THE HONORABLE ROBERT M. PITTENGER
Chairman

FOR MORE INFORMATION:
(202)225-1976

CONGRESSIONAL TASKFORCE ON TERRORISM AND UNCONVENTIONAL WARFARE

8th Parliamentary Intelligence Security Forum

Riga, Latvia
June 19, 2017

Congress of the United States

Washington, DC 20515

Dear Colleague:

Thank you for your continued interest in our Parliamentary Intelligence Security Forums. This past June, we recently hosted our 8th forum in Riga, Latvia. Over the past several years, these forums have reached over 60 countries and over 650 Members of Parliament.

The Latvian Parliament co-hosted our event, and we extend our sincerest thank you for their hard work and dedication. Because of their input, our June forum in Riga provided an exceptional opportunity for collaboration among international government leaders.

During the event, participants discussed a variety of international security topics, including terrorist group financing, combatting Russian and Chinese counterintelligence, information sharing, and developing a successful cybersecurity defense strategy. Panelists at this event included several American and European security experts, financial institution representatives, and senior federal government enforcement officials.

We were fortunate to have 28 countries attend our event in Riga. Enclosed you will find an official forum agenda, a list of panelists, a list of foreign participants, and an official summary of events.

Thank you for your continued interest in our forum, and we look forward to working with you in the future.

Sincerely,

Robert

Robert Pittenger
Member of Congress
Chairman, Congressional Taskforce on Terrorism
And Unconventional Warfare

8th Parliamentary Intelligence Security Forum

19 June 2017
Baltic Hall

Parliament of the Republic of Latvia
Jēkaba Street 6/8, Riga

8:30 **CHECK-IN**

9:00 **WELCOME**

SPEECHES

H.E. Ms Ināra Mūrniece, Speaker of the Parliament of the Republic of Latvia

H.E. Ms Nancy Bikoff Pettit, Ambassador of the United States of America to the Republic of Latvia

Congressman Pittenger with Latvian Parliament Co-hosts, Ms. Solvita Āboltiņa and Mr. Ainars Latkovskis

Mr Paweł Chorąży, Undersecretary of State at the Ministry of Economic Development of the Republic of Poland

Ms Solvita Āboltiņa, Chair, Saeima National Security Committee

Mr Robert Pittenger, Member of Congress, Chairman of the Congressional Taskforce on Terrorism and Unconventional Warfare

PANEL I

9:30 – 10:30

Mr Mark Hanson, Director, Cyber and Emerging Technologies Section, Financial Crimes Enforcement Network, U.S. Department of the Treasury

Mr Michael Shanahan, Assistant Legal Attaché, U.S. Embassy Tallinn

Mr Bryan Carroll, Foreign Service Officer, U.S. Embassy Riga

PANEL II

10:30 – 11:45 **BANK AND FINANCIAL SECURITY**

Mr Frederick Reynolds, Global Head of Financial Crimes, Barclays

Mr William Fox, Managing Director, Global Financial Crimes Compliance, Bank of America

Mr Charles Bretz, Director of Payment Risk, Financial Services Information and Analysis Center

11:45 – 12:50 **LUNCH**

Hosted by **Mr Ainars Latkovskis**, Chairman of the Defense, Internal Affairs and Corruption Prevention Committee of the Saeima

Guest Room and White Room, Jēkaba Street 11

12:50 **FAMILY PHOTO**

Plenary Chamber, Jēkaba Street 11

PANEL III

13:00 – 14:00 **HOSTILE USE OF INFORMATION**

Mr Jānis Sārts, Director of NATO StratCom COE

Mr Varis Teivāns, Deputy Manager at Latvian Cybersecurity Unit Cert.lv

Mr Stefan Meister, Director, Center for Central and Eastern Europe, Russia, and Central Asia, German Council on Foreign Relations

PANEL IV

14:00 – 15:15 **CYBERSECURITY AND FOREIGN INVESTMENT**

Mr J.R. Helmig, Chief Analytics Officer, SAS Federal

Mr Andrew Davenport, Chief Operating Officer, RWR Advisory Group

Mr Rene Summer, Director, Government and Industry Relations, Ericsson

Mr Matīss D. Kukainis, Former President, American Chamber of Commerce in Latvia

15:15 – 15:30 **COFFEE BREAK**

PANEL V

15:30 – 16:45 **INTERNATIONAL ENFORCEMENT**

Ms Maija Treija, Director of Compliance Control Department, Latvian Finance and Capital Market Commission

