



MADRID PARLIAMENTARY INTELLIGENCE-SECURITY FORUM
MAY 22-23, 2025

SUMMARY REPORT



MAY 22nd

OPENING REMARKS

- **Congressman Robert Pittenger**, Chairman, Parliamentary Intelligence-Security Forum

Congressman Robert Pittenger welcomed participants to the Parliamentary Intelligence-Security Forum in Madrid, held at the Senate of Spain. He expressed gratitude to the President of the Senate and acknowledged the leadership of Speaker Rollán and his team in organizing the forum.

He emphasized the vital role of parliamentarians in shaping legislation and allocating national resources, underlining the importance of their access to current, transformational technologies. Congressman Pittenger noted that the forum has no commercial agenda—only a sincere commitment to supporting lawmakers in their leadership for global freedom and security.

Congressman Pittenger concluded by turning the floor over to the Speaker, expressing deep appreciation for his contributions to making the forum possible.

- **Hon. Pedro Rollán**, President of the Senate

In his opening remarks, Hon. Pedro Rollán, President of the Spanish Senate, warmly welcomed participants of the Parliamentary Intelligence-Security Forum and expressed gratitude to Congressman Robert Pittenger and the diplomatic community. He emphasized the significance of hosting such a prestigious international forum in Madrid, noting that it provides an important opportunity for reflection, dialogue, and the development of practical proposals on global security. President Rollán highlighted Spain's commitment to supporting these efforts, offering the full collaboration of the Senate to ensure a successful event. He underscored the forum's importance in addressing vital issues with the participation of global experts from both public and private sectors.

President Rollán detailed Spain's prominent role in global security, citing its geostrategic position, NATO and EU membership, and its historic and cultural ties with Latin America and North Africa. He acknowledged Spain's painful experiences with terrorism, including the ETA and the 2004 Madrid train bombings, which have shaped its advanced intelligence and security capabilities. He also pointed to Spain's growing leadership in cybersecurity, as recognized by international indices, and stressed the urgent need to adapt to new threats such as cyberattacks, hybrid warfare, and foreign interference in democratic processes, especially in light of the Russian invasion of Ukraine.

Finally, President Rollán called for stronger international cooperation to confront the transnational nature of modern threats. He advocated for increased investment in intelligence and defense, harmonization of legal frameworks, and enhanced communication and joint training between countries. Emphasizing that organized crime and cyber threats transcend borders, he urged nations to act collectively and decisively. He concluded by encouraging participants to see the forum as a platform to generate coordinated and transformative measures that safeguard democracy, human rights, and the international rules-based order.

Special remarks:

- **Hon. Ferdinand Martin G. Romualdez**, Speaker, Philippines House of Representatives

Speaker Ferdinand Martin G. Romualdez of the Philippine House of Representatives emphasized the importance of global collaboration in the face of unprecedented geopolitical, technological, and security challenges. He highlighted the critical role of forums like the PISF in fostering cooperation among parliamentarians and experts, reaffirming a shared commitment to international peace and stability. Speaker Romualdez also reflected on the success of the 28th PISF hosted earlier in Manila, which focused on the peaceful resolution of territorial disputes through international law, the resilience of global supply chains, and the regulation of emerging technologies.

Reaffirming the Philippines' unwavering dedication to these principles, Speaker Romualdez asserted the nation's commitment to upholding its rights in the West Philippine Sea, grounded in international law and the 2016 Arbitral Award. He strongly condemned attempts to undermine Philippine sovereignty through coercion or disinformation. Stressing the growing complexity of modern threats—including cyberattacks, hybrid warfare, and the misuse of artificial intelligence—he urged democratic nations to strengthen their legislative frameworks, enhance transparency, and unite in defense of the democratic rule of law.

Speaker Romualdez also highlighted the Philippines' leadership in promoting responsible AI development within the ASEAN region, referencing the recent resolution adopted at the 45th ASEAN Interparliamentary Assembly. He underscored the value of platforms like the PISF in extending such regional initiatives to the global stage, emphasizing the need for shared strategies, solidarity, and legislative cooperation. Concluding his remarks, he expressed deep gratitude to Senate President Pedro Rollán and Chairman Robert Pittenger for their leadership, calling on all participants to remain united in their pursuit of peace, security, and global cooperation.

- **Senator Francisco Javier Márquez**, Senate of Spain

Senator Francisco Javier Márquez of the Spanish Senate delivered a compelling address focused on the global challenges brought about by rapidly advancing technologies and their geopolitical consequences. He emphasized that we are living in a transformative era shaped by artificial intelligence, quantum computing, and widespread misinformation. These developments, he argued, demand not only reflection but coordinated international action to create legal and ethical frameworks capable of addressing new and complex realities.

He stressed the need for lawmakers to develop a clear and responsible understanding of technology—not to become engineers, but to recognize its societal and legal implications. Senator Márquez highlighted the growing gap between technological advancements and existing laws, urging for better alignment to safeguard individual rights and democratic values. He raised concerns about the ability of certain technologies to intrude on personal thought and privacy, calling for vigilance and foresight in how societies manage these tools.

In closing, the senator called for a spirit of international cooperation and shared responsibility, particularly in securing the necessary funding for global security. He underscored the importance of open, honest, and respectful debate in addressing transnational issues such as cybercrime, human trafficking, and economic exploitation. By embracing diverse perspectives and working collaboratively, he concluded, the forum can offer innovative and practical responses to the world's most urgent challenges.

- **Hon. Matt Pottinger**, Former Deputy National Security Advisor (video message)

Matt Pottinger outlined the global threats posed by the Chinese Communist Party (CCP), emphasizing

its role in undermining health, security, and liberty worldwide. Key points included:

- The CCP's coverup of the COVID-19 outbreak and its continued violations of international treaties.
- Economic disruption through state-sponsored intellectual property theft and predatory trade practices.
- Military threats, including support for authoritarian regimes and potential conflict over Taiwan.
- Efforts to export autocratic governance and influence global narratives through propaganda and technology.
- Pottinger called for unified global action to deter Beijing's aggression, defend democratic values, and protect international sovereignty.

