conference

- **Hon. László Kövér,** Speaker of the Hungarian National Assembly (Hungary)

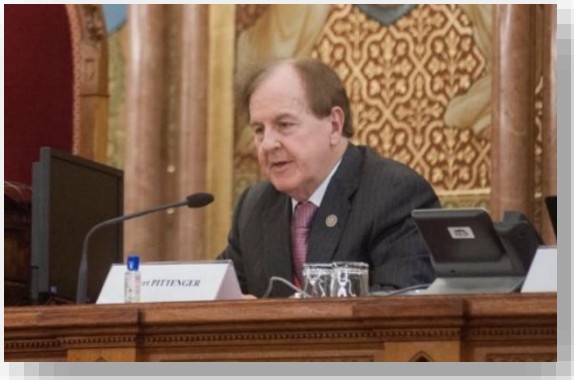
László Kövér, Speaker of the Hungarian National Assembly called the information superiority of democratic states and thus their advantage in action against non-democratic states, organised private powers and terrorist and criminal groups vital. Security has now become a primary competitive factor in all aspects of life, and therefore opponents seeking to undermine one's competitiveness will also seek to undermine that actor's security. As the events in Kabul today show, it can be a matter of life and death whether intelligence is providing wrong or even false information to decision-makers, and whether politicians are using intelligence information as intended, or for manipulation or are deliberately ignoring it. Military, financial and technological superiority alone is not sufficient if it is not combined with information superiority that can be used in policy-making, or if policy-makers do not make appropriate use of the information they obtain. The Speaker stressed that the exciting questions of the future are whether states and their intelligence and security services will remain competitive in the world's information wars, and whether people and societies will be the winners or the victims of technological progress. He expressed his conviction that international politics in the coming decades will be defined by the competition and clashes between states as public powers and private powers organised above them. He added that he was confident that the rivalry would eventually lead to cooperation. As a consequence, not only politicians but also the intelligence or security community will have to decide whether they want to serve public or private interests/powers. As it is not legitimate that those working in the political or intelligence-security services of public power should serve the interests of private powers, just as those working for private powers are not expected by their clients to serve the interests of public powers and the common good.



- **Congressman Robert Pittenger,** Chairman, Parliamentary Intelligence-Security Forum (United States)

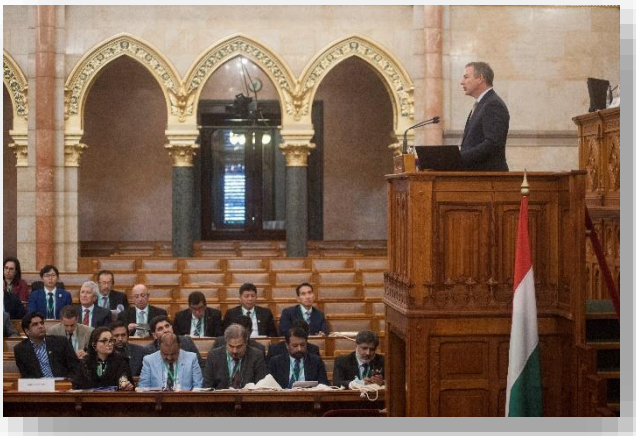
Congressman Pittenger began by giving thanks to Hungarian representatives for their gracious offer to host what he believes is a very important meeting. He showed his gratefulness to all attendees by saying that their leadership is honored and respected by the United States of America.

"We are only as strong as our weakest link" is what Congressman Pittenger stated while wishing everyone a tremendous day.



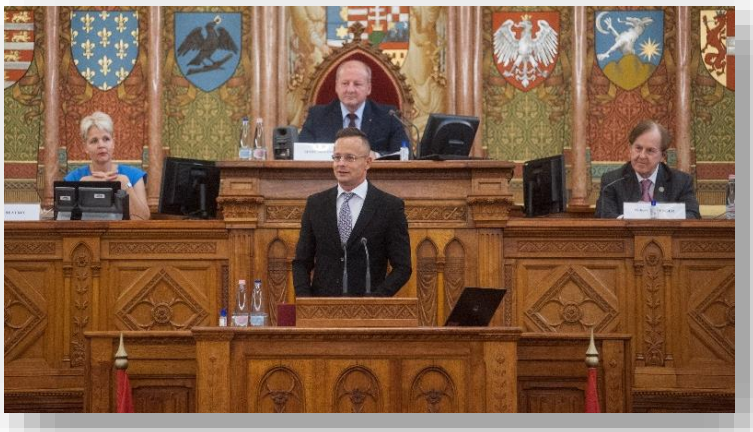
❖ **Hon. Marc Dillard,** Chargé d'Affaires, a.i., U.S. Embassy in Budapest (Hungary)

The Honorable Marc Dillard began his speech addressing the concern of technology risks and expressed his satisfaction that this was going to be a strong subject in the forum. His remarks stated that we need to understand the risks, as well as the benefits, of new technology, more specifically 5G. He went on to say that the Chinese are big owners of this technology, posing a security threat for those countries that buy that technology from the Chinese.



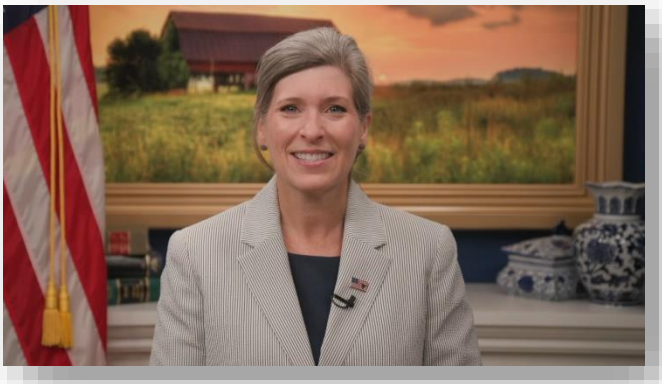
Introductory speech by:

❖ **Hon. Péter Szijjártó,** Minister for Foreign Affairs and Trade (Hungary)



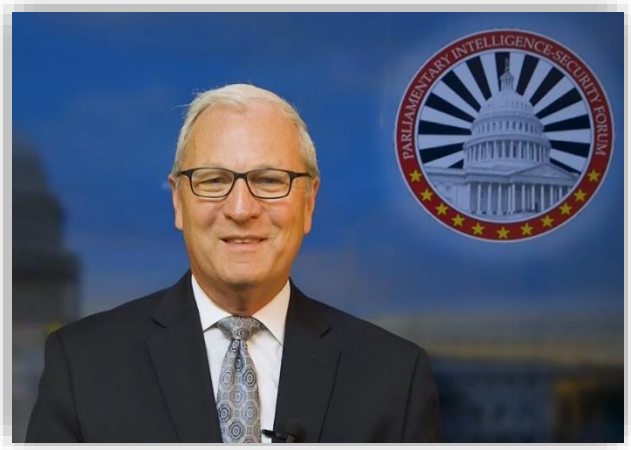
Péter Szijjártó, Hungarian Minister for Foreign Affairs and Trade stressed that data has become a primary resource, about as significant as the invention of the steam engine in the 18th century or hydrocarbons in the 20th century. As an example, he highlighted that in 2010, there were around 820 million mobile broadband subscriptions globally, which has now reached 5.2 billion, a six-fold increase in less than ten years. He also noted that in 2010, 2 zettabytes of data were generated, compared to 64.2 zettabytes this year. He stressed that cyber-attacks have increased in frequency and volume, and cybercriminals pose a serious threat not only to private users but also to businesses and public organisations, potentially crippling healthcare systems, as demonstrated by the cyber-attack that paralysed 400 hospitals in the US. Home office and distance learning, which were imposed during the coronavirus epidemic, have exacerbated the problem, with many inexperienced users accessing the web, which terrorist and extremist groups are also trying to exploit to spread their ideology. He added that cybercriminals have caused $6,000 billion in damage to businesses worldwide this year, and experts predict that this figure could exceed $10,000 billion by 2025. Hungary is doing everything to protect entrepreneurs and citizens, and our national security strategy places great emphasis on this threat, Szijjártó said, adding that the European Union and NATO will soon adopt a new cybersecurity strategy.

- **Senator Joni Ernst,** United States Senate (Video message)



United States Senator, Joni Ernst defended America's democratic values, stating that the United States fights with the consent of the people and that the US's military is very much prepared for the threats that the US faces.

- **Senator Kevin Cramer,** United States Senate (Video message)

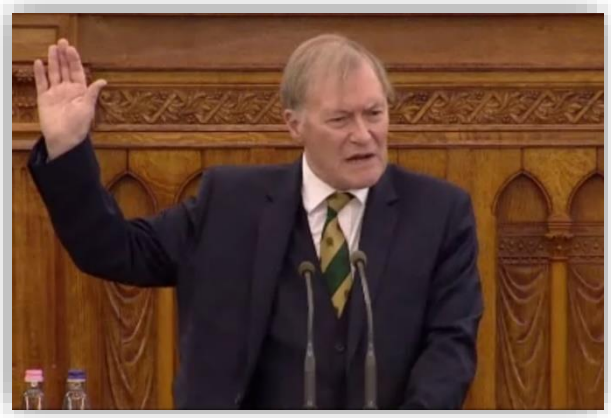


United States Senator, Kevin Cramer began his remarks by stressing how security must be our upmost priority. He then mentioned that cyber-security is very important. Afterwards, he pointed out that small states have as much potential to develop new technology as superpowers. He specifically referred to his North Dakota's contribution into innovative technologies. In addition he said that if corporations and universities don't care (only filling their pockets), then they would be completely disregarding the country's interest and security.

Keynote speech by:

- **Sir David Amess,** MP, United Kingdom, Member of the Panel of Chairs (United Kingdom)

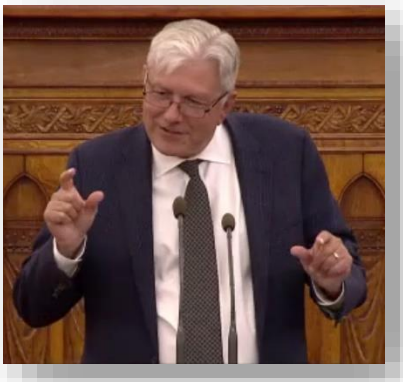
Sir David Amess began his keynote speech by praising how the US, the UK, and the rest of the world have come together. He then went on to speak about how he supports the democratization of Iran and is hoping for Afghanistan to do the same. He stressed on the threat that Iran poses and mentioned that the Taliban need to be dealt with at an international level. It is our responsibility to deal with terrorism, he stated.