Mr Joseph Humire, Executive Director, Center for a Secure Free Society

Mr Lawrie Elder, Principal, Intelligence & Investigation Practice, SAS Corporation

Mr David Murray, Vice President for Product Development and Services, Financial Integrity Network

CLOSING

REMARKS 18:00 – 20:00

RECEPTION

Attendance list – 8th Parliamentary Intelligence Security Forum

Members of Parliament
Arta Dade, Albania
Namik Dokle, Albania
Grubešić Željko, Bosnia and Herzegovina
Borislav Bojić, Bosnia and Herzegovina
Sifet Podžić, Bosnia and Herzegovina
Tsvetan Tsventanov, Bulgaria
Dimitar Lazarov, Bulgaria
Filip Popov, Bulgaria
Mustafa Karadayi, Bulgaria
Valentin Kasabov, Bulgaria
May ElBatran, Egypt
Raivo Aeg, Estonia
Kseniya Svetlov, Israel
Irakli Beraia, Georgia
Andreas Jahn, Germany
Mārtiņš Bondars, Latvia
Ojārs Ēriks Kalniņš, Latvia
Kārlis Krēsliņš, Latvia
Jānis Ruks, Latvia
Kārlis Seržants, Latvia
Veiko Spolītis, Latvia
Solvita Āboltiņa, Latvia
Ināra Mūrniece, Latvia
Ainars Latkovskis, Latvia
Vytautas Bakas, Lithuania
Emanuelis Zingeris, Lithuania
Eugene Berger, Luxembourg
Alex Bodry, Luxembourg
Talat Xhaferi, Macedonia
Mihaela Spatari, Moldova
Ulf Leirstein, Norway
Ingjerd Schou, Norway
Pedro Bacelar de Vasconcelos, Portugal
Sergio Sousa Pinto, Portugal

Constantin-Laurentjiu Rebega, Romania
Dirk Stubbe, South Africa
Tabiso Wana, South Africa
Luis Fernandes Aznar, Spain
Vicente Moret, Spain
Helene Petersson, Sweden
Krister Hammarbergh, Sweden
Anti Avsan, Sweden
Madeleine Moon, United Kingdom
Robert Pittenger, United States
Government Officials and Private Sector Experts
Germain Poirier, Canadian Armed Forces
Maja Cavlovic, Defence and National Security Adviser to the President of Croatia
Davide Colella, Italy
Marco Bernardy, Italy
Archil Sokhadze, Senior Counsellor of the Embassy of Georgia to Latvia
Elza Paegle, Special Advisor for Foreign Policy and Intelligence, Germany
Klaus Wittman, Brigadier General, Germany
Stefan Meister, Director, German Council on Foreign Relations
Vineta Mēkona, Representative of NATO StratCom COE
Simona Gurbo, U.S. Embassy in Riga, Latvia
Mārtiņš Spravņiks, U.S. Embassy in Riga, Latvia
AeKyong Sweeton, U.S. Embassy in Riga, Latvia
Vanessa Acker, U.S. Embassy in Riga, Latvia
Sanda Liepina, Association of Latvian Commercial Banks
Jānis Brazovskis, Association of Latvian Commercial Banks
Arnis Lagzdiņš, Latvian Financial and Capital Market Commission
Uldis Elksnīts, Representative of Latvian Ministry of Foreign Affairs
Laura Ošleja, Adviser to the Latvian National Security Committee
Paulius Bačiulis, Lithuania
Aušra Lazauskienė, Lithuania
Claude Trierweiler, Deputy Head of Mission, Embassy of Luxembourg
Illir Selmani, Chief of Cabinet, Macedonia
Vjolca Bajrami, Collaborator at the Cabinet, Macedonia
Besa Drndar, Macedonia
Maija Treija, Finance and Capital Market Commission