Session 1: ARTIFICIAL INTELLIGENCE AFFECTING GLOBAL SECURITY

- **Mr. Matt Turpin**, Senior Counselor, Palantir

Mr. Matt Turpin, Senior Counselor at Palantir, opened his remarks by emphasizing the early stage of the artificial intelligence (AI) revolution. Drawing from his decades of government service and recent private sector work, he described AI as a still-immature industry poised to shape global society, democracy, security, and economics over the coming decades. Mr. Turpin highlighted key challenges and risks, including autonomous weapons, cyber warfare automation, proliferation disparities, synthetic biology, disinformation, ethical governance, inequality, and the potential impact on nuclear command and control systems.

He emphasized that while there is a great deal of discussion about artificial general intelligence or superintelligence, we remain in an era of artificial narrow intelligence (ANI). These current AI applications are focused on narrow, well-defined tasks that require human supervision and curated data. He cited examples like facial recognition, autopilots, and self-driving features, as well as generative models like large language models. Mr. Turpin cautioned that these tools are not self-aware and tend to underperform outside of their limited domains, especially when presented with low-quality data.

In terms of real-world applications, Mr. Turpin pointed to promising uses of AI in manufacturing, healthcare, energy, and national defense. In all these sectors, he stressed that AI's true value lies in human-machine teaming, not in full automation. He concluded by placing AI within the context of global competition, particularly between the U.S. and China, both of which are leveraging narrow AI capabilities to gain economic and security advantages. He noted that this dynamic is shaping strategies and technological development across the world and will likely continue for years to come.

- **Mr. Combiz Abdolrahimi**, Esq., Vice President, Global Head of Government Affairs, ServiceNow

In his remarks, Mr. Combiz Abdolrahimi, Vice President and Global Head of Government Affairs at ServiceNow, highlighted the profound and growing influence of artificial intelligence (AI) on democracy, security, and governance. Reflecting on his experiences, including his first forum in Guatemala, Mr. Abdolrahimi underscored the urgency of addressing how AI is being weaponized to distort information and interfere with democratic processes, especially elections. He emphasized that AI is not merely a technological advancement but a transformative force—capable of both empowering societies and threatening their foundational values.

Mr. Abdolrahimi presented a dual narrative: while malicious actors exploit AI for disinformation and destabilization, democratic governments can use the same tools to protect elections, modernize public services, and enhance cybersecurity. He cited examples such as the use of AI to detect influence campaigns, monitor threats to digital infrastructure, and streamline government operations. He also noted the global race to lead in AI development, with countries investing heavily in AI as a strategic asset, signaling not only technological ambitions but ideological commitments.

Calling for responsible AI governance, Mr. Abdolrahimi urged policymakers to embrace principles such as human-centered design, transparency, inclusivity, and accountability. However, he stressed that principles must be backed by concrete action—through governance frameworks, regulatory innovation, and global cooperation. He warned that AI can accelerate freedom or fragility depending on how it is managed, and concluded by calling on democratic leaders to ensure AI serves as a tool for strengthening trust, upholding human rights, and reinforcing democratic integrity worldwide.

- **Prof. Jamil Jaffer**, Founder and Executive Director of the National Security Institute at the Antonin Scalia Law School at George Mason University
Venture Partner at Paladin Capital Group

In his remarks, Prof. Jamil Jaffer, Founder and Executive Director of the National Security Institute, emphasized that artificial intelligence (AI) is rapidly becoming the central force in global economic growth and national security. Drawing from his background in both government and the private sector, Prof. Jaffer framed AI as a transformative technology—one that will not only drive intelligence gathering and defense capabilities but also enable economic advancement for nations willing to embrace its potential. He acknowledged real concerns such as discrimination, disinformation, and military misuse, but stressed that AI offers extraordinary opportunities for nations to accelerate economic development and global competitiveness, citing the rapid expansion of AI markets and investment worldwide.

Prof. Jaffer illustrated the scale and speed of AI growth through compelling statistics: from a \$93 billion market in 2020 to a projected \$826 billion by 2030. He noted that nearly half of the billion-dollar "unicorn" companies created in 2023 were AI companies. However, he warned that AI success depends on access to three critical resources: data, computing power, and energy. He highlighted a troubling disparity: while the U.S. and China dominate AI model development, only a small fraction of such innovation originates in Europe or other regions. He challenged lawmakers to view this as a wake-up call, urging them not to treat AI as merely a threat but as a generational opportunity to uplift their populations.

In closing, Prof. Jaffer cautioned against overregulation, suggesting that the European model of "regulate first, innovate second" has stifled economic growth. Instead, he proposed approaches like regulatory sandboxes, moratoriums on premature regulation, and strong incentives for AI innovation. He encouraged governments to create

environments conducive to private investment in secure and ethical AI, emphasizing that trusted technologies will see faster and more widespread adoption. Ultimately, he framed the AI revolution as a historic moment—one where national success will depend on swift, strategic, and values-based engagement with this transformative force.

Session 2: THE GEOPOLITICAL IMPACT OF CRYPTO AND DIGITAL CURRENCIES

- **Dr. Lisa Cameron**, Former Member of Parliament, United Kingdom

Dr. Lisa Cameron, former Member of Parliament of the United Kingdom, opened her remarks by expressing appreciation for the forum and sharing her unique journey into the digital currency space. As the first clinical psychologist elected to the UK Parliament, she initially had no background in technology. However, in 2021 she was asked to chair the UK's cross-party cryptocurrency working group, sparked in part by a constituent who had been a victim of a crypto scam. Discovering that there had been no prior parliamentary debate on digital assets, she recognized the urgent need for regulation and consumer protection, especially given the growing public engagement with cryptocurrencies despite Parliament's initial skepticism.

Dr. Cameron emphasized the importance of education and engagement for lawmakers in understanding digital currencies and blockchain technology. Under her leadership, Parliament released its first joint report from the House of Commons and House of Lords exploring the UK's potential as a digital hub. Her group facilitated meetings with stakeholders across compliance, innovation, and security sectors, both within and outside Parliament, to expose legislators to emerging technologies. She highlighted powerful use cases, such as Ukraine's deployment of digital assets during wartime to deliver aid directly and efficiently—an example that influenced UK thinking on how blockchain can improve transparency and impact in public finance.

Looking to the future, Dr. Cameron stressed the need for global collaboration in developing interoperable regulatory frameworks, especially as frontier technologies like AI, Web3, and quantum computing converge. Since leaving Parliament, she has continued her advocacy through the UK-US Crypto Alliance and a global forum of lawmakers focused on blockchain and digital currencies. She underscored that informed regulation must be rooted in best practices and shared learning, which requires international cooperation and ongoing education for policymakers. Her work now focuses on equipping legislators with the knowledge they need to guide responsible innovation.