He then went on to mention a few things regarding the Taliban. Minority groups are at the biggest risk of scrutiny in that country and stressed that they are at the biggest risk of human rights abuse apart from women and children. Animals are also at risk

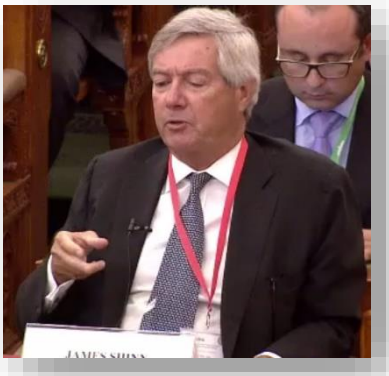
of abuse; therefore, they must be saved from that terror ravaged country. If the Taliban continue to abuse human rights, they cannot enjoy international recognition. He then went on expressing his concern over military technology being taken over the Taliban in abandoned bases.

Panel 1. – Risks and Rewards of Cryptocurrencies, Stablecoins and CBDCs



- **Mr. J.C. Boggs,** Partner and Co-lead, FinTech, Blockchain and Cryptocurrency practice, King & Spalding (United States)

- **Mr. Erik Bethel,** Distinguished Fellow at Chamber of Digital Commerce (United States)



- **Dr. James Shinn,** former Assistant Secretary, U.S. Department of Defense (United States)

- **Mr. Theodore S. Boone,** Of Counsel, Dentons Budapest, Member of the Faculty, Corvinus University of Budapest School of Business and former President of the American Chamber of Commerce in Hungary (Hungary)

These four distinguished panelists presented to the Parliamentarian Intelligence-Security Forum on Cryptocurrencies, Stablecoins and Central Bank Digital Currency (CBDC).

First, they explained the basics about these forms of currency and the differences between the three. Cryptocurrency is essentially a digital or virtual currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently from a central bank. Stablecoins are a subset of cryptocurrency where the price is designed to be pegged to fiat currency or basket of currencies, or to exchange-traded commodities (such as gold or other precious metals). The phrase central central bank digital currency (CBDC) has been used to refer to the various proposals involving digital currency issued be a country or region's central bank.
Second, the panel discussed the risks and opportunities associated with cryptocurrency, stablecoins and CBDCs. On the risk side, the panel talked about cryptocurrency being use for money-laundering, terrorist financing and ransomware. They also touched upon potential volatility of crypto in the currency markets, the threat to fiat currency sovereignty ("dollarization") and potential for disintermediation of the banking system. On on the other hand, the adoption of cryptocurrencies, including CBDCs, will likely increase financial inclusion, reduce payment costs (especially cross-border payments and foreign exchange), and is expected to enhance competition and innovation in the financial markets.

Third, the panel reviewed a number of regulatory and policy challenges around cryptocurrencies, noting that financial regulators typically have limited technical resources and recognizing that regulatory oversight of digital currency is often contested and subject to regulatory arbitrage. At the international level, they also mentioned that the World Bank, IMF and Bank for International Settlements (BIS) are playing low-key coordination roles.

At the conclusion of the discussion, the panel also referenced how China is leading the development of its own digital currency which presents cause for concern as China will want to export its cryptocurrency to other developing countries in exchange for debt reduction or other economic benefits. Further, mass surveillance will be achieved at an astronomically higher rate. For example, the government will be able to see every transaction on the digital ledger so that they know if you are purchasing forbidden reading material, such as a pro-democracy newspaper or a Bible. This will only lead to greater mass surveillance and dominion.

Panel 2. – Enhancing cooperation of Parliaments, Best Practices

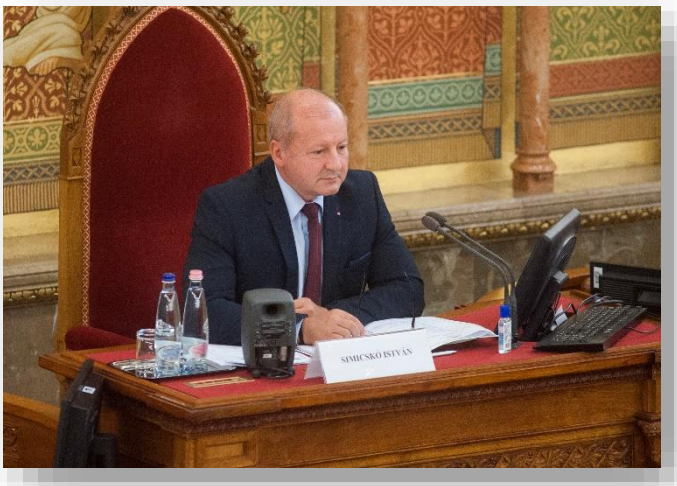
- **Hon. Cristian Bușoi,** Member of the European Parliament (Romania)

The Honorable Cristian Bușoi made remarks about regarding the transformation of cybersecurity in the medium and long term. He mentioned that there are already proposals by lawmakers to promote an open and safe cyber space. He mentioned pillars that lawmakers should consider, which are

- Strategy
- Preparation
- Strengthen partnership capabilities

He then talked about how there needs to be better cooperation between member states (EU).

❖ **Hon. István Simicskó,** Member of the Hungarian National Assembly, former Minister of Defense (Hungary)



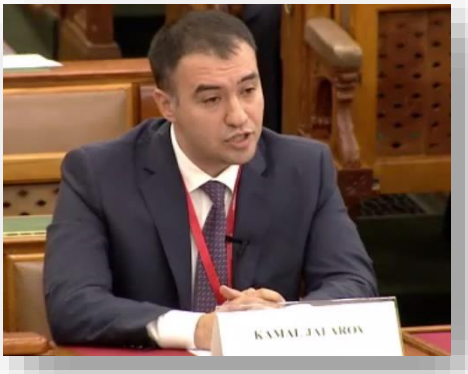
István Simicskó former Hungarian Minister of Defence briefly presented Hungarian achievements in the fields discussed, the Hungarian legislation adopted in this context and the institutional structures. He stressed that cross-border security threats can only be effectively tackled through international cooperation. A good example of this is the cooperation between the Financial Intelligence Units (FIUs) within the Egmont Group, which carry out analytical and evaluation activities on suspicious financial transactions. The Hungarian Financial Intelligence Unit (FIU), which is part of the National Tax and Customs Administration, has been actively involved in developing the Customs and Financial Intelligence Unit Cooperation Manual, a joint project of the World Customs Organisation and the Egmont Group. The manual serves as a guide for customs, FIUs and law enforcement authorities to cooperate more effectively in the areas of financial crime, money laundering and terrorist financing. Based on the 2017 national risk assessment on the risks identified in the area of money laundering and terrorist financing in Hungary and addressing and mitigating them, the number of money laundering offences through commodity trafficking in Hungary is low, with a risk rating of 1.8 (moderately significant) on a scale of 1 to 4 in the national risk assessment.

Governments use their own state resources to protect themselves against adversarial foreign investment. In Hungary, the purchase of a controlling stake and the pursuit of certain activities are investigated, authorised or prohibited by the licensing and supervisory authorities (e.g. the Hungarian Competition Authority, the Hungarian National Bank, the Hungarian Energy and Utilities Regulatory Office). The Hungarian authorities have been detected several adversarial foreign investment efforts in the last decade and a half, affecting key players in strategic sectors. The Constitution Protection Office has recently detected hostile foreign investment efforts by several smaller players in the credit institutions sector.

The Hungarian government considers digitalisation and 5G as a priority strategic area, as 5G is not only a telecommunication policy issue, but also an economic strategy issue. 5G is one of the most influential technological innovations of our time, radically expanding the capabilities of telecommunication services and fostering the emergence of radically new, innovative and sometimes disruptive services and business models in a wide range of sectors, including automotive, transport, manufacturing, agriculture, healthcare, energy industry, retail, entertainment and media. But the deployment of 5G also poses significant national security risks. In this context, we will monitor the activities of foreign telecommunication service providers and tech companies (in particular) to ensure that the Hungarian public sector involved in the 5G network roll-out is free from outside influence.
Hungary's AI Strategy for 2020-2030 prioritises the introduction of control systems for law enforcement. In the field of cyber defence, he mentioned the law, which established the Hungarian cyber defence organisational system. The National Cyber

Coordination Council and the Cyber Security Forum, established to channel private sector expertise into government decision-making, are strategic elements of this system. As a result of the 2015 amendment to the law, the National Security Special Service (NSS) was designated to perform operational tasks with regard to the information systems of state and local government organisations, and the National Cyber Defence Institute (NKI) was established within its structures on 1 October 2015.
In order to improve cooperation between parliaments, he has proposed the creation of a database of legislation and best practices on the issues on the agenda, which could help other countries to draft legislation in these fields.

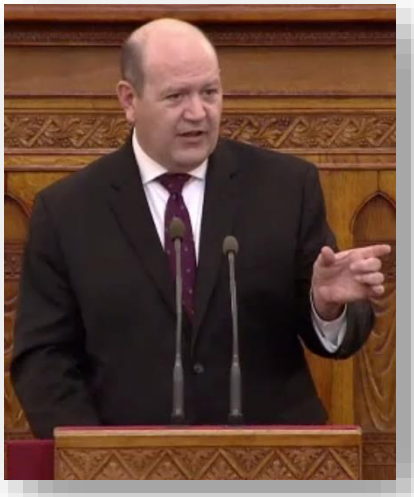
- **Hon. Kamal Jafarov,** Member of Azerbaijani Parliament, Head of Azerbaijani Delegation to GRECO (Azerbaijan)



Hon. Jafarov made brief remarks stating that only 1/3 of participant countries are not member of the European Convention and that cybercrime is a transnational crime.

Panel 3. - Assessing the risks of biological weapons use: the dual-use dilemma and challenges for arms control.

- **Dr. Steve Bennett,** Ph.D., Director Global Public Sector at SAS; former Director of the National Bio surveillance Integration Center, U.S. Department of Homeland Security (United States)



Dr. Steve Bennett made remarks regarding how to mitigate the risks of biological weapons arising from terrorism, nation-states, and naturally-occurring sources.

Take-aways:

Key policy actions:

- Mitigating biological weapons risks from terrorism
  - Continue to monitor scientific publications around the world
  - Withhold sensitive methodological details from open scientific publication
  - Place a premium on countering radicalization for highly skilled / highly trained scientists.
  - International collaboration and information sharing
  - Collaborate globally to deny terrorist organizations safe haven for biological weapons planning and training
- Mitigating biological weapons risks from nation-states

    - Continued international participation and support for the Biological Weapons and Toxins Convention (BWTC)
    - Strengthen and modernize the BWTC to cover new technologies like CRISPR and gene editing
    - Strengthen the BWTC Implementation/compliance functions with the BWTC
- Mitigating biological risks from naturally-occurring sources
    - Focus on Prevention, Prediction, and Early Warning
    - Apply Data, Analytics, AI, and Investigative analytics to help

Summary:

Biological weapons use presents unique challenges distinct from conventional weapons, or other forms of WMD like nuclear or radiological weapons. Unlike these other weapons, it can be difficult to understand the true risks posed by biological weapons because of the dual-use nature of biological and medical research – telling the difference between legitimate and nefarious research can be difficult or impossible. In this talk, Dr. Bennett discussed methods for assessing the risks from biological weapons deployed by terrorist organizations and nation-states, as well as the risks from naturally-occurring threats like COVID-19. In addition to highlighting the key factors that contribute to the risk, Dr. Bennett outlined key policy actions for each, presenting a roadmap for improving security and reducing proliferation of these threats.