Ana Kachakova, Deputy Head of the International Cooperation Department, Macedonia
Abaz Xheljadini, Macedonia
Eugen Revenco, Ambassador of Moldova to the Republic of Latvia
Pieter Jan Langenberg, Ambassador of the Netherlands to the Republic of Latvia
Lisabeth Stock, Adviser of the International Department to the Norwegian Parliament
Jarosław Ćwiek-Karpowicz, Counsellor – Political and Economic Section, Poland
Pawel Chorazy, Undersecretary of State at the Ministry of Economic Development, Poland
Peter Hatiar, Ambassador of Slovakia to the Republic of Latvia
Varis Teivāns, Deputy Manager at Latvian Cybersecurity Unit
Madeleinne Brant, Executive Director, Office of the Speaker of Parliament, South Africa
Wilhelm Janse van Rensburg, South Africa
Rick A. De Lambert, Senior Commercial Officer of the U.S. Embassy in Helsinki
Clark Fonda, Deputy Chief of Staff, Office of U.S. Congressman Robert Pittenger
Nancy Bikoff Pettit, Ambassador of the U.S. to the Republic of Latvia
Mark Hanson, Director, Cyber and Emerging Technologies Section, U.S. Department of the Treasury
Mike Shanahan, Assistant Legal Attaché, U.S. Embassy Tallinn
Bryan Carroll, Foreign Service Officer, U.S. Embassy Riga
Frederick Reynolds, Global Head of Financial Crimes Compliance, Barclays
William Fox, Global Financial Crimes Compliance, Bank of America
J.R. Helmig, Chief Analytics Officer, SAS Federal
Andrew Davenport, Chief Operating Officer, RWR Advisory Group
Rene Summer, Government and Industry Relations, Ericsson
Matīss D. Kukainis, American Chamber of Commerce in Latvia
Joseph Humire, Center for a Secure Free Society
Lawrie Elder, SAS Corporation
Charles Bretz, Director of Payment Risk, Financial Services Information and Analysis Center
David Murray, Vice President, Financial Integrity Network
Ross Armstrong, Center for a Secure Free Society
Jason Wrobel, Center for a Secure Free Society

Subject: 8th Parliamentary Intelligence Security Forum:

Congressman Pittenger with Ksenia Svetlova (Israel), May El Batran (Egypt), and Davide Colella (Vatican)

1. Congressman Pittenger joined officials from 30 different countries to discuss national security challenges facing both governments and public sectors, alike. Discussions at this forum focused on terror financing, cybersecurity, information sharing, and countering Russian and Chinese counterintelligence. The panels were comprised U.S. and international experts who discussed the challenges that financial institutions and governments may face in preventing terror finance, as well as cybersecurity and counterintelligence threats posed by adversaries. The day began with remarks from European Officials and Congressman Pittenger.

   Ms. Ināra Mūrniece, The Speaker of the Parliament of Latvia, started her remarks with the current challenges that Latvia and Eastern Europe face. Cybersecurity and Russian propaganda were mentioned as a threat to democratically established governments in the region, specifically by the Russian government's efforts to undermine the people's confidence in their elected government. Next, Ms. Nancy Bikoff Pettit, the Ambassador of the United States to Latvia commented on the renewed vulnerability that their countries and the U.S. share because of ramped up cyber-attacks by state and non-state actors. Ambassador Pettit stated that the high level of connectivity between nations raises threats such as attacks on a country's power grid or private business. Cybercrime costs businesses an estimated $400 billion per year.

   Mr. Paweł Chorąży, the Undersecretary of State at the Ministry of Economic Development of Poland was the next panelist to speak. He focused on a few specific policies that Poland has put in place dealing with the discussed issues, which he stated have been successful. The 2016 Anti-Terror Act created a foundation for close cooperation between law enforcement entities, making it easier for Poland to have large international events without fearing for security, such as the NATO Summit.

   Congressman Pittenger also joined the panel with a message of cooperation between countries, stating that in the fight against terror we are only as strong as our weakest link. He discussed how the tools of unconventional and cyberwarfare are as important if not more important than the tools of kinetic warfare.

2. The forums first panel consisted of law enforcement and government officials tasked with cybersecurity issues. Mark Hanson, the head of Cyber and Emerging Technologies at Fincen, spoke about an issue that is paramount to the terrorism and illicit finance policy sphere – bitcoin and

virtual currency. He stated the importance of maintaining agility with emerging technologies, such as virtual currencies and money transfers. Bitcoin's structure and prominence was also a focus of the discussion, noting that there are 1.3 Billion transactions on virtual currencies per day.

Brian Carroll, a Foreign Service Officer at the U.S. Embassy in Riga, gave the State Department's perspective on cybersecurity. The State Department uses a holistic approach to ensure that the internet is open and secure enough to be the basis for all modern diplomatic efforts. Mr. Carroll mentioned four points that the State Department was concerned with: International Security, a multi-state stakeholder in the internet (the concept that the government of a single state should not have total control over their country's internet), using the internet as an engine of economic growth, and countering cybercrime.