- **Dr. Oonagh McDonald**, CBE - Former Member of Parliament, United Kingdom

Dr. Oonagh McDonald, CBE, focused her remarks on the challenges and risks posed by stablecoins, especially Tether, which dominates the market with over 60% share. She questioned the value of purchasing a dollar-pegged stablecoin in a country like the U.S., where direct access to dollars is already available. McDonald emphasized the importance of regulated, basic bank accounts and transparent payment systems as safer and more efficient alternatives for low-income individuals needing to send remittances. She argued that converting funds into stablecoins incurs unnecessary fees and that blockchain-based systems—often promoted for such transfers—are frequently slow, opaque, and congested.

McDonald raised serious concerns about Tether's lack of regulatory oversight and transparency. For years, the company operated without audited financial statements and was previously registered in the British Virgin Islands, a jurisdiction plagued by corruption. It has since relocated to El Salvador, a country whose attempt to adopt Bitcoin as legal tender recently failed. She noted the potential for stablecoins like Tether to be misused in illicit transactions, citing reports of their use in arms purchases by Russia. McDonald concluded by calling for strict enforcement of financial regulations—especially the FATF travel rule requiring identification of senders and receivers—to limit anonymity in crypto transactions and reduce the risks posed by unregulated digital currencies. Such developments are wide open to corrupt use, including money laundering, for which the users of cryptos are entirely responsible. Indeed, the anonymity of blockchains... the transactions are transparent, but the sender and the recipient of such funds remain anonymous through the use of their private keys. That is the point of cryptos.

- **Ms. Lilita Infante**, CEO, CAT Labs, Former DOJ Special Agent

In her speech, Ms. Lilita Infante, CEO of CAT Labs and former DOJ Special Agent, outlined the urgent threat posed by the misuse of cryptocurrencies by transnational criminal organizations, terrorist groups, and adversarial nation-states. Drawing on her decade of experience with the DEA, including leading the takedown of Hydra Market—the world's largest dark web marketplace—Ms. Infante described how cryptocurrencies have enabled criminals to move money globally at unprecedented speed and scale. This has left law enforcement and intelligence agencies struggling to keep pace. She emphasized that these technology-enabled threats demand equally agile responses and highlighted how criminals exploit the anonymity and lack of intermediaries in crypto to bypass traditional financial controls.

Ms. Infante proposed a practical and actionable solution: governments must adopt policies that mandate scanning all digital evidence for private keys and other cryptocurrency indicators as early as possible in the investigative process. She stressed that most seized data now contains potential access to significant criminal funds and that understanding how to extract and secure this data is critical. She said, the goal is to empower every agent and analyst—not just experts—to detect, trace, and seize illicit

digital assets. By turning data into actionable financial intelligence, law enforcement can both disrupt criminal networks and recover substantial assets, as Ms. Infante and her colleagues have repeatedly demonstrated.

- **Mr. Jean Diederich**, Board Member, VNX Stablecoins

In his address, Mr. Jean Diederich, Board Member of VNX Stablecoins, emphasized the urgent need for governments—particularly in Europe—to confront and properly regulate the evolving digital currency landscape. He explained the differences between three major types of digital currencies: unregulated cryptocurrencies like Bitcoin, government-backed central bank digital currencies (CBDCs), and stablecoins, which are pegged to fiat currencies and managed by private companies. Mr. Diederich criticized the European Union’s fragmented and hesitant regulatory response, especially under ESMA, which has created significant obstacles for legitimate companies trying to operate within a legal framework. He cited the example of Tether’s creation as a response to banks rejecting fiat from crypto exchanges and noted that while stablecoins are vital for financial stability in the crypto space, lack of regulatory clarity is stalling innovation and inadvertently empowering bad actors.

Mr. Diederich also highlighted stark contrasts between the European and U.S. approaches. While the U.S. has placed legal limits on CBDCs to protect privacy and financial freedom, Europe risks drifting toward an overly centralized model reminiscent of authoritarian systems. He warned against letting central banks dictate technological infrastructure, stressing that innovation must be driven by competition in the private sector. He urged European lawmakers to follow through on the promises of the MiCAR regulation by issuing licenses and enabling compliant firms to operate. Concluding with a call to action, Mr. Diederich appealed for a collaborative, balanced approach—one that doesn’t build walls between central banks and crypto, but rather builds bridges to ensure both innovation and consumer protection thrive together.

Session 3: ILLICIT FINANCE & FOREIGN INVESTMENTS: NAVIGATING THREATS IN A GLOBALIZED ECONOMY

- **Mr. Alejo Campos**, Regional Director, Crime Stoppers, Americas and Caribbean

Mr. Alejo Campos, Regional Director for Crime Stoppers in the Americas and Caribbean, delivered a compelling presentation on the growing complexity of illicit economies and the urgent need to confront the evolving dynamics of transnational organized crime. He explained that illicit economies today are sustained by a convergence of criminal organizations, kleptocratic governance, and systemic social failures such as inequality, poverty, and lack of education. These networks are no longer limited by national borders; instead, they operate globally, forming sophisticated criminal corporations that control routes of trafficking—whether of drugs, counterfeit goods, or human beings—rather

than just the products themselves. Mr. Campos emphasized that this convergence has created a portfolio of criminal services, where parallel crimes such as human trafficking, illegal mining, forgery, and counterfeit trade often generate as much or more revenue than traditional drug trafficking, especially in non-drug transit countries.

He further illustrated how global criminal operations are exploiting weak legal frameworks and loopholes in international trade systems to move illicit products and launder money. With detailed examples from Latin America, Europe, and Asia, Mr. Campos exposed how criminal groups collaborate across continents, often leveraging legitimate logistics hubs and financial systems to sustain illegal activities. He highlighted cases where organized crime used counterfeit cigarettes and forged goods to fund operations, and emphasized the devastating human cost of trafficking, particularly of women and girls. Concluding his remarks, Mr. Campos called for renewed political will, updated and harmonized transnational legislation, and improved international cooperation and intelligence sharing. Without these efforts, he warned, the global illicit economy will continue to outpace law enforcement and institutional responses.