Panel 4. - Human Trafficking/Illicit Finance

- **Ms. Anne Basham,** Chief Executive Officer at Anti Trafficking International (United States)

Ms. Anne Basham made remarks regarding human trafficking. According to her reports, there are 40.3 billion people that have been enslaved and points that human trafficking is the second largest criminal activity in the world, however, she argues that it might be number one.

Now, who is targeted? The popular age is between 11 and 15 years of age, mostly girls. According to the report, this illicit activity is a primary source of revenue for terrorist financing.

How can it be stopped or prevented?

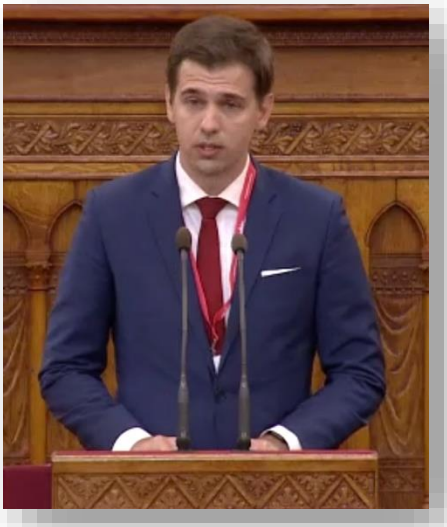
- Follow the money – see where all the money is flowing to
- Education – assign funds for schools to implement human trafficking education to the school curriculum

What can we do?

- Defensively – cut flow of money
- Offensively – provide money for education

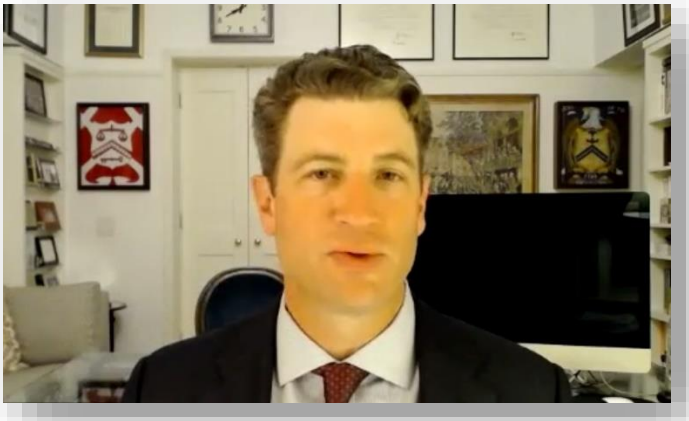
Panel 5. - Abusive practices in global economic expansion

❖ **Mr. Milos Ivkovic**, MA, LLM, LLM, International Arbitrator / Advisor to Governments (Austria)



Mr. Miloš Ivković commenced his speech by addressing major abuses and violations of international law committed by foreign adverse powers disguised as investors. He recalled that, at present, illegal child labor flourishes in many oppressed countries. The governments at need feel forced to accept predatory credits and hand over their respective economies which, in turn, become controlled by the same adverse powers who breach domestic and international laws. Mr. Ivković concluded that the allied states are not only confronted by a matter of national security, but the crises thereof. In conclusion, Mr. Ivković invited MPs to strengthen their alliances and continue their fight for the future of our children and the freedom we all stand for.

❖ **Hon. Brent McIntosh,** Former Under Secretary for International Affairs, U.S. (Virtual)



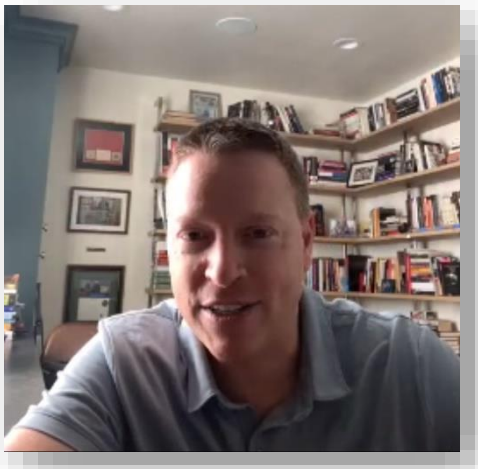
The Honorable Brent McIntosh made remarks regarding adversarial practices in economic expansion. He talked about foreign adversaries' efforts to acquire American businesses in sensitive sectors for non-commercial reasons, including businesses that hold Americans' sensitive personal data. He also discussed the state of sovereign borrowing and suggested improvements.

What do we need to do?

- We need a multilateral efforts of likeminded countries to combat adversarial foreign investment. We need share best practices and lessons learned in investment screening, as well as information on threats and adversary tactics. Through this all, we must be very vigilant.
- As to sovereign debt, both borrowing countries and lending countries must know we are paying attention to the terms of their arrangements. Ensuring that the IMF, the World Bank, and countries such as the United States have visibility into developing countries' sovereign debt situations helps ensure that those countries do not find themselves subject to predatory terms or fall into unsustainable debt profiles.
- Take away?

It is critical to continue to advance sustainability and transparency in sovereign debt, just as it is essential that we continue to bolster out investment screening mechanisms to thwart adversarial foreign investment.

❖ **Hon. Matt Pottinger,** Former Deputy National Security Advisor (United States)



Hon. Pottinger began his remarks by saying that Beijing has viewed the United States as their adversary for decades. China has waited patiently to accumulate power over the past few decades.

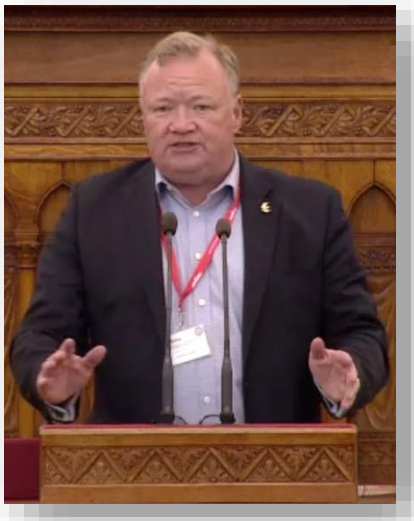
In addition, he stated how president Xi has deliberate plans to decouple from major economies on Beijing's terms, and accumulate economic leverage to coerce countries into making political concession that threaten their sovereignty. The US and Europe must work hard to restrict flow of investment to China's tech sector.

What must be done?

- Capital flows – money is used for human right abuses and to build China's military juggernaut
- Information Flows – offensive/defensive strategy is needed
- Technology flows – restrict exports that would allow China to become self-sufficient in making semiconductors.

Panel 6. - The dual use of AI – Possibilities and risks, legal regulation, cybersecurity, 5G

❖ **Mr. John Strand,** CEO, Strand Consult (Denmark)



Mr. Strand began his remarks by stating that telecommunications are essential and vital in our society. In the coming years, the cloud will be fully integrated with 5G. On that note, the Chinese government owned and military aligned firms provide many products and services across the network and infrastructure. This is concerning because of technical vulnerabilities (backdoors, kill switches which can be illicitly installed in the equipment) as well as illegal and unethical Chinese government government practices including surveillance, human rights violation, and so on. A kill switch is a force operation designed to shut down network, device, or piece of software. Circuits can be enabled with a kill switch which can trigger a shutdown of the device in which they are embedded or in other parts of the equipment. The Chinese government could use a kill switch

to shut down networks or equipment in retaliation for Taiwan or other disputes. For more information please look at this research note: All countries should have at least one mobile network free from Chinese tech like Huawei and ZTE and this research note: Yesterday the White House, UK government and European Union simultaneous published statements calling for China to stop cyberattacks. What is the impact for the telecom industry?

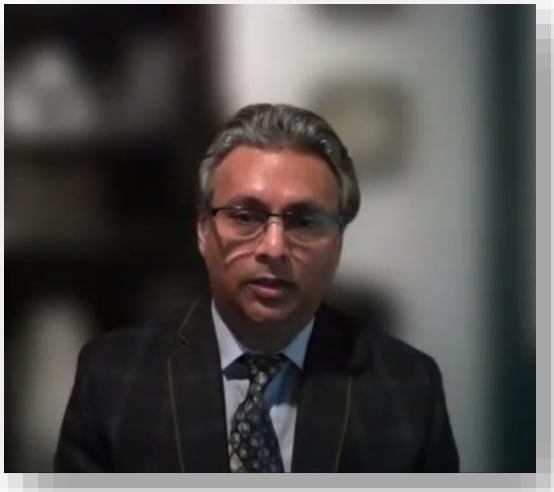
❖ **Hon. Pavel Popescu,** Member of Parliament (Romania)

The Honorable Pavel Popescu began his remarks by saying that the world we live in is not the same world as 10-20 years ago. It is constantly changing; therefore, we need the appropriate legislation for this "brand new world". The solution to this is to bring experts into parliament in order to make proper legislation.

❖ **Mr. Jacob Norwood**, Cybersecurity Executive, Booz Allen Hamilton (Netherlands)

Mr. Jacob Norwood made remarks about artificial intelligence. He had a pro-AI approach. He talked about how AI can be very beneficial to detecting data breaches. An example he stated was on how companies currently take a long time to detect data beaches. He specifically referred to an enterprise who was breached and how it took them a while to figure out that multiple smaller incidents were all part of a much larger breach. With AI, he argued, we would be able to detect these breaches in a matter of hours, given data of sufficient quantity and quality. He also noted that bad actors have access to the same technology and, when combined with personal, corporate, or national data, they can use AI and that data to pick targets for espionage, influence, or for breaches. How can we combat this issue? We need to invest more in cybersecurity and AI in order to counter this problem. Most importantly, lawmakers can pass legislation to protect national, corporate, and citizen's data, preventing it from falling into the hands of adversary AI.

❖ **Mr. Surjeet Mahant**, Managing Director at K2 Integrity and head of Cyber Risk Management Services (United States) (Virtual)



Mr. Mahant argued that cybersecurity is one the leading areas where AI could be most effectively leveraged, an early warning mechanism coupled with cohesive threat intelligence garnered using AI technology will allow a robust ability to dynamically identify, protect, detect and respond.

Panel 7. - Illicit finance, financial integrity software solutions, biological warfare

❖ **Dr. Gábor Simonka,** Head of HFIU (Hungary)

Dr. Simonka made remarks about money laundering and the role of FIUs.