Congressman Pittenger moderating Panel II, which included Frederick Reynolds from Barclays, William Fox from Bank of America, and Charles Bretz from the Financial Services Information and Analysis Center

The next panelist was Mike Shannahan, an FBI Supervisory Special Agent and Assistant Legal Attache. Mr. Shannahan spoke about the FBI program he was involved with, which stationed him in Eastern Europe to work with foreign law enforcement counterparts. This concept has been applied to the National Cyber Investigative Joint Task Force, an interagency group led by the FBI, including 24 law enforcement agencies which are co-located. The goal of this task force is cooperation between law enforcement and interagency cooperation.

3. Private sector officials from the financial industry discussed the challenges that they face in tracking illicit finance and sharing information with the government. The first panelist in this series was Charles Bretz from the Financial Services Information and Analysis Center. The goal of his organization is to protect financial institutions and the financial services industry in general from cyber and fiscal attacks. He advocated for larger information sharing between financial institutions, since terrorist groups now use multiple small accounts to finance their operations. He stated that in the $5 Billion worldwide that was stolen in cyber-attacks and then recovered, the money was moved between 57 countries, which in his view demonstrates the need for international cooperation between financial institutions.

Frederick Reynolds, representing Barclays, was the next panelist to give testimony. He reiterated the need for information sharing between financial institutions, while mentioning that local law sometimes inhibits colleagues in the same building from communicating regarding a security threat, and that it must be addressed on a federal level. He stated the need to expand sections 314A of the PATRIOT Act to have a discussion between industry and government, building a more expansive picture of terrorist financing networks. Mr. Reynolds also stressed the need for a consistent policy from government, since banks rely on and depend on consistency in all operations.

Bill Fox of Bank of America brought real world examples into the fold. He discussed Bank of America's role in arresting the Boston Marathon Bombing terrorists, and pointed out that without both an ATM camera video and the information being shared with the government, the suspect would have taken much longer to be apprehended. Tracking the financial transactions of the suspect ultimately led to the bank being able to immediately give law enforcement his location. This was an example of financial institutions having more current information than government.

Ms Ināra Mūrniece, Speaker of the Parliament of the Republic of Latvia

4. Jānis Sārts, Director of NATO StratCom COE, began the discussion regarding the hostile use of information in the cyber sphere. He gave a view of information distribution as a more social tool. He began by discussing that there is no hierarchy of information flow, stating that the impact of information that an organization or government may release is based on the size of its network, which is unique to cyber. He proposed three strategies to counter disinformation released by hostile actors. The first of these proposals is educating the public in knowing when an outside actor is trying to influence them – when the public is educated on these matters the effect of the propaganda drops dramatically. Next was the government and media being trained to recognize when a news story is being manipulated to have a social impact on a country. The last is for governments to create their own narrative and go on the offensive with information.

   Mr Varis Teivāns, Deputy Manager at Latvian Cybersecurity, spoke about the technical perspective to counter hostile information sharing. He called for a multilateral perspective to counter these issues, and an example from the French Presidential election. In the French election, Russian

affiliated attacks were releasing leaks, however these were fed to them by a French intelligence agency, and were false. Therefore, the information was easily traced and discredited, minimizing the effect of the leaks.

Panel IV included Joseph Humire from the Center for a Secure Free Society, David Murray from the Financial Services Integrity Network, Lawrie Elder from SAS, and Maija Treija from the Finance and Capital Market Commission

Last in this panel was Stefan Meister the director for Central and Eastern Europe on the German Council of Foreign Relations. He spoke specifically about the threat that Russia poses to the EU with disinformation. He also states that it was surprising that these operations were not ramped up earlier by the Kremlin. The three ways that Russia spreads its disinformation is through state media such as Russia Today, internet trolls that intentionally disseminate this information online, and hacker groups.

5. The penultimate panel featured panelists discussing cybersecurity and foreign investment. J.R. Helmig started his statements discussing data analytics. He stated that the amount of data is not the solution, it is translating large amounts of data into actionable information that can be used to stop a transaction. Until the processes to translate data to information is set, data sharing will be less successful than it could be potentially. Per Mr. Helmig, from a business perspective disregarding policy, the challenge is the translation of the data not the amount.