Session 4: 5G, QUANTUM COMPUTING AND NEUROTECHNOLOGY: INNOVATIONS, RISKS AND GLOBAL IMPLICATIONS

- **Hon. John Strand**, CEO of Strand Consult

In his remarks, Hon. John Strand, CEO of Strand Consult, highlighted the growing threats to digital infrastructure and national security stemming from dependence on untrusted technology vendors, particularly from China. He underscored how modern societies are becoming deeply interconnected—from energy systems and electric vehicles to telecommunications—making them vulnerable to exploitation through embedded hardware and software. Mr. Strand presented new research revealing that Chinese-manufactured solar panels and electric vehicles may transmit sensitive data to mainland China, raising serious concerns about privacy and control. He warned against the integration of unverified foreign technology, especially within critical infrastructure, noting that seemingly benign tools like AI applications or vehicle systems can serve as gateways for mass data collection. He referred to Chinese electric vehicles as “spies on wheels” and criticized the lax enforcement of EU-wide cybersecurity measures, such as the 5G Toolbox, noting that only a fraction of member states have fully implemented agreed safeguards.

Mr. Strand also turned his attention to the geopolitical implications of Europe's energy and technology dependencies. He condemned the EU's contradictory behavior of purchasing vast amounts of Russian energy while failing to provide adequate military support to Ukraine. Citing Denmark as a model, he lamented that some of Europe's largest economies—France, Spain, and Italy—have contributed less in military aid than smaller countries like Denmark. He was particularly critical of European hypocrisy, naming specific examples such as the French satellite company Eutelsat, which continued to broadcast Russian propaganda despite EU sanctions. Mr. Strand stressed the

importance of transparency, accountability, and unity in the face of rising digital threats and authoritarian influence, calling on European nations to match their rhetoric with action, particularly in defending Ukraine and securing their digital infrastructure from hostile foreign control.

- **Mr. Mikel Díez Parra**, Quantum Global Sales Enablement Lead in IBM

Mr. Mikel Díez Parra, Quantum Global Sales Enablement Lead at IBM, addressed the growing risks posed by quantum computing to global security and cryptography systems during his speech at the Intelligence and Security Forum. He began by providing a high-level introduction to quantum computing, emphasizing its foundation in subatomic physics and its increasing computational power compared to classical computing. He highlighted IBM's dual objective: making quantum computing practically useful while ensuring that its development does not jeopardize digital safety. A major concern he outlined is the vulnerability of current cryptographic systems, which underpin virtually all aspects of the digital economy—from banking apps to digital certificates—to future quantum decryption capabilities. As critical infrastructure systems often have very long update cycles, he warned that quantum threats cannot be addressed overnight and that preparedness must begin now.

Mr. Díez Parra elaborated on how quantum computing could eventually break today's encryption standards, referencing theoretical algorithms like Shor's, which could dismantle public-key cryptography once enough quantum processing power is available. He raised the alarm that malicious actors might already be collecting encrypted data, intending to decrypt it in the future once quantum capacity allows. In response, IBM and global institutions like NIST have been developing quantum-resistant algorithms, with IBM contributing three of the first such standards. He concluded by advocating for coordinated, cross-sector and international action, particularly through regulatory efforts like the NIS2 directive in Europe. The key takeaway: the quantum era is approaching rapidly, and nations, industries, and organizations must urgently begin modernizing cryptographic protections in a unified and forward-thinking manner.

Session 5: CYBERSECURITY

- **Senator José Antonio Monago Terraza**, Senate of Spain

Senator José Antonio Monago Terraza delivered a compelling speech highlighting the evolving nature of national security threats, particularly those emerging from cyberspace. He underscored that modern warfare no longer relies solely on traditional arms but instead operates subtly through hybrid tactics—cyberattacks, disinformation campaigns, and infrastructure sabotage—that destabilize democracies without a formal declaration of war. He warned that sovereignty today is undermined not by bullets but by attacks that can paralyze hospitals, manipulate elections, or disrupt emergency networks. The Senator stressed that cybersecurity is not merely a technical issue but a cornerstone of

state policy, vital for protecting public trust, critical services, and democratic institutions. Drawing from Spain's 2024 national security report, he confirmed that cyber threats—from espionage to digital influence operations—are increasing, often orchestrated by hostile state actors like China, Russia, Iran, and North Korea.

Senator Monago emphasized the urgent need to develop doctrinal intelligence for cyberspace, treating it as a strategic defense domain alongside land, sea, and air. He warned of emerging risks from artificial intelligence and quantum computing, both of which could either fortify or devastate cybersecurity systems depending on their use. In response, Spain has established a parliamentary investigation committee to study these technologies and recommend protective measures. He called for systemic resilience based on European strategic frameworks and advocated for stronger legislation, enhanced public-private cooperation, and sustained investment in cybersecurity. Stressing that national security now lies in code and cloud infrastructure, he concluded by reaffirming Spain's commitment within the Euro-Atlantic digital security alliance and urged all democratic institutions to act decisively before the invisible war escalates further.

- **Senator Olivier Cadic**, Member of the French Senate

Senator Olivier Cadic delivered a sobering and urgent speech highlighting the increasing severity and complexity of cyber and information warfare targeting democracies. He shared his personal experience as one of 116 parliamentarians from 15 countries targeted by the cyber espionage campaign "APT31," specifically due to his involvement in the Inter-Parliamentary Alliance on China (IPAC). Emphasizing that these were acts of hybrid warfare from authoritarian regimes, he praised the FBI and U.S. Department of Justice for their support. As chair of the French Senate's special committee on critical infrastructure resilience, Senator Cadic discussed the recent legislative efforts in France to implement key EU cybersecurity directives— REC, NIS2 and DORA —and underlined the importance of raising digital awareness and building rapid cyber response capabilities. He also recounted the establishment of France's VIGINUM agency, which has exposed multiple disinformation campaigns targeting European democracies, primarily orchestrated by Russia and amplified through sophisticated networks like Portal Combat, "Mriya", and Storm-1516.

Cadic further detailed recent information operations, including attempts to manipulate elections in Romania and Taiwan, and aggressive disinformation campaigns in Africa involving Russia's Wagner Group. He warned of the economic and reputational risks associated with digital information warfare, citing the DeepSeek R1 incident that briefly disrupted global markets. Drawing comparisons between Russia as a storm and China as climate change, he stressed the need for democracies to shift from a reactive posture to a proactive one. Senator Cadic called for the creation of a cyber deterrence force and stronger public-private collaboration, likening the necessary transparency and cooperation to that seen in nuclear defense. He concluded with a call for unity among democracies, noting that no system is invulnerable, but resilience and strategic initiative can prevail.