Money Laundering

- The perpetrators of money laundering legitimize the proceeds of crime – concealing or disguising the criminal nature of funds
- Illicit financial flows/activities occur in the forms of transactions such as:
    - Cross-border funds transfer via transit accounts
    - Real estate purchase
    - Transactions on virtual currency
    - Trade-based money laundering related transactions
    - Gambling activities
- Representatives of the private sector have the knowledge, experience, and expertise to detect the unusual, illicit, suspicious activity of perpetuators – obliged entity

After that, he gave a brief overview of the functions of the Financial Intelligence Units (FIUs). FIUs are entities that aid in the fight against money laundering through suspicious reported emitted by the private sector, specifically banks and financial institutions.

Core Functions of an FIU

- Receive information from private entities (obliged entities)
- Analyze information
- Disseminating information
- International information exchange with other FIUs

Essentially, FIUs transform **financial information/intelligence** (emitted by private sector) **into criminal intelligence**.

Egmont Group is an international body of FIUs. This organization is a web of FIUs at an international scale that support each other with information sharing to combat money laundering**.**

Egmont Group

- International body – FIUs are members
- Provides a global platform for international exchange
- Setting up standards with which the FIUs must comply
- Supports the groups of the FIUs through its project and its capacity-building training centre (ECOFEL)

If an obliged entity suspects that funds from the proceeds come from illegal sources, it should be required, by law, to report promptly the suspicions to the FIU

Reporting obligation of obliged entities

- Subjective - the obliged entity decides on making a report
- Low level of suspicion
- Inclusive – the reporting obligation covers the predicate offenses
- Reporting obligation is basically determined by red flag indicators, typologies, and profile
- Obliged entities follow the international and national indicators
- FIU feedback improve the reporting practices of obliged entities

FIUs share information at a global scale. He then explained how it is shared.

International Information Sharing

- Routinely carried out by FIUs
- Exchanging financial information between LEAs and judicial authorities (MLA at an international level
- Exchanging financial information is not the monopoly of the FIU. In other words, they share more than just financial information

After talking about how FIUs share information, he began with remarks related to how the increasing peed of transactions make it more challenging to detect illicit activity.

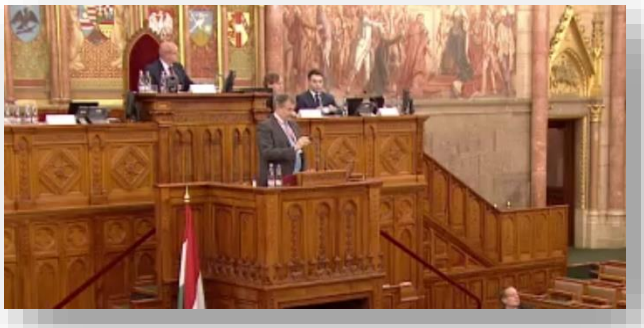
The Speed of Transactions

- Need of customers increased – credit institutions serve the customer
- Cross border transactions became very fast
- This feature becomes very apparent in the cross-border transfer of fraud-related funds
- Difficult to identify illicit financial flows on time during the monitoring activity of the credit institutions and other obliged entities
- Fast cross-border transactions should be counterbalanced with effective monitoring activity

Afterwards, he concluded by saying that FIUs play a key role in in the fight against money laundering, TF, and proceeds-generating crimes. He also said that exchanging information through LEA's and judicial authorities (MLA) at international levels should be enhanced. Also, the role of advanced IT solutions and the need for PPP mechanisms has significantly increased in the AML/CFT domain. He later suggested the strengthening of the supervisory bodies of non-financial obliged entities and the cooperation between these supervisory bodies and the FIU.

❖ **Hon. Andreas Frank,** AML/CFT advisor for the Bundestag, Council of Europe and the European Parliament (Germany)

Hon. Frank made remarks regarding illicit financial flows (IFF). IFF, as he explained, are illegal movements of money or capital from one country to the other. After that, he talked about the Taliban's involvement in this practice and their sources of income, which includes:



- Drugs - $560 million
- Mining - $537 million
- Extorsion and taxes - $215 million
- Charitable donations - $322 million
- Exports - $322 million
- Real estate - $107 million

He then went on to explain how corruption was the most serious threat to war on terror.

- The US government has spent 20 years and $145 billion trying to rebuild Afghanistan
- More on Afghanistan that the reconstruction of Western Europe after WWII
- Reconstructing Afghanistan has been the largest expenditure to rebuild a single country in US history
- 30% of the US taxpayers' funds were misappropriated
- Corruption has eroded the legitimacy of the Afghan government, limiting its effectiveness, and bolstering support to the opposing insurgency

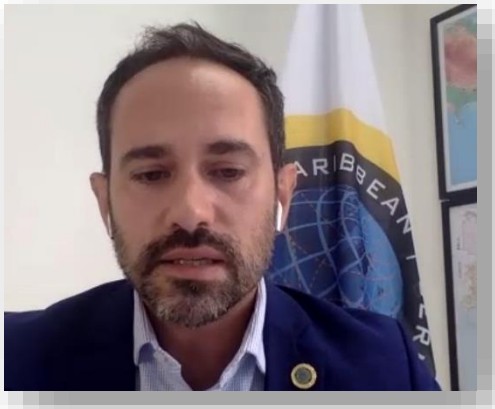
Afterwards, he changed the topic to talk a little about climate change. According to NATO, climate change is a threat multiplier. Then he made remarks regarding environmental crime, which is an ongoing war between autocracies and democracies.

What needs to happen?

- As an inherently transnational issue, global money laundering is perhaps the definite problem in cross-border crime
- The G-7 founders of FATF must take lead again in strengthening and enforcing global norms
- Implementation and enforcement of the AML/CFT norms need to be properly resourced

Panel 8 – Illicit trade, trade-based money laundering, adversarial foreign investments, adversarial threats

❖ **Mr. Alejo Campos,** Regional Director – CEO, CBLA Crime Stoppers (Panama) (Virtual)



Mr. Alejo Campos made remarks focusing on the issue of illicit trade. He suggested that there needs to be stronger multilateral cooperation. Then he went on to speak about the model law:

- Legal framework for implementation of laws
- Model laws in Latin America and the Caribbean would be good laws to implement in Europe

Why is illicit trade an issue that must be focused on?

- It has a negative impact on tax collection (illicit proceeds don't pay tax, while licit proceeds do)
- It detours the market
- Negative economic and health consequences

How do we prevent illicit trade? According to Mr. Campos, it is in collaboration with the private sector (information sharing). Parlatino helps in the fight against illicit trade.

Recommendation:

- Understanding trade-based money laundering
- Establishing cooperation
- Working with the private sector
- Specific profiles to money laundering and FIUs

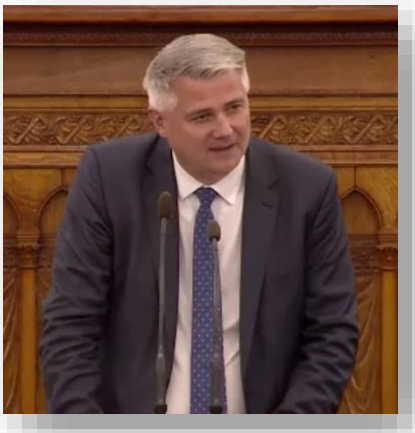
He finished his remarks by saying that this is a global problem, therefore it needs a global law.

❖ **Dr. Sohan Dasgupta,** Former Deputy General Counsel, U.S. Department of Homeland Security (United States)

Dr. Dasgupta discussed the National Security threats that we face, more specifically the threats we face by using technological infrastructure such as 5G. 5G may completely transform our lives; however, there is a potential for grave damage to the supply chain. These threats emanate from giving untrustworthy actors virtually unchecked power and control over our technology, infrastructure, and data.

Relatedly, there are steps that may be taken to limit the risk. In the United States, for instance, the Committee on Foreign Investment in the United States (CFIUS) is empowered to review foreign entities' acquisitions in the United States that may jeopardize America's national security. Specific scope and criteria affect that analysis. Other nations may use their own criteria to mitigate national-security vulnerabilities through adversarial foreign investment.

❖ **Hon. Andreas Jahn,** Bundestag Foreign Policy Senior Advisor (Germany)



Hon. Andreas Jahn, Senior Foreign Policy Advisor, made very extensive remarks regarding predatory investments. He underlined that especially European SMEs are extremely on the focus of cyber-attacks. He especially highlighted that the political leadership in Europe has to raise awareness together with the strategic economic stakeholders of the Western would in order to protect our economic infrastructure in Europe against predatory investment of foreign countries.

Open Floor Dialogue

Pakistani Delegation

This speaker representing Pakistan stated off their remarks by extending their gratitude. She then suggested for there to be more women speakers in the forums.

Egyptian Delegation

This speaker from Egypt said that they are committed to work together to combat all the mentioned issues and is asking parliamentarians to do their part

Ghana Delegation

This speaker made remarks regarding human trafficking and the challenges that we face. He said that it is important to engage in government-to-government collaboration.

Albania Delegation

This delegate made remarks stressing the fact that to combat these issues, we need bilateral, transnational, and international cooperation.

Yemen Delegation

The Yemenis delegate made remarks on how Iran is trying to take the heart out of the Arab people. They stated that not all Arab nations are rouge and most support democracy. He also made remarks on how he wishes that Israel and Palestine find a solution and most importantly peace.

Closing of the Conference

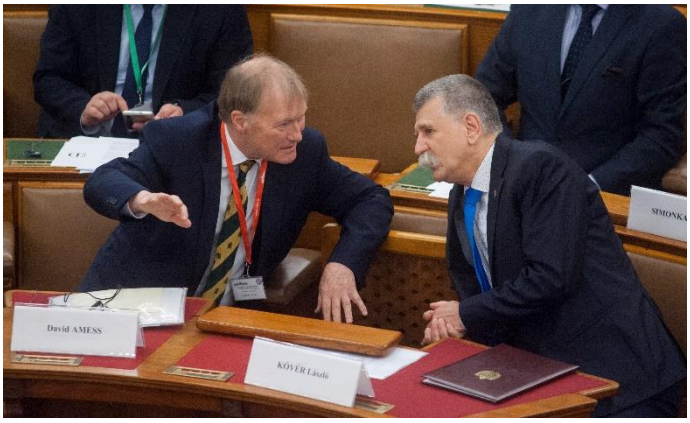
- **Congressman Robert Pittenger,** Chairman, Parliamentary Intelligence-Security Forum (United States)

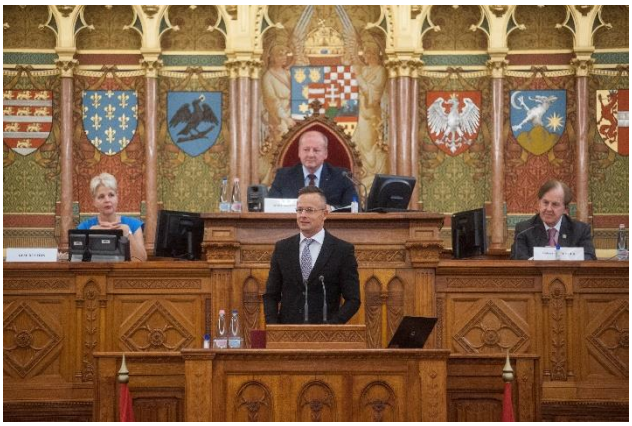
Congressman Robert Pittenger concluded the forum by thanking everyone for having attended and inviting everyone to the Washington Forum.