   Andrew Davenport started his statements discussing money laundering via real estate transactions. He stated that this problem has been recognized by not only national governments but also international organizations. The money can be laundered most easily between exclusive transactions since there are no comparable properties. Governments of emerging economies may turn a blind eye to these foreign investments because they are weary of stopping foreign investment. He also mentioned Secretary Mattis' statements regarding CFIUS, which Mr. Davenport agrees lacks cohesiveness and modernity.

   Matīss D. Kukainis, the former President of the American Chamber of Commerce in Latvia, rounded out this panel by stating that the next wave of technology will help us gain value, however this will leave industries more dependent on technology and therefore more vulnerable to cyber-attack. Cyber-Attacks could go from hacking Netflix to hacking an E-Healthcare System. This raises the risk that businesses face and that countries face due to increased dependency, reinforcing the need for more government action in this sphere.

6. International enforcement was the topic of the final panel, including international law enforcement. Joseph Humire, the Executive Director of the Center for a secure and Free Society was the first panelist in this series. Mr. Humire stated the need for modernization of the sanctions process, since the President needs to declare a national emergency every time sanctions are applied. He also focused on the asymmetry of the fight against cyber-attacks, which in the case of the United States led to a strict enforcement of not only civil but also criminal enforcement, affecting the financial industry. Maija Treija reiterated the globalization of the financial industry and the role that this plays in foreign investment.

   Lawrie Elder, who is the Principal in the Intelligence & Investigate Practice in SAS. Mr. Elder plays a role in between law enforcement and SAS, assisting them when cooperation is necessary. He gave the example of the creation of DHS after 9/11 in order to have greater cooperation between government agencies, however the amount of data and lack of trust in political systems are the difficult elements of information sharing. The trust is not only public trust but interagency trust, which is commonly a jurisdictional issue that may hinder cooperation.

###

UNITED STATES DEPARTMENT OF THE TREASURY

FinCEN

FINANCIAL CRIMES ENFORCEMENT NETWORK

2 August 2017

SUMMARY OF REMARKS AT THE 8TH PARLIAMENTARY SECURITY INTELLIGENCE FORUM IN RIGA, LATVIA

Mark Hanson, Chief of the Cyber and Emerging Technologies Section at the Financial Crimes Enforcement Network (FinCEN), provided a discussion of how FinCEN has strived to stay ahead of the technical evolution in financial crimes and terrorist financing. He described how changes in information technology and innovations in fintech are bringing many benefits to society, while also leading to more technology-oriented financial crimes. He shared his team's experience adapting its financial crime mission to the cyber domain—developing expertise in cybercrime, emerging payment systems, and new financial infrastructure that allow them to combat evolving threats, such as criminals' abuse of virtual currencies.

Mr. Hanson provided an overview of issues in virtual currencies and how the U.S. has incorporated these new technologies into existing regulatory frameworks. He described how virtual currencies, like bitcoin, have achieved technological breakthroughs in their advancement of blockchain technology, sparking a wide range of new innovations and applications in fields outside of finance. He explained how these virtual currencies have been exploited in a variety of financial crimes, such as in darknet marketplaces, at scales that, while small compared to the global financial system, supports a concerning amount of illicit activity. By engaging with these new technologies early and providing guidance to industry, FinCEN has received many thousands of reports from virtual currency money services businesses identifying suspicious activity associated with virtual currencies. Mr. Hanson described how law enforcement has been able to use this data and specialized tools to successfully investigate financial crimes conducted through virtual currency.

In the face of a variety of cyber-enabled crimes, he noted that many of these schemes continue to take advantage of regulatory gaps between jurisdictions and exploit vulnerabilities in traditional business processes. Mr. Hanson encouraged legislators and government agencies to stay engaged with changes in technology, look to international standards, and to work with their local industry to study relevant issues.

Threat Analysis
SAS Institute

Environment and History

Recent military success against Salafi jihadist terrorist groups has seen the Islamic State in Iraq and the Levant (ISIL) losing their foothold in territories that have been considered their heartlands in Iraq and Syria. A notable consequence of these developments has been a strengthening of these groups' commitment to target Europe and North America. This approach has met with some success, drawing on the experience of European ISIL fighters returning from the frontlines. Simultaneously, they have set out to motivate "lone-wolf" attacks and to develop localized networks of extremists using on line propaganda.

These activities have driven several recent high-profile, high-casualty attacks, primarily against European civilian targets in heavily populated public areas. Their tactics have varied greatly, ranging from sophisticated, highly coordinated attacks to crude, blunt-force strikes by individuals. Perhaps more significantly, these attacks have served to highlight failings in the local, national, and international intelligence and enforcement services who are perceived to have missed opportunities to preemptively disrupt them.