- **Dr. Paul J. Maurer**, President of Montreat College

Dr. Paul J. Maurer, President of Montreat College, delivered a compelling speech framing cybersecurity not merely as a technical challenge, but as a deeply human and ethical one. He emphasized that while the tools of cyber warfare evolve rapidly, the solution lies in cultivating trustworthy, ethical professionals who make sound decisions under pressure. In partnership with the U.S. National Security Agency (NSA), Montreat College developed a curriculum and a book titled *The Code of Honor: Embracing Ethics and Cybersecurity*, now available to the nearly 500 NSA-designated Centers of Academic Excellence. This initiative aims to instill a standardized ethical framework for current and future cyber professionals, comparable in importance to the Hippocratic Oath in medicine or the Geneva Conventions in warfare.

Dr. Maurer introduced the Code as an oath that students and professionals voluntarily adopt, committing to principles like honesty, collaboration, self-control, and respect for privacy. He argued that these values are essential in high-stakes situations such as ransomware attacks, where decisions must be made quickly, often in ethical gray zones. The code offers structured guidance for such scenarios, helping leaders respond with integrity rather than instinct. In conclusion, Dr. Maurer called on international leaders to incorporate ethics education into their cybersecurity training programs, offering Montreat's model and resources as a global tool in the "forever war" against cybercrime.

- **Dr. Varun Suthra**, Director International Relations, KIIT University

Dr. Varun Suthra opened his speech by emphasizing the Indian philosophy of "Vasudhaiva Kutumbakam"—"the world is one family"—as a guiding principle for international cooperation and trust. He praised Congressman Pittenger for creating a platform that fosters this spirit of global dialogue and unity. Reflecting on recent conflict near India's northern border, Dr. Suthra described his personal experience during hybrid warfare, highlighting how conventional attacks were paralleled by cyberattacks and misinformation campaigns. He underscored the unprecedented threat posed by social media and false narratives, stressing the need for trustworthy information and strategic communication.

To address these challenges, Dr. Suthra proposed integrating ancient Indian strategic wisdom with modern defense mechanisms. Drawing from the 2,300-year-old text Kautilya's *Arthashastra*, he outlined key doctrines such as protection of national assets, psychological resilience, espionage, and counter-propaganda—concepts that remain strikingly relevant today. He translated these principles into modern terms like cyber laws, digital firewalls, internal security checks, and public education. Dr. Suthra concluded by urging policymakers to blend historical strategic insight with contemporary digital defenses, stating that while the battlefield may have shifted from terrain to technology, the foundational wisdom for protection remains timeless.

Session 6: CHINA INFLUENCE THROUGHOUT THE AMERICAS

- **Hon. Mariano Federici**, Senior Managing Director, K2 Integrity, former President of FIU-Argentina and Chairman of Egmont Group.

Hon. Mariano Federici emphasized the critical and growing influence of China's authoritarian expansion across Latin America and the Caribbean, highlighting it as a multifaceted and strategic challenge rather than a mere commercial engagement. He explained how China has become a dominant economic, technological, and financial force in the region through investments in infrastructure like ports, satellite stations, and digital networks, often under opaque terms that prioritize long-term geopolitical control over short-term gains. Federici warned that Chinese capital and technology embed dual-use capabilities, including surveillance and control over vital maritime logistics, digital ecosystems, and financial systems, thereby threatening regional sovereignty, transparency, and democratic institutions.

Federici underscored the urgent need for coordinated responses from all democracies to counterbalance this influence with transparency, accountability, and alternative investment. He also highlighted China's role in facilitating transnational organized crime through illicit finance linked to drug cartels, deepening institutional corruption and violence. The speech called for safeguarding democratic values and rule of law by supporting transparent partnerships, developing secure infrastructure, and investing strategically in resilient governance. Ultimately, Federici framed the Americas as a frontline in a global contest for democratic resilience, where the future hinges not only on military might but on control over ports, digital platforms, and financial systems.

Session 7: STOPPING TRAFFICKING IN BUSINESSES AND SUPPLY CHAINS

- **Ms. Anne Basham**, Chief Executive Officer at Interparliamentary Taskforce on Human Trafficking

Ms. Anne Basham highlighted the critical importance of human trafficking as not only a human rights issue but a significant global security concern that affects every nation, particularly free democracies. She emphasized that combating trafficking requires awareness and involvement beyond law enforcement—every citizen and business can play a role in identifying and preventing exploitation. Using a real-life example of an informed bystander who recognized trafficking signs at an airport, Basham illustrated how awareness can lead to rescue and encouraged widespread training to increase victim identification, noting that only about 0.4% of trafficking victims are currently identified worldwide. She stressed that human trafficking is fundamentally a corrupt financial business model, making businesses uniquely positioned to disrupt it.

Basham then presented a practical solution—the [Global Businesses Against Trafficking \(GBAT\) program](#)—which empowers businesses to recognize and report trafficking

indicators within their environments. The program offers training and a scalable model for nations worldwide to adopt, mobilizing businesses as crucial allies in the fight against trafficking. She encouraged lawmakers and attendees to engage with the initiative and expressed gratitude to Congressman Pittenger and others for their leadership in prioritizing anti-trafficking efforts.

- **Senator Linda Reynolds CSC, Australia**

Senator Linda Reynolds emphasized the critical connection between human trafficking and national security, particularly highlighting China's role in exploiting modern slavery for strategic and economic gain. Drawing on her experience as Australia's defense minister, she described how China, alongside Russia, Iran, and North Korea, forms an authoritarian axis united against democracy, employing hybrid warfare tactics that include exploiting enslaved labor in global supply chains. She outlined how forced labor is embedded in the production of critical minerals and renewable energy components—such as cobalt from Congo, polysilicon from China, and nickel from Indonesia—used worldwide, including in “green” technologies. Reynolds criticized the global complacency toward these abuses, warning that prioritizing environmental goals without addressing human rights creates a dangerous ethical blind spot that China exploits for market dominance and as a weapon against democratic nations.