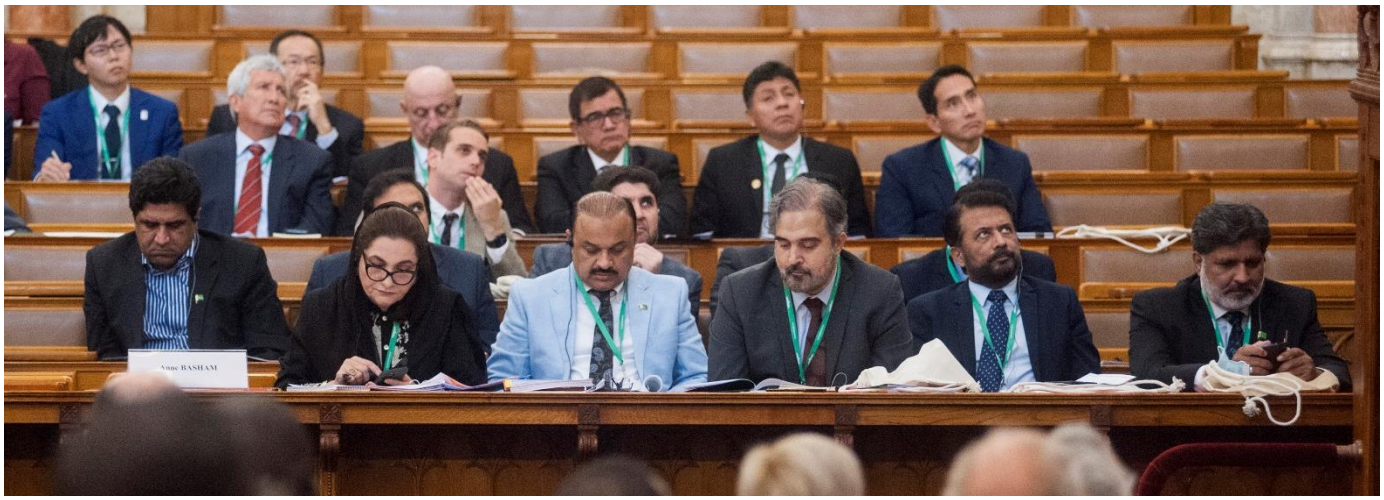
- **Hon. István Simicskó,** Member of the Hungarian National Assembly, former Minister of Defense (Hungary)

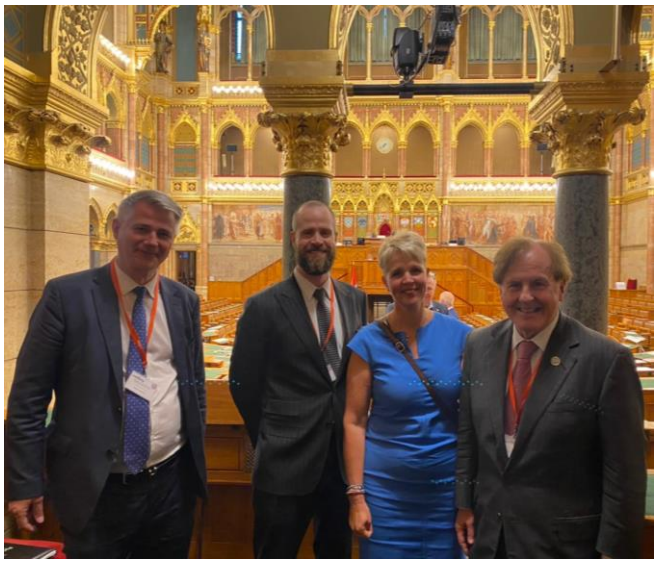
Hon. Simisko started off with a joke. Afterwards he made remarks thanking everyone for their attendance. He praised everyone for their commitment to resolve issues of the world. He suggested for an erection of a statue like the Statue of Liberty, the “statue of responsibility”.

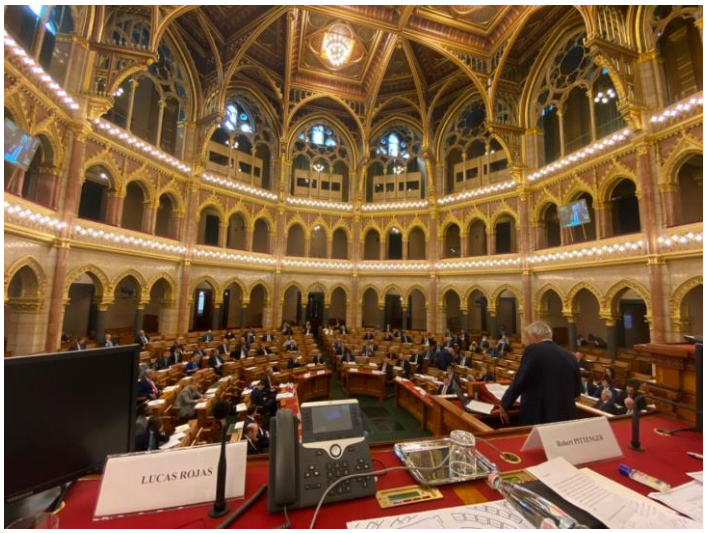
Pictures from the Forum, U.S. Embassy Reception and more