The changing nature of the terrorist threat has required intelligence and enforcement agencies to shift their focus and adjust their tactics. Perhaps the greatest influence on this change has been that recent attacks have been largely perpetrated by individuals who have been known criminals. Indeed, many of ISIL's successes can be directly attributed to this ability to radicalize young men through a one-way channel of on line communication. These individuals typically have a background in gangs and petty crime, are from 2nd generation immigrant families and have shown no particularly strong religious attachment until they began to access the ISIL propaganda.

These factors are driving changes in the counterterrorism dynamic and have exposed weaknesses in the traditional capabilities around gathering, exploiting, and sharing of intelligence within and between agencies and nations. While counterterrorism has traditionally been the domain of intelligence and homeland security agencies, recent terrorist attacks (born out of and planned within criminal networks) have to a large extent ranged beyond these services' purview. This change in dynamic has placed law enforcement at the center of counterterrorism endeavors and has, as a direct consequence, seen general policing or community information elevated to being among the most critical of data sources.

Examples

Sophisticated and Coordinated: In November 2015 a brutal, highly coordinated attack took place in Paris when ISIL-inspired terrorist cells, using assault rifles and wearing suicide vests, simultaneously attacked multiple soft targets, including the Bataclan Theatre, where 89 died. The terrorist network behind the attack was led by Salah Abdesalam, a radicalized individual with strong links to known criminal networks. The group also included individuals who had previously fought in Syria.

Michael Leiter, former director of the United States' National Counterterrorism Center, commented afterward that "the attacks demonstrated a sophistication not seen in a city attack since the 2008 Mumbai attacks, and would change how the West regards the threat" of terrorism generally.

Blunt Force: In July 2016 Mohamed Lahouaiej Bouhlel drove a lorry into a Bastille Day celebration in Nice, France, killing 84 people. This blunt-force attack might have lacked the sophistication and planning of the Paris attack, but it ultimately had a similarly deadly effect. Although Bouhlel was known to law enforcement for involvement in petty criminality, there were no reports of his having any direct links with a terrorist group. However, he was subsequently claimed by ISIL as a "soldier of Islam." Significantly, he was known to have psychiatric problems, a characteristic increasingly common in these incidents.

The evidence indicated that Bouhlel had been radicalized by ISIL propaganda, and he was subsequently classified by elements of the mainstream media as a "lone-wolf" actor. Nevertheless, he did not act alone in the planning and development of his attack, and his actions were facilitated by criminal contacts through which, among other activities, he procured a firearm.

The use of Intelligence

Transatlantic law-enforcement communities have publicly acknowledged their current weaknesses and their vulnerability to future terrorist attacks. This recognition has resulted in a number of initiatives to assist with building understanding of possible ways to mitigate such threats in the future.

A significant body of work is to be found in the GLOBSEC Intelligence Reform Initiative (GRI), which recently published a paper, "Reforming Transatlantic Counter-Terrorism". One of the important observations of this paper was the following:

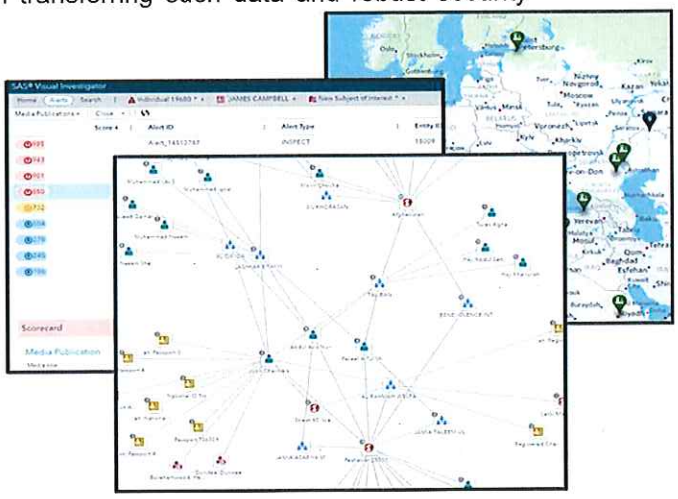
> *"The key problem the Globsec Intelligence Reform Initiative addresses is that of intelligence and personal data sharing and its operationalisation at the domestic as well as transnational level. Although many intelligence agencies have been at the centre of counter-terrorism efforts since 9/11, this report recognises that as terrorism is fundamentally viewed as a crime in both Europe and North America, Law enforcement is increasingly at the centre of better pan-European and transatlantic counter-terrorism cooperation. Crucially, better fusion of intelligence processes, and intelligence and law enforcement agencies, is needed to provide the means for pre-empting terrorist attacks before they occur, rather than relying on effective investigation after the event."*

While the need for data sharing and the operationalization of intelligence products is widely accepted, there is also a recognition that to be effective, agencies must enhance the information technology capabilities around collation, analysis, and the associated management of operational processes.