Reynolds called for a stronger collective response, urging lawmakers and citizens to openly confront and expose human trafficking and modern slavery within supply chains. She highlighted Australia's modern slavery legislation as a starting point but acknowledged that compliance often amounts to minimal, box-ticking efforts rather than meaningful action. To make real progress, she stressed the importance of mobilizing public awareness and listening to the voices of survivors to generate political will for reform. Reynolds concluded by stressing the need for global partnerships and citizen engagement to confront this multifaceted threat, framing the fight against trafficking as both a moral imperative and a critical national security priority.

- **Ms. Jane Lasonder, OSCE ISTAC (International Survivors of Trafficking Advisory Council)**

Ms. Jane Lasonder shared her powerful personal journey from being a victim of child sexual exploitation and trafficking to becoming a vocal survivor advocate. She described the harrowing experiences of abuse, invisibility, and betrayal she faced as a child trafficked by a gang that included trusted figures like a policeman and a doctor. Despite suffering severe injuries and numerous chances to seek help—such as during hospital visits—her cries for rescue went unnoticed due to lack of awareness among healthcare workers and educators. Jane highlighted the urgent need for specialized training for medical professionals to recognize signs of trafficking and exploitation, sharing a poignant example of a man trapped in forced labor whose suffering was ignored by hospital staff for years.

Jane's message emphasized the power each person holds to make the invisible visible and to drive change. She urged governments and organizations to meaningfully include

survivors in policy design and advocacy, rather than tokenizing them, and recommended establishing national survivor councils as bridges between affected individuals and lawmakers. Ending with a vivid story about a public rescue of a pigeon, she challenged listeners to prioritize rescuing trafficked people with the same urgency and attention. Jane's speech was a call to action to recognize the humanity of trafficking victims and mobilize collective efforts to bring them out of the shadows and into safety and dignity.

MAY 23rd

Session 8: TRANSNATIONAL THREATS & BORDER INSECURITY

- **Hon. Mariano Federici**, Senior Managing Director, K2 Integrity, former President of FIU-Argentina and Chairman of Egmont Group.

Hon. Mariano Federici discussed the recent U.S. designation of major Mexican cartels, such as the Sinaloa and Jalisco cartels, as Foreign Terrorist Organizations (FTOs). This move marks a significant shift in how organized crime is addressed, placing these cartels in the same legal category as groups like ISIS and Hezbollah. As FTOs, any form of material support—including financial transactions, logistics, or even unintentional business engagement—can now be prosecuted under U.S. counterterrorism laws, with severe consequences such as asset freezes, sanctions, and criminal liability.

He emphasized that these cartels are not just drug traffickers but insurgent groups with territorial control, military capabilities, and deep institutional penetration. Their influence extends into sectors like human trafficking, illegal mining, extortion, cybercrime, and control over supply chains. A key enabler, according to Federici, is the role of Chinese networks—particularly chemical suppliers and underground banking systems—which facilitate both fentanyl production and money laundering, creating a convergence between Mexican violence and Chinese financial opacity.

Federici warned that financial institutions, especially in Mexico and Europe, are dangerously unprepared to manage the risks this designation implies. Many lack proper intelligence, due diligence, or risk-mapping systems. He called for urgent action, including the creation of financial intelligence units, public-private partnerships, and real-time information-sharing platforms. The FTO designation has already altered the global legal and financial landscape and failing to respond promptly and collectively could jeopardize financial stability, border security, and democratic institutions worldwide.

- **Prof. Jose Sanmartin**, University of Alicante

Professor José Sanmartín described disinformation as a global war that aims to destabilize societies by spreading hatred, delegitimizing institutions, and promoting radicalism. It operates by creating scapegoats— “black beasts”—to channel public outrage, and by infiltrating decision-making spaces through media, politics, and culture. He emphasized that disinformation is not just a political or cultural issue, but a form of organized criminal activity driven by economic interests and power struggles.

He stressed that the key to combating disinformation lies in attacking its economic foundations. This means identifying and dismantling the financial networks that sustain these toxic operations. According to Sanmartín, defensive measures are insufficient states must go on the offensive by targeting the sources of illicit funding, disrupting networks, and severely penalizing those involved. He also warned that disinformation is often supported or tolerated by political actors, making a unified state-level and international agreement essential.

Finally, he called for greater investment in intelligence services, both in resources and professionalization, to effectively track and respond to disinformation. Sanmartín highlighted the urgency of creating strong, well-funded, and independent intelligence agencies capable of detecting economic and ideological threats. He concluded by urging governments to “follow the money,” as financial disruption is the most effective way to stop the spread and power of disinformation networks.

- **Hon. Victor Gonzalez**, Former Member of Parliament, Spain

Hon. Víctor González focused his intervention on the growing strategic alliance between Cuba and Russia in the context of the war in Ukraine. He highlighted how Cuba, traditionally aligned with Moscow, has intensified its collaboration through high-level visits, military cooperation, and media support. Cuban state media has become a key amplifier of Russian disinformation in Latin America, echoing Kremlin narratives while abstaining or voting against U.N. resolutions condemning the invasion of Ukraine.

The most alarming aspect, he stressed, is the reported recruitment of thousands of young Cubans to fight alongside Russian forces in Ukraine. Many of these recruits are misled with promises of payment, like Cuba’s past export of doctors under state-controlled programs. González warned that once these combatants return to Cuba or other Latin American countries, they could become agents of instability—militarized, traumatized, and vulnerable to recruitment by organized crime or insurgent groups, posing a transnational threat.

He concluded by criticizing the European Union for maintaining cooperation agreements and financial support for Cuba while the regime collaborates with Russia. With billions in unpaid Cuban debt and ongoing repression, González argued that continuing to fund the Cuban state indirectly supports Russian aggression. He called for a firm and unified Western response, including suspending EU-Cuba agreements and closely monitoring returning fighters, warning that ignoring the threat could have severe consequences for regional and global security.

Session 9: IS PRESIDENT PUTIN TO BE BELIEVED?

- **Sir Liam Fox**, Former Minister of Defense in the United Kingdom

Sir Liam Fox emphasized that Russia's invasion of Ukraine is Europe's greatest security threat and highlighted the failure of past Western deterrence. He criticized Western leaders for underestimating Vladimir Putin, pointing to weak responses to Russia's actions in Georgia (2008) and Crimea (2014), which emboldened further aggression. He described Putin as a war criminal, a liar, and a tyrant who cannot be trusted, warning that any ceasefire would only be seen by Putin as a temporary pause.