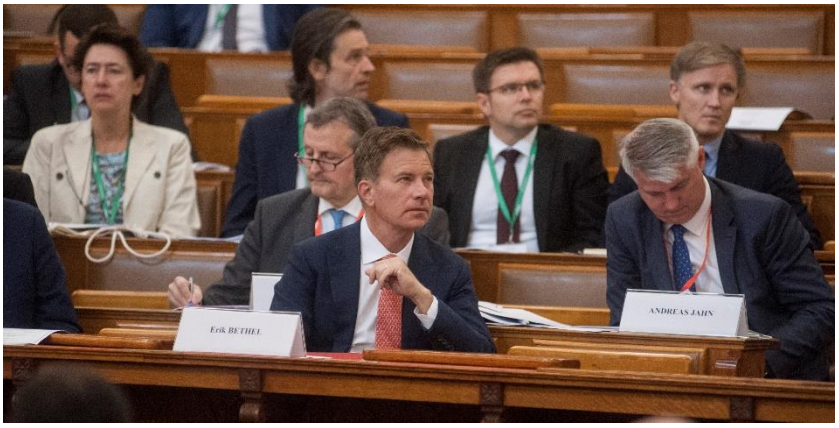


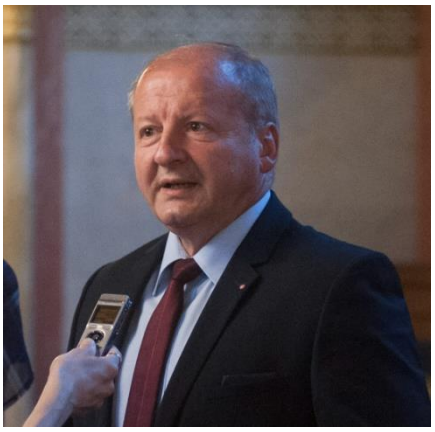


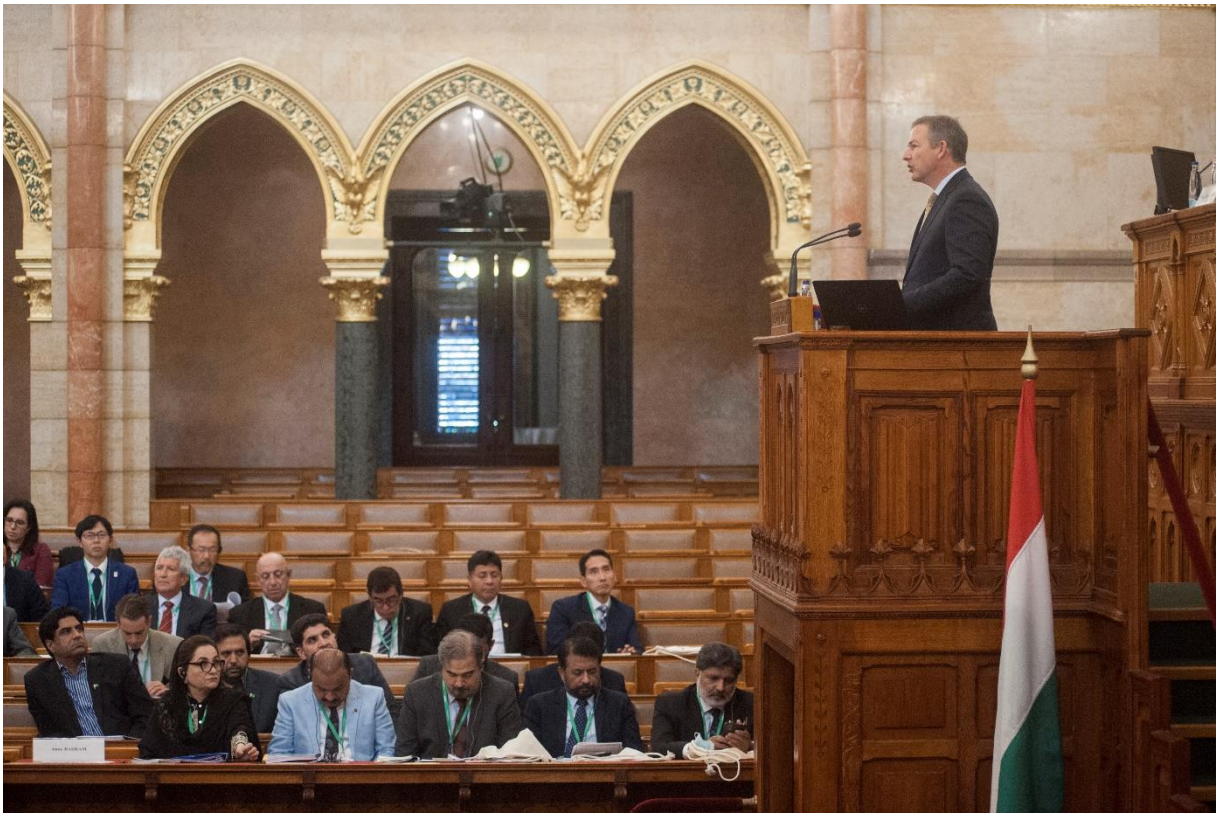


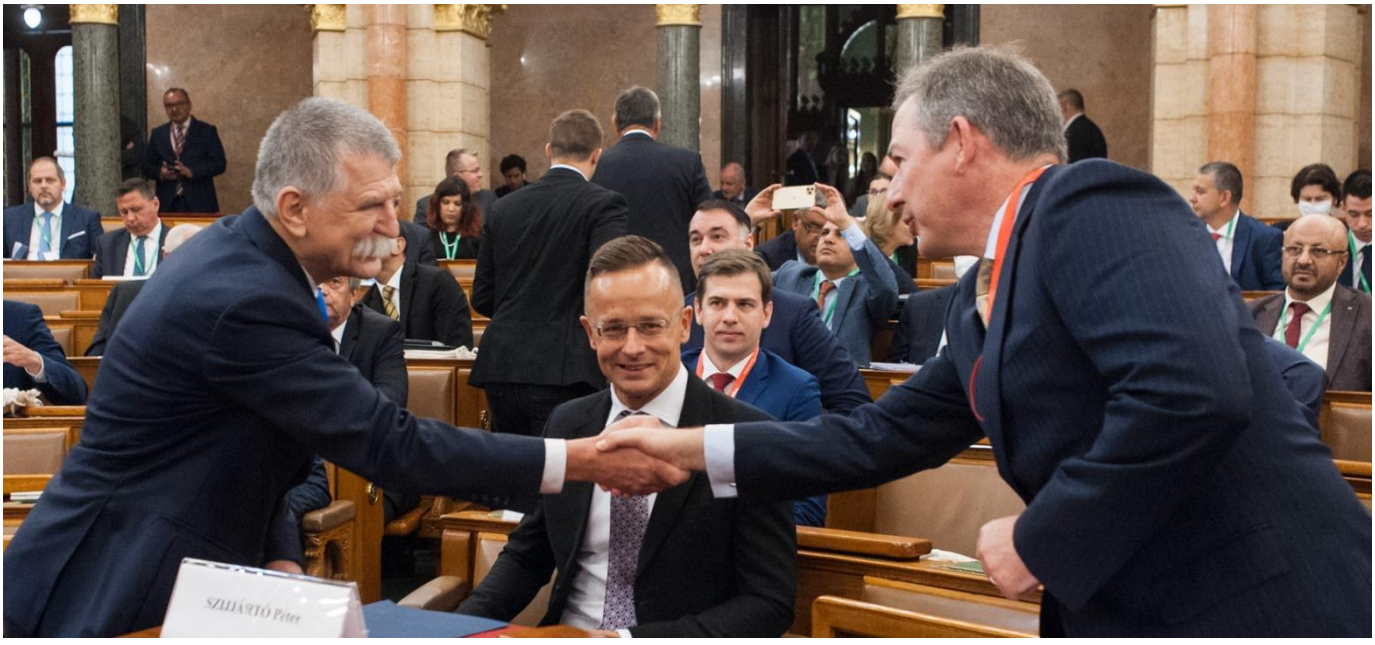


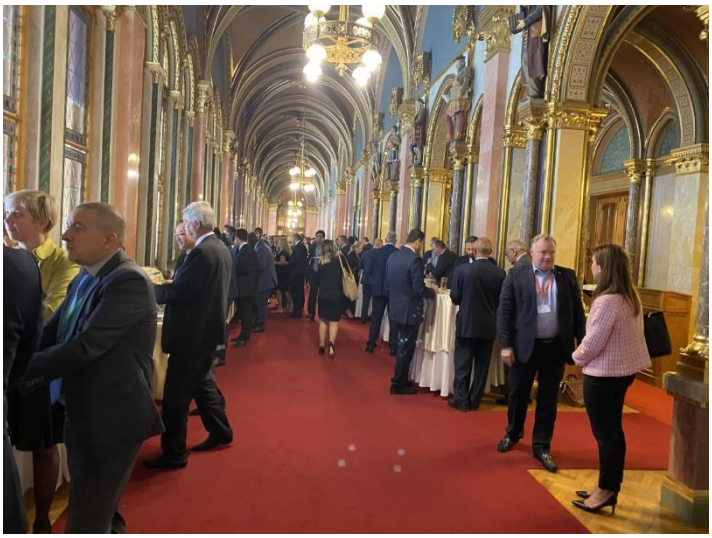


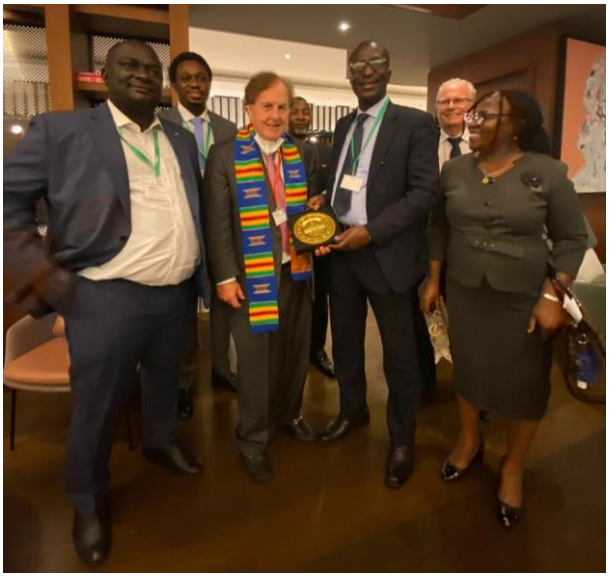

Erik BETHEL
ANDREAS JAHN

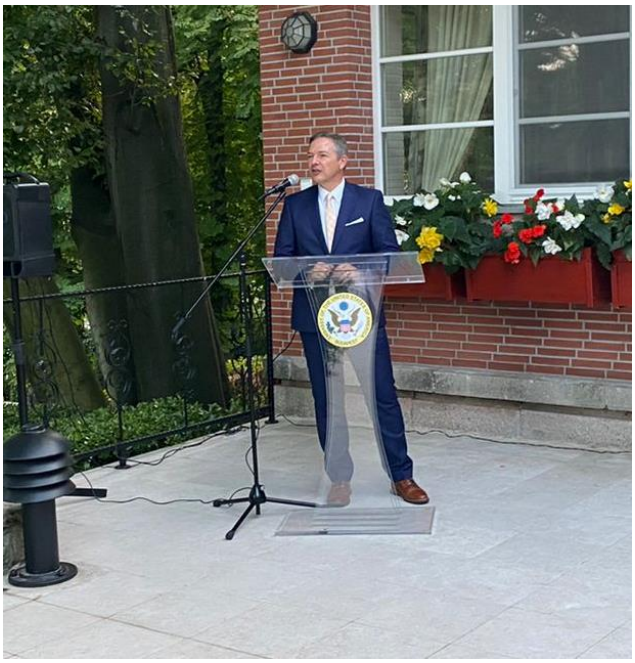


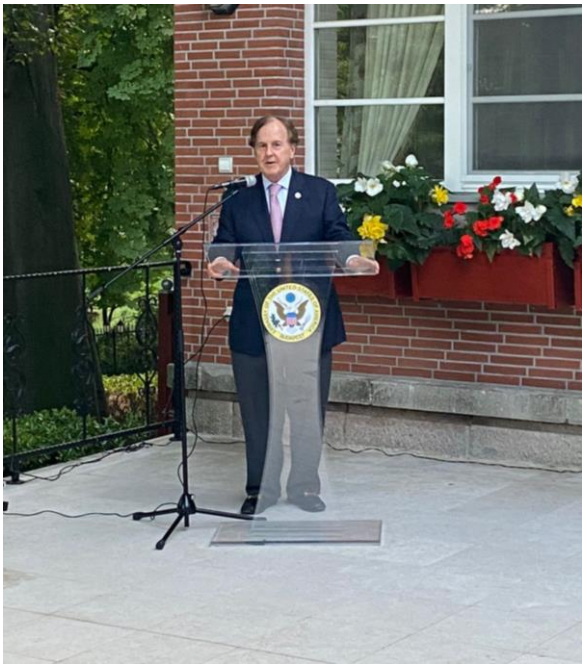


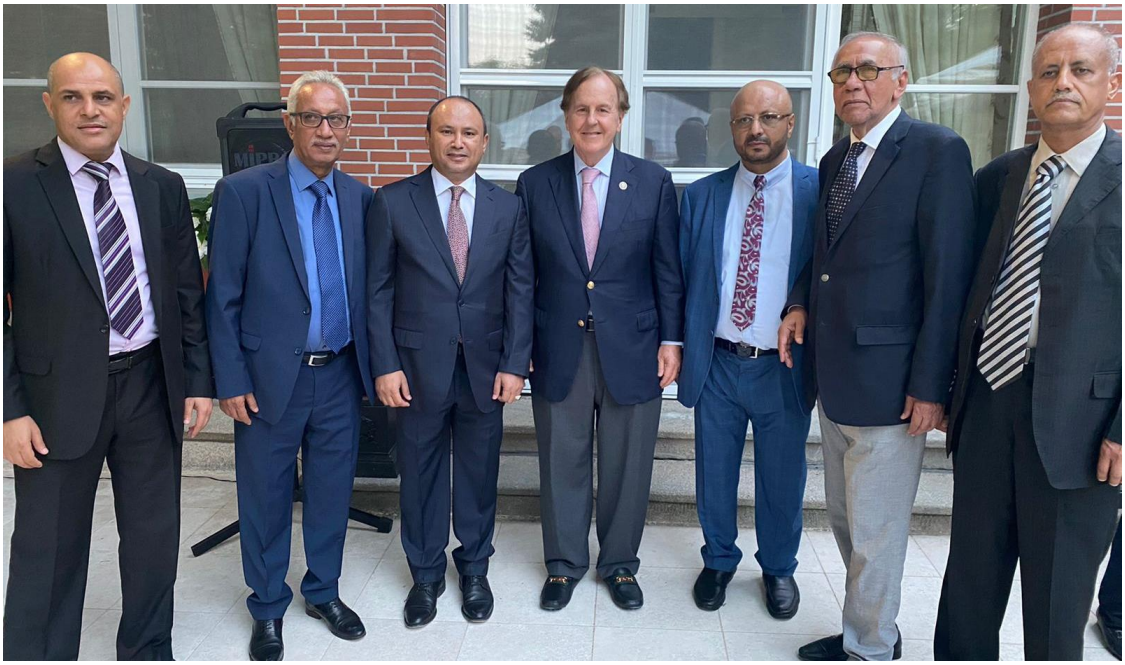

SZIJJÁRTÓ Péter

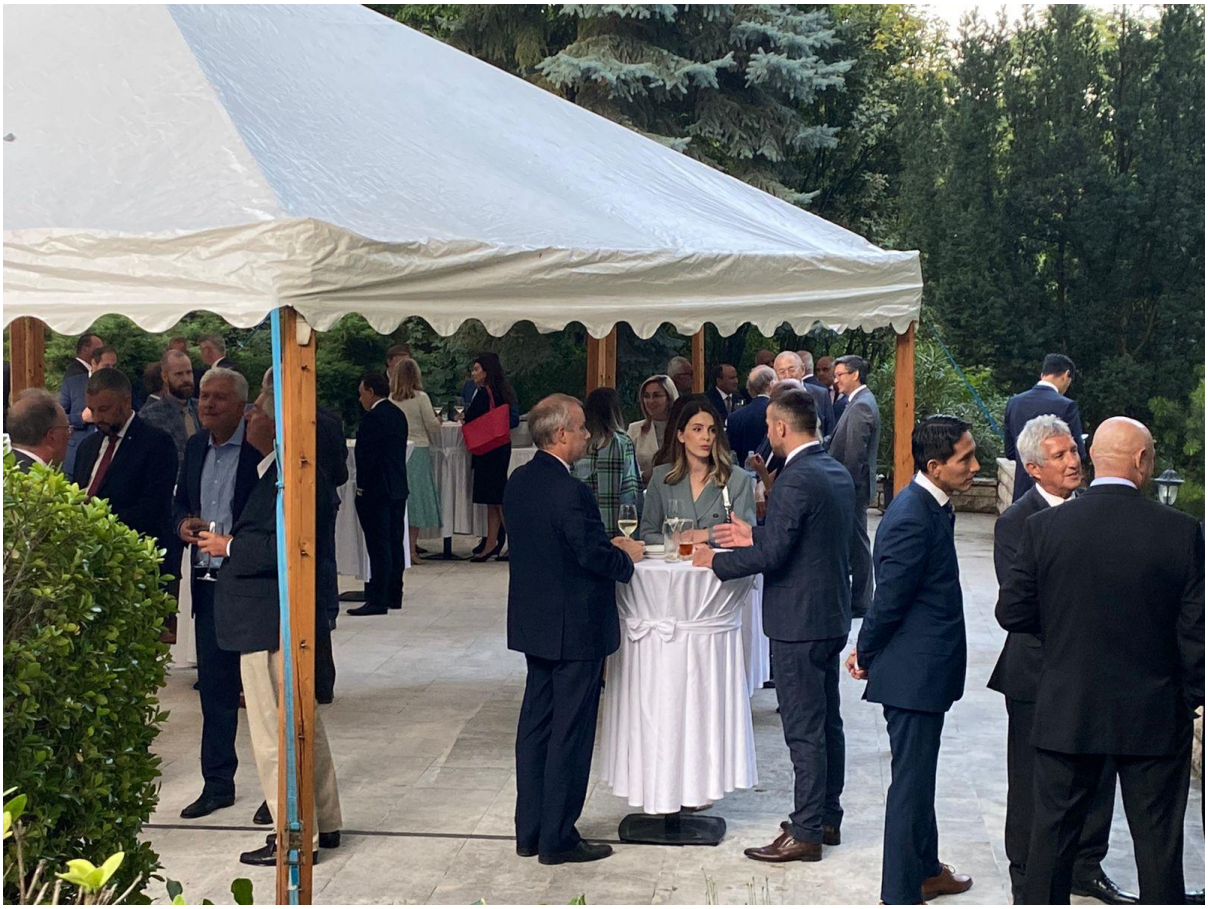


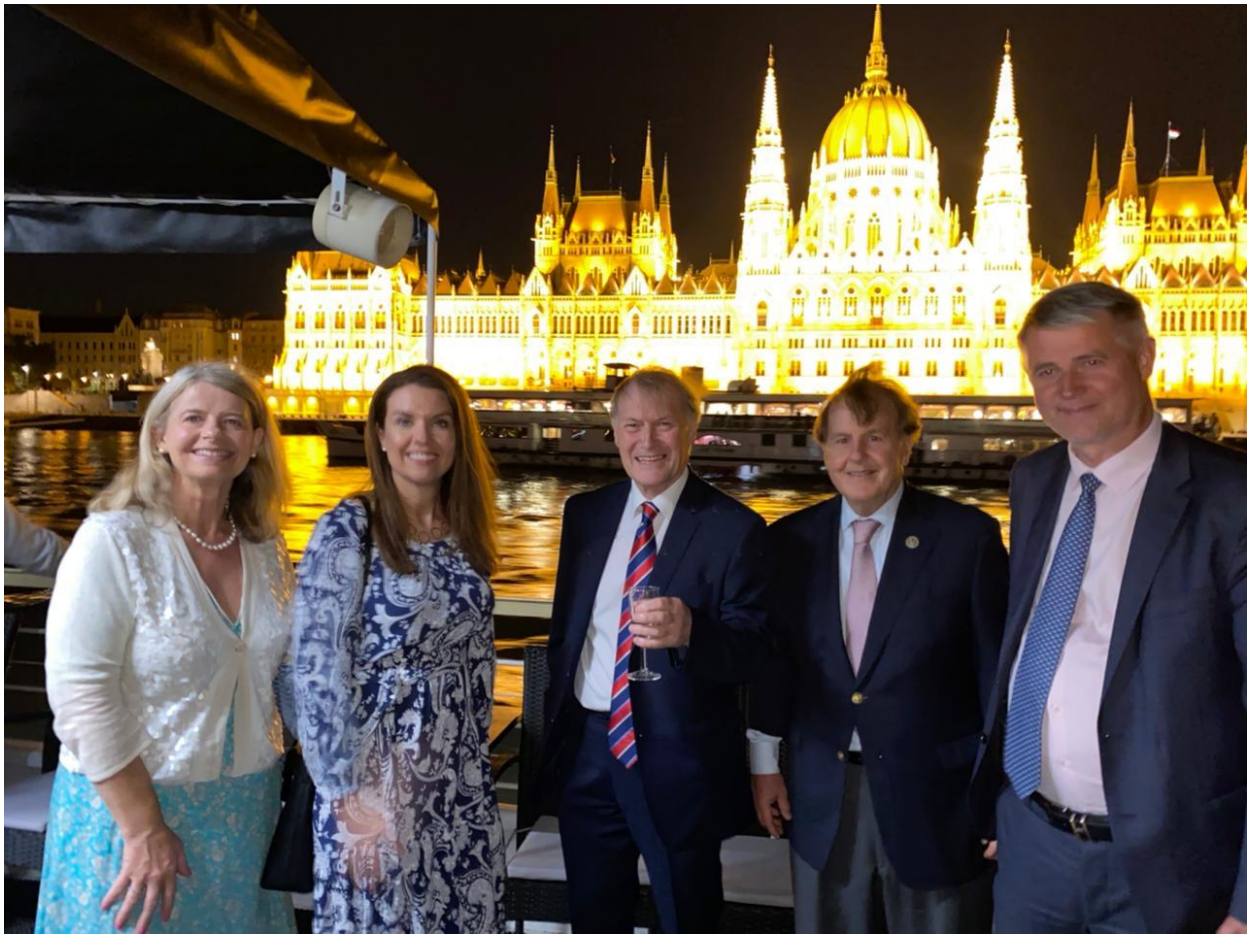


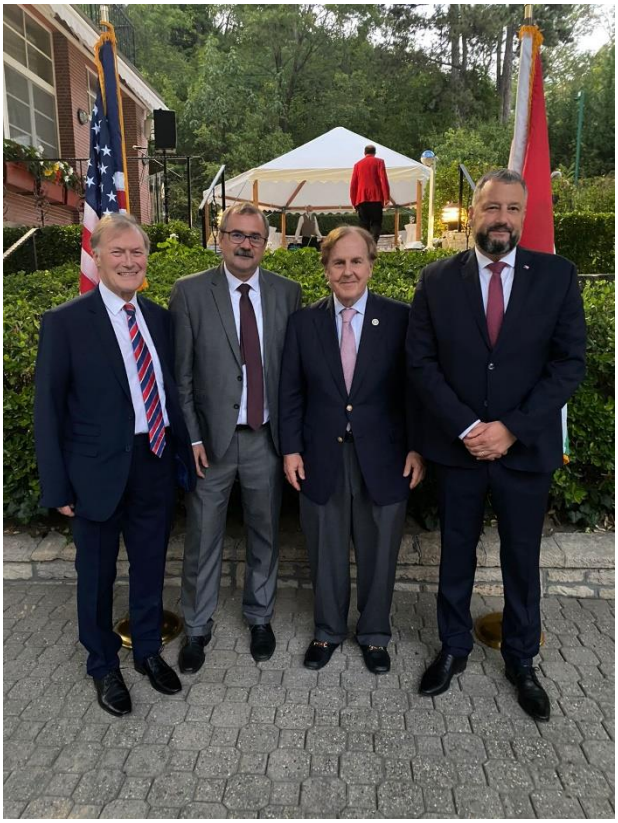


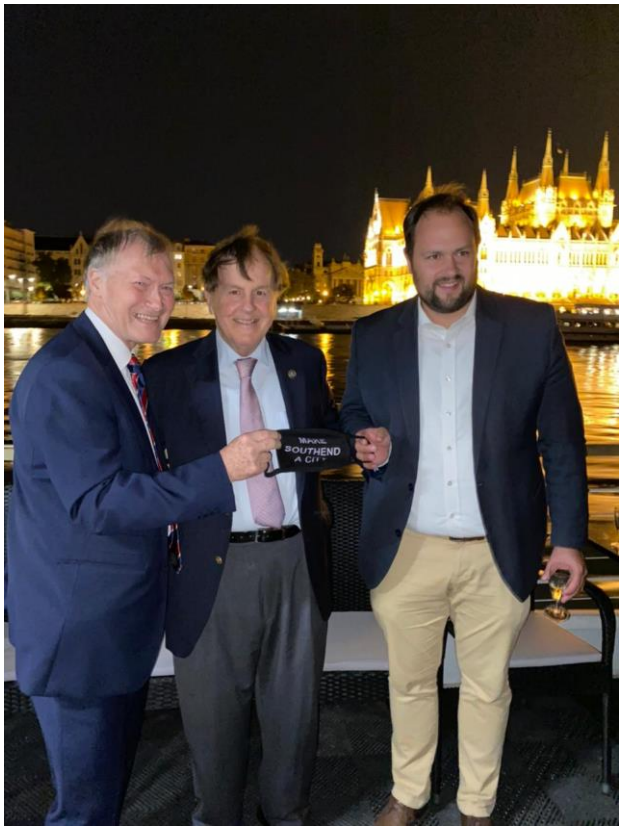


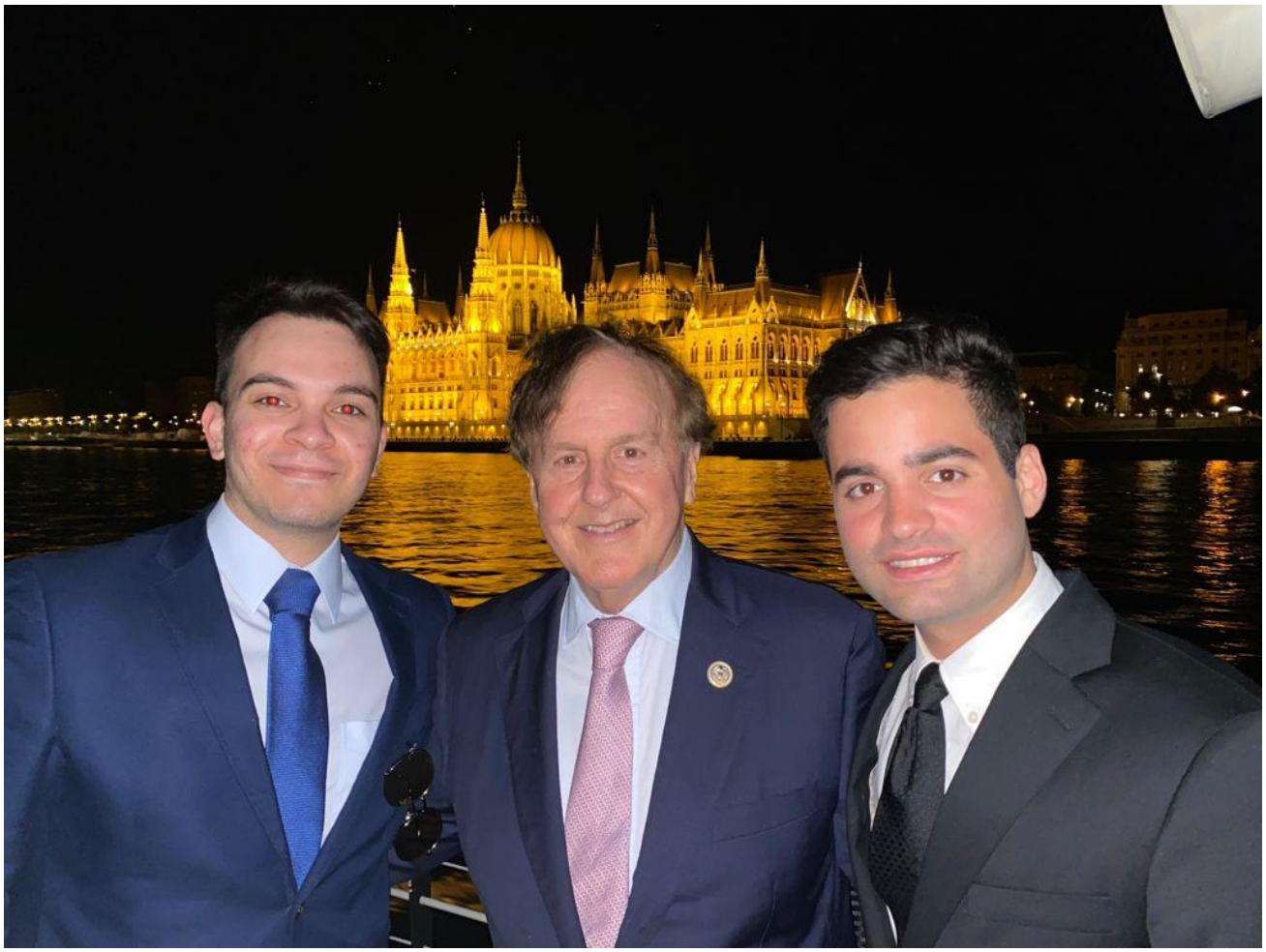


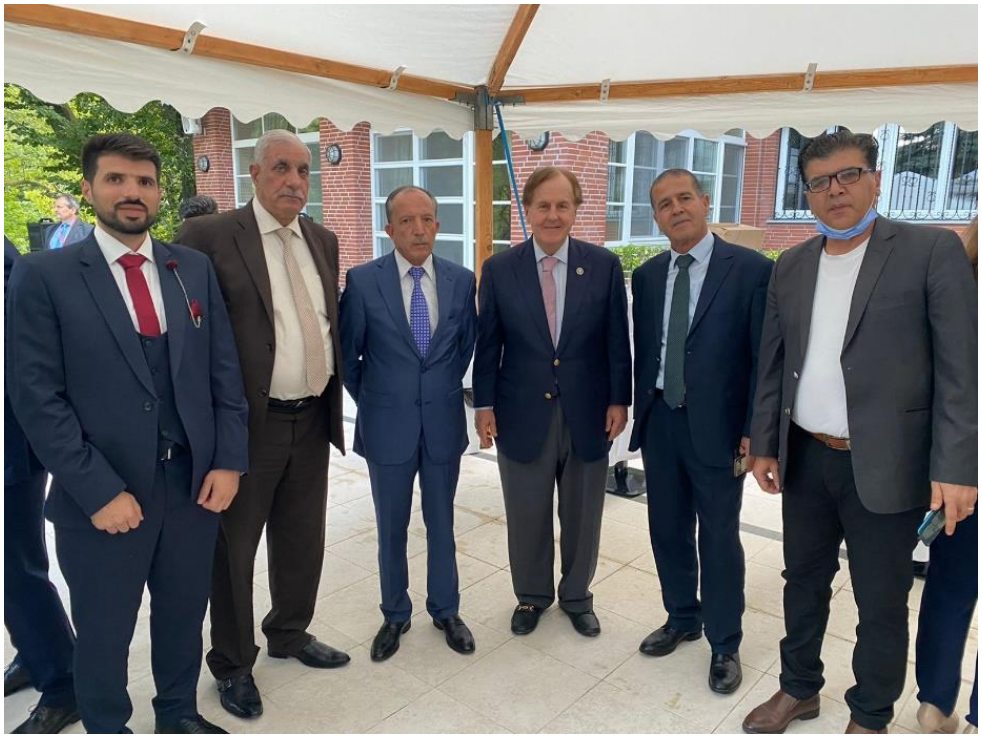


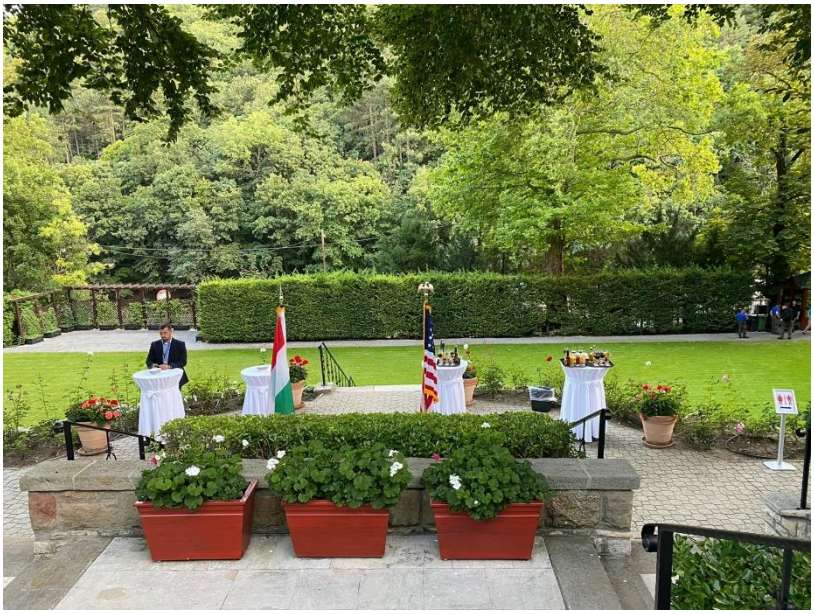


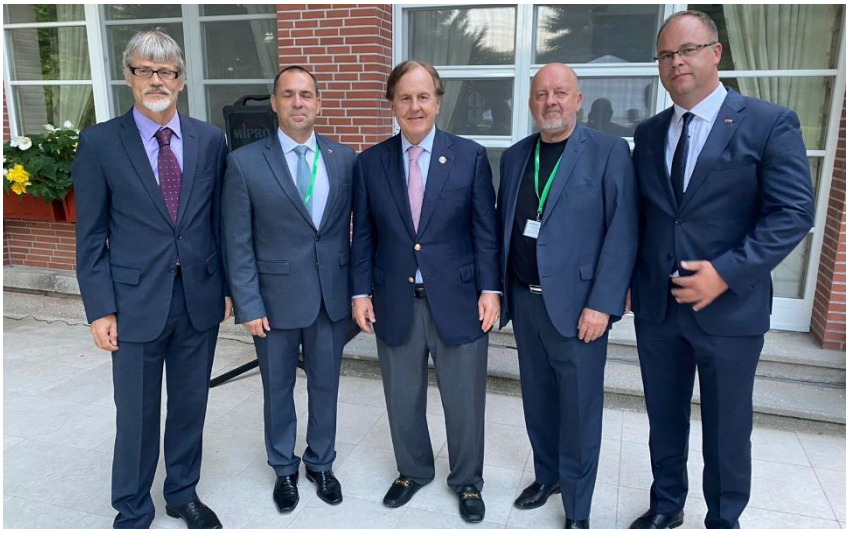



SOUTHEND
A CITY









Communique of the Parliamentary Intelligence-Security Forum held in Budapest, Hungary on September 6, 2021.