The related significant challenges are often magnified rather than lessened by the volume of data that exists for agencies to exploit. Information sources are vast and varied, a complexity that is only increased by this now essential inclusion of day-to-day community and policing data.

In order to reduce complexity and cost it is always beneficial to, as far as possible, bring all of that data together for process management and analysis on a single secure platform – complete with proper governance and privacy controls.

As a first step then, the challenge is to collect, collate, classify and (crucially) de-conflict large amounts of data both structured and unstructured from a wide variety of disparate sources. Aside from the surmountable technical challenge, there are obvious political and legislative concerns in transferring such data and robust security models in the technology and processes will need to be evidenced to provide confidence that inter-agency data will be secure.



Once the above processes have been undertaken we have enhanced the value of the data and can categorize it as information. Only once this information has been graded for relevance, veracity and security can it be categorized as useful intelligence which can then be used to provide the intelligence products (target profiles, risk assessments) to drive disruptive, pre-emptive or investigative security operations. At all times during the above process raw data, structured information and collated intelligence are made available for analysis to find indicators, insights and outliers which then augment, inform and drive the intelligence and investigative process.

In short: technology is not a "magic bullet" to prevent terrorism or solve crime. It does however provide security agencies with the capability to deal with the growing amounts of information available and to analyze, process and act with the enhanced insight, efficiency and effectiveness that the current situation demands.

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
MS2 – 2C104
WASHINGTON, D.C. 20511

July, 2017

Dear Participants of the 8th Parliamentary Intelligence Security Forum:

As a previous participant and presenter at these forums, I understand the benefit these events offer for healthy dialogue and understanding of important global security issues, such as combatting terrorism. Many forum participants are familiar with the Privacy and Civil Liberties Oversight Board (PCLOB). For those who are not, I would like to provide a brief background on this independent agency in the executive branch of the U.S. government.

The PCLOB is a five-member board created as a result of a recommendation of the National Commission on Terrorist Attacks Upon the United States (also known as the 9/11 Commission). The Commission examined the intelligence failures that led to the events on September 11, 2001, and analyzed what the United States could do to prevent future attacks. The 9/11 Commission report offered 41 recommendations to keep America safe – mainly emphasizing the need to strengthen information sharing across the intelligence community.

However, while recommending changes to the way the government collects and shares intelligence, the Commission also recognized the need for a central voice in the executive branch to oversee privacy and civil liberty concerns. To that end, the Commission recommended creating a board within the executive branch to monitor actions across the government.

Congress and the President enacted legislation to establish this Board, but it has taken nearly a decade to stand it up in the fashion that it is today. In fact, the Board only began its work in earnest in 2014 soon after the 5th member – its Chairman – was appointed and confirmed by the Senate.

As an independent, bipartisan agency, the PCLOB has two fundamental statutory responsibilities: advice and oversight. First, it provides advice relating to executive branch actions or efforts to protect the nation from terrorism and, second, it provides oversight to executive branch counterterrorism actions or efforts – a role that entails close attention to implementation of both law and policy.

Although the PCLOB does not make law, nor draft or enforce regulations, the U.S. Congress and other federal agencies may consult the PCLOB for its legal and policy perspectives as they engage in the legislative or other regulatory processes. Over the years, the U.S. intelligence community often has sought advice from the PCLOB on executing its programs. This practice gives national security officials an extra degree of assurance that their efforts do not unnecessarily trespass upon civil liberties.

It is important to stress to our foreign partners that PCLOB's statute only permits it to engage on privacy and civil liberties matters in the counterterrorism realm. Under this specific mandate, PCLOB successfully produces reports that are relevant to the U.S. intelligence community, elected officials, non-governmental organizations, and others concerned about how best to simultaneously protect America and privacy and civil liberties. While some of the PCLOB's work is classified to allow for the rigorous examinations of executive branch counterterrorism efforts, including some of the most prevalent intelligence security issues of the day, the PCLOB makes its reports public to the extent consistent with the protection of classified information and applicable law.