Sir Fox stressed the need for sustained, smarter sanctions targeting Russia's economic vulnerabilities, especially its dependence on high-tech imports and capital. He argued that sanctions must now aim to trigger capital outflows and limit Russia's war-making capabilities long-term. He also proposed using frozen Russian overseas assets—particularly the \$300 billion held in Europe—not just for interest, but to fund Ukraine's recovery and defense, especially if U.S. support declines.

Sir Fox urged unity and resolve in the free world, warning that ignoring international law and failing to act would embolden tyrants like Putin. He called for moral clarity: freedom must be defended, aggression must be punished, and the West must act decisively—because history is watching.

Session 10: ENERGY SECURITY & CRITICAL MINERALS

- **Ms. Diana Furchtgott-Roth**, Director, Center for Energy, Climate, and Environment, The Heritage Foundation

Ms. Diana Furchtgott-Roth delivered a pointed critique of net-zero climate policies, arguing they offer minimal environmental benefits while significantly weakening Western economies. She stressed that affordable and reliable energy is essential for national security and economic resilience, yet Western nations are overspending on renewables that fail to reduce global emissions. This, she warned, diverts critical resources away from defense, policing, and support for Ukraine.

She highlighted that China, the dominant producer of wind, solar, and battery technology, continues to expand its coal use—undermining Western climate efforts. Meanwhile, Europe and the U.S. are losing energy-intensive industries due to high electricity costs, effectively offshoring emissions to more polluting economies. In her view, this global imbalance worsens both energy security and climate outcomes.

Furchtgott-Roth advocated for a pragmatic energy strategy that includes nuclear power, natural gas, and cleaner coal. She cited Spain's Vora gas field as an example of how domestic energy development can align with environmental goals while boosting energy independence. Concluding her remarks, she called on Western leaders to reconsider the net-zero agenda, arguing that real security and economic strength require energy policies rooted in realism, not ideology.

- **Mr. J.C. Boggs**, Partner, King & Spalding

Mr. J.C. Boggs emphasized two key reasons why the U.S. should care: human rights and national security. Boggs outlined China's strategic dominance in the global critical minerals supply chain, controlling most refining and processing despite limited raw material production. This control poses a national security risk, especially if geopolitical tensions escalate. He cited examples of China weaponizing trade, manipulating prices, and using state-backed investments to dominate refining in countries like Indonesia.

He urged the U.S. to respond with aggressive strategies, including executive orders to boost domestic mining, partnerships with allies like Canada, the UK, and Australia, and investment in cleaner mineral processing technologies.

He warned of the inadequate U.S. talent pipeline in mining and stressed the need for securing every stage of the supply chain in collaboration with trusted allies.

- **Mr. Francois Baird**, Distinguished Fellow, Energy Policy Research Foundation, Inc. (EPRINC)

Mr. François Baird emphasized that energy access lies at the heart of Africa's poverty and underdevelopment. Speaking passionately about the continent's challenges, he argued that nearly everything in modern life, whether infrastructure, industry, or daily needs, starts with mining and energy. Yet, 600 million Africans still lack basic electricity, with the average African (excluding South Africa) receiving only enough power to run a fridge for six and a half hours a day.

Baird highlighted that state fragility, hunger, unemployment, and poor health in Africa are directly tied to energy poverty. Despite over \$100 billion invested in renewable energy for Africa over two decades, the results have been dismal due to unrealistic expectations and burdensome debt. He criticized the global push for Africa to rely solely on renewables, while wealthier nations continue to use fossil fuels and build coal plants, especially in countries like China.

He called for Africa to be allowed to develop its own natural gas and other affordable energy sources, arguing that economic prosperity, peace, and industrialization are impossible without reliable base load power. He advocated for private sector investment in African energy infrastructure, asserting that state-led and donor-driven approaches have failed. Baird concluded with a powerful message: to prevent migration crises and foster true development, the West must stop imposing double standards and let Africa power itself to prosperity.

Session 11: EUROPE BEFORE THE CHALLENGE OF ARTIFICIAL INTELLIGENCE

- **Mr. Miguel Ángel López-Valverde**, Councilor for Digitalization of the Community of Madrid

Mr. Miguel Ángel López-Valverde emphasized the vital role of public institutions in leading the ethical and responsible adoption of artificial intelligence (AI). He argued that AI development should not be confined to tech labs or corporations but must involve the

public sector, which is uniquely positioned to ensure transparency, equity, and democratic values.

He outlined Madrid's strategic priorities in using AI: improving public services, strengthening citizens' trust, and contributing to Europe's technological leadership. Concrete examples from Madrid include AI applications in healthcare (e.g., optimizing surgery waitlists, early lung cancer detection), education (e.g., dropout prevention), and citizen services. The region has implemented over 149 AI initiatives, 89% of them in the health sector.

López-Valverde highlighted the importance of transparency, algorithmic audits, and alignment with European ethical guidelines to maintain public trust. He also underscored the region's efforts to promote digital skills, especially among youth, through training initiatives.

He positioned Madrid as a proactive actor in shaping a European AI model that is inclusive, regulated, and people-centered, calling for continued collaboration, innovation, and responsibility from public institutions.

- **Ms. Isabel González Hervás**, Security and Defense partner at EY

Ms. Isabel González Hervás stressed that Europe is no longer anticipating the future of AI—it is already living it. She emphasized that the nature of modern conflict has shifted: battlefields are now digital, algorithmic, and increasingly autonomous, making artificial intelligence a matter of strategic sovereignty, not just technological or economic advancement.

From a European perspective, she identified critical vulnerabilities: overregulation, underinvestment, fragmented industrial efforts, and lack of private capital and entrepreneurial culture. Europe has lagged behind in foundational AI model development, with only three models developed in the region last year compared to dozens in the U.S. and China.

However, she acknowledged positive momentum. Europe's recent AI Action Plan, launched in April, lays out five key pillars: computing infrastructure, data access, adoption, talent development, and smarter regulation. González Hervás argued these areas are essential to transition from being AI bystanders to active global shapers.

She also highlighted Europe's existing strengths: expertise in key industries (such as aerospace, health, and green tech), robust ethical and democratic values, and credibility as a global regulatory leader. These assets, she suggested, must be leveraged to build meaningful, human-aligned AI systems.