Considering that the Parliamentary Intelligence-Security Forum is the leading international security forum to increase understanding and providing expertise and collaboration among Parliamentarians and government officials with the United States' allies and partners regarding the global threats of terrorism in all its manifestations and in adversarial nation states, while creating actionable solutions that counter these threats.

Considering that the Parliamentarians, who write the legislation and fund the government are critical players in this mission, the Parliamentary Intelligence-Security Forum organized a one-day conference co-hosted by the National Assembly of Hungary.

The Forum is emphasizing that the presentations and panel discussion from Parliamentarians and experts from every corner of the world highlighted the challenges all participating countries are facing.

The Parliamentary Intelligence-Security Forum is recognizing the efforts from many countries (certain countries to strengthen their efforts) in the fight against illicit trade, all forms of transnational organized crime, money laundering, human trafficking, cyber security, 5G, foreign investments and the financing of terror.

The Parliamentary Intelligence-Security Forum states that more support from developed economies is needed for the countries to keep up their efforts.

We must strengthen bilateral, cross border, regional, and international cooperation through the Parliamentary Intelligence-Security Forum and the Inter Parliamentary Union (IPU) and other similar fora.

We are looking forward to the next Parliamentary Intelligence-Security Forum in Washington, DC.

Articles about the Forum

https://hungarytoday.hu/intelligence-security-forum-budapest-hungary-kover/

https://en.vietnamplus.vn/vietnam-attends-18th-parliamentary-intelligencesecurity-forum/207525.vnp

https://www.sggp.org.vn/dien-dan-an-ninh-tinh-bao-nghi-vien-lan-thu-18-ban-ve-rui-ro-tien-so-va-muc-dich-su-dung-kep-cua-tri-tue-nhan-tao-759509.html

https://www.qdnd.vn/chinh-tri/tin-tuc/thuong-tuong-tran-quang-phuong-du-dien-dan