The PCLOB continues to exercise its oversight function to review and analyze actions the executive branch takes to protect the nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties. Although the agency is currently in a sub-quorum status pending the appointment of new members, the staff continues its work on advice and oversight projects previously approved by the Board.

PCLOB's responsibilities also include oversight of the executive branch's use of financial information to combat terrorism and its financing. Financial information can provide uniquely timely and accurate information about terrorist financing. This is because the reliable movement of funds demands precision in identifying the sending and receiving entities. The PCLOB's oversight of the executive branch's use of financial information in its counterterrorism efforts is a critical component of the U.S. government's overall effort to protect privacy and civil liberties.

All of the forum's participants and speakers – whether from a major financial institution or a member of Parliament – play a role in safeguarding the world's citizens from terrorism. I would like to thank Rep. Robert Pittenger and the Parliament of Latvia for organizing such a diverse group of experts to discuss collaborative efforts to counter terrorism in all of its forms.

Sincerely,

Elisebeth B. Collins
Board Member

Combating Terrorist Financing

An International Bank Perspective

BARCLAYS

Combating Terrorist Financing

- The Keys To Combating Terrorist Financing Are:
  - Information sharing
  - Cooperation between governments and the private sector
- Terrorism financing is inherently challenging to detect—made even more difficult with the shift to lone wolf and less centrally organized attacks
- Critical to focus resources and attention on vulnerabilities and where the greatest impact can be made

Formal Processes for Information Sharing in the U.S.

Section 314(a), USA PATRIOT Act

- Requests to FIs from law enforcement (via FinCEN) for information on accounts and transaction activity of specified individuals or entities
- Response to 314(a) requests is mandatory

Section 314(b), USA PATRIOT Act

- Voluntary program to facilitate sharing of information between eligible US FIsfor the purpose of identifying potential terrorist activity or money laundering
- Participating FIs must register with FinCEN
- Statutory safe harbor from liability for sharing customer information
- Similar provisions coming into force in the UK this fall

"SAR Back-Up Request" (31 CFR 1020.320(d))

- FinCEN regulations require FIs to maintain supporting documentation for SAR filings for a period of five years and to make available to law enforcement and regulatory authorities on request

Informal Mechanisms for Information Sharing

Industry Forums

- Discussion among FIs, law enforcement, and regulatory authorities of emerging trends and threats
- Focus on typologies, industries, etc., rather than on specific entities

FinCEN Advisories/Bulletins

- FinCEN, through its Financial Institution Advisory Program, issues public and non-public advisories to financial institutions concerning money laundering or terrorist financing threats for the purpose of enabling financial institutions to guard against such threats

Other Law Enforcement / Regulatory Outreach

- Symposiums (Fed/FBI, HIDTA/ HIFCA)
- Case Studies
- Law Enforcement and Industry small group meetings
- JMLIT

Takeaways

- **Granular Risk Analysis:**
  - Don't broadly de-risk a country because it is "easier" and "less risky". Financial flows are the lifeblood of the economy and cutting them off wholesale only makes the problem worse.
  - Utilize all sources of information to conduct your analysis if possible (i.e. negative news, commercial solutions, NGOs, device IDs)
- **Dispel the Myths:**
  - Unlike some areas of regulation where good minds differ, no legitimate financial institution wants to bank criminals, terrorists or aid proliferation
  - Information sharing and advanced analytics in many ways increases rather than reduces privacy.
  - Despite the headlines, most financial institutions are not looking to spend less, cut corners or do less with their financial crime programs. Most industry suggestions look to make the money and time spent more effective.

Takeaways

- **What do we need from Governments:**
  - Provide Banks with actionable information. No one wants to bank criminals or terrorists.
  - Inconsistent legislative approaches in the areas of information sharing and data privacy makes our job much more difficult. To have an enterprise wide view and approach, we must be able to share information enterprise wide.
  - Banks want to be part of this fight. Vilifying or shaming "good" banks for small errors is counterproductive. It will only produce de-risking and less visibility.
  - Balance the policy objectives. Recognize that you cannot have financial inclusion, speed and transparency without some degree of risk of illegal money moving through a bank. If we totally de-risk, the illegal money is harder to find.
  - Law Enforcement should advocate for its priorities.