To close, she offered four calls to action: invest more aggressively, integrate AI into strategic industrial sectors, empower and retain talent, and enhance collaboration among EU member states to build strategic autonomy and safeguard democratic values.

Special remarks:

- **Congressman Darrell Issa**, House of Representatives U.S. (video message)

Congressman Darrell Issa, acknowledging the global challenges post–Cold War, he emphasized that the current era also presents significant opportunities for renewed cooperation among free nations.

He defended the U.S. administration's foreign policy posture, rejecting claims of isolationism and framing it instead as a strategy of “peace through strength.” Congressman Issa pointed to efforts to reassert American leadership globally—from promoting peace with honor in Ukraine and countering Iranian influence in the Middle East to deterring the Chinese Communist Party's expansion.

On artificial intelligence, he cautioned against overregulation, contrasting the U.S. approach—focused on innovation and individual liberty—with what he characterized as Europe’s more restrictive stance under the AI Act. He warned that ceding AI leadership to authoritarian regimes like China would undermine democratic values. Instead, Issa called for a vision of AI rooted in open markets, freedom, and prosperity.

Closing on an optimistic note, he reaffirmed America's role as a trusted ally and partner in building a more secure and prosperous future for coming generations.

Session 12: SPACE FORCE

- **Hon. Oleg Dunda**, Member of Parliament, Ukraine

Hon. Oleg Dunda described how traditional military assets like tanks and aircraft carriers are increasingly outdated, likening them to “dreadnoughts” of a bygone era. Instead, Ukraine's advantage in the Black Sea—achieved through U.S. satellite support and systems like Starlink—demonstrates the strategic edge provided by advanced space capabilities. In contrast, Russia’s space infrastructure is obsolete and insufficient, limiting its effectiveness on the battlefield.

Hon. Dunda urged nations to restructure defense budgets to prioritize space technologies over traditional heavy weaponry. He predicted a global shift where geopolitical influence will depend more on space capabilities than on nuclear arsenals. Without investment in space forces, countries risk becoming dependent on the orbital dominance of powers like the U.S. or China.

Session 13: HUMAN TRAFFICKING AND ITS ROLE IN SPONSORING TERRORISM

- **Dame Karen Bradley DBE MP**, Member of Parliament, Chair of the Home Affairs Committee, United Kingdom

Dame Karen Bradley addressed the intersection of human trafficking and terrorism, challenging traditional thinking by asserting that trafficking is not just a humanitarian or immigration issue—it is a profitable criminal enterprise that often funds terrorism. She cited cases like the Russian trafficking of Ukrainian children, Boko Haram’s abduction of

girls, and state-sponsored migrant manipulation at borders as examples of how trafficking can be both a tool and a funding source for terror.

Hon. Bradley emphasized the importance of a victim-centered approach and called for breaking down silos between agencies addressing trafficking, terrorism, and immigration. Using the UK's "Four Ps" strategy—Pursue, Prevent, Protect, prepare—she stressed the need for law enforcement to connect the dots between organized crime and terrorism more effectively.

A major focus of her remarks was the financial dimension of trafficking. She advocated for public-private partnerships to track and cut off financial flows that enable trafficking, drawing parallels with efforts to eliminate illegal content on platforms like Pornhub by targeting their payment systems. Bradley called for financial institutions to be proactive in identifying transactions that may be linked to human exploitation, arguing that chasing the money is one of the most powerful ways to disrupt both trafficking networks and the terrorism they may fund.

- **Hon. Cristian Bacanu**, Former Member of Parliament, Romania

Hon. Cristian Bacanu emphasized that human trafficking is the second most profitable criminal enterprise globally, generating an estimated \$236 billion annually, and that unlike drug trafficking, it is far harder to prosecute due to the trauma and vulnerability of victims. He outlined how trafficking is interwoven with other major crimes—espionage, corruption, terrorism—and cited examples like ISIS and Boko Haram, who have used trafficking to support terror operations.

A central concern was how to make the fight against human trafficking more appealing to policymakers. Hon. Bacanu stressed the need to build strong, resilient communities of lawmakers and stakeholders committed to action, even in the face of bureaucracy. He advocated for the creation of transnational parliamentary task forces and friendship groups dedicated to combating trafficking, to promote collaboration and the exchange of best practices.

Importantly, Hon. Bacanu called for independent monitoring bodies, differentiated policies for source, transit, and destination countries, and the creation of a "political hammer" to pressure non-compliant actors. He also highlighted the growing challenge of online child exploitation, particularly in Southeast Asia, and urged lawmakers worldwide to unite in pressuring big tech companies to adopt technologies that could help automatically detect and block abusive content.

Session 14: RELIGIOUS FREEDOM, HUMAN RIGHTS AND FREEDOM OF CONSCIENCE CHALLENGES UNDER REPRESSIVE RULE

- **Dr. Bob Fu**, Founder and President, China Aid

Dr. Bob Fu delivered a passionate address highlighting the deep connections between religious persecution in China and the broader global crisis of human trafficking and authoritarian control. Having personally survived arrest and exile for his underground Christian work in China, Dr. Fu described how the Chinese Communist Party (CCP) represents a grave existential threat to freedom, not just within China but worldwide.

He drew attention to the CCP's systemic persecution of religious communities, including Christians, Muslims (notably the Uyghurs), and other faith groups. He described the CCP's three-pronged campaign launched under Xi Jinping—a war against the cross, the Bible, and Christian leaders. This includes demolishing thousands of churches, banning children from attending worship services, and imprisoning or disappearing prominent pastors and lawyers.

Dr. Fu pointed out that in some state-sanctioned churches, images of Xi Jinping and Mao Zedong are placed above altars, demonstrating the Party's goal of not just controlling citizens' bodies, but also their minds and spirits.

He warned that China's use of modern-day concentration camps, forced re-education, and digital surveillance represents the CCP's strategy of spiritual and ideological domination, with disturbing parallels to global trafficking practices. The repression, he said, often involves child arrests, forced disappearances, and state-controlled religious indoctrination—methods eerily similar to trafficking tactics.

Dr. Fu challenged legislators and civil society to speak out boldly and publicly advocate for the persecuted, sharing examples where international attention helped secure the release of detained Christians and children. He urged believers to engage in prayer as spiritual warfare, but also to leverage their voices and platforms—even a single tweet—to pressure the CCP, which he emphasized is always watching and listening.

