Chairman of the International Border Management and Technologies Association (IBMATA), Tony Smith CBE, discusses the future of border management which faces a multitude of complications

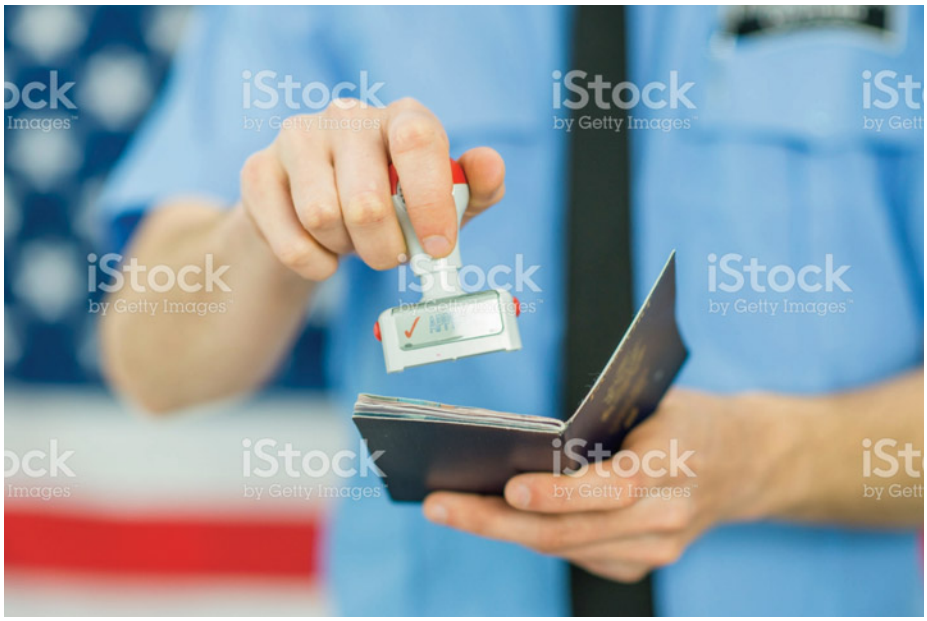
Securing borders in the modern world

Managing borders has never been an easy task; I lived through many challenging times during my career. From managing the Canadian ports of entry through the 9/11 period and the aftermath, managing the UK border through the growth of home-grown terrorism after 7/7, to securing the UK border for the London 2012 Olympics, and beyond; some things went well, some things not so well.

But through it all, one thing remained constant; the volume of people and goods crossing international borders continued to rise. If terrorism was designed to strike fear into the heart of travellers and to prevent passenger growth, it has patently failed to do so.

Some estimates suggest that air traffic will double in volume over the next 20 years. Passengers continue to subject themselves to the most stringent screening checks – both physical and virtual – to keep on the move. Those that guard the borders are expected to continue to process them at an ever-increasing rate, whilst at the same time finding that needle in the haystack who could be a terrorist.

We have also seen massive displacements of people across land and sea borders, who are on the move for different reasons. The crises in Myanmar and Syria have seen people fleeing for their lives, whilst others migrate for economic reasons – often becoming victim to the international gangs that prey on the vulnerable. Governments play their part, supported by international organisations such as the United Nations High Commissioner for Refugees (UNHCR), but ultimately there are no open doors. Governments are elected and immigration control (or the lack of it) always sits highly on the agenda of the electorate.



What is the role of border agencies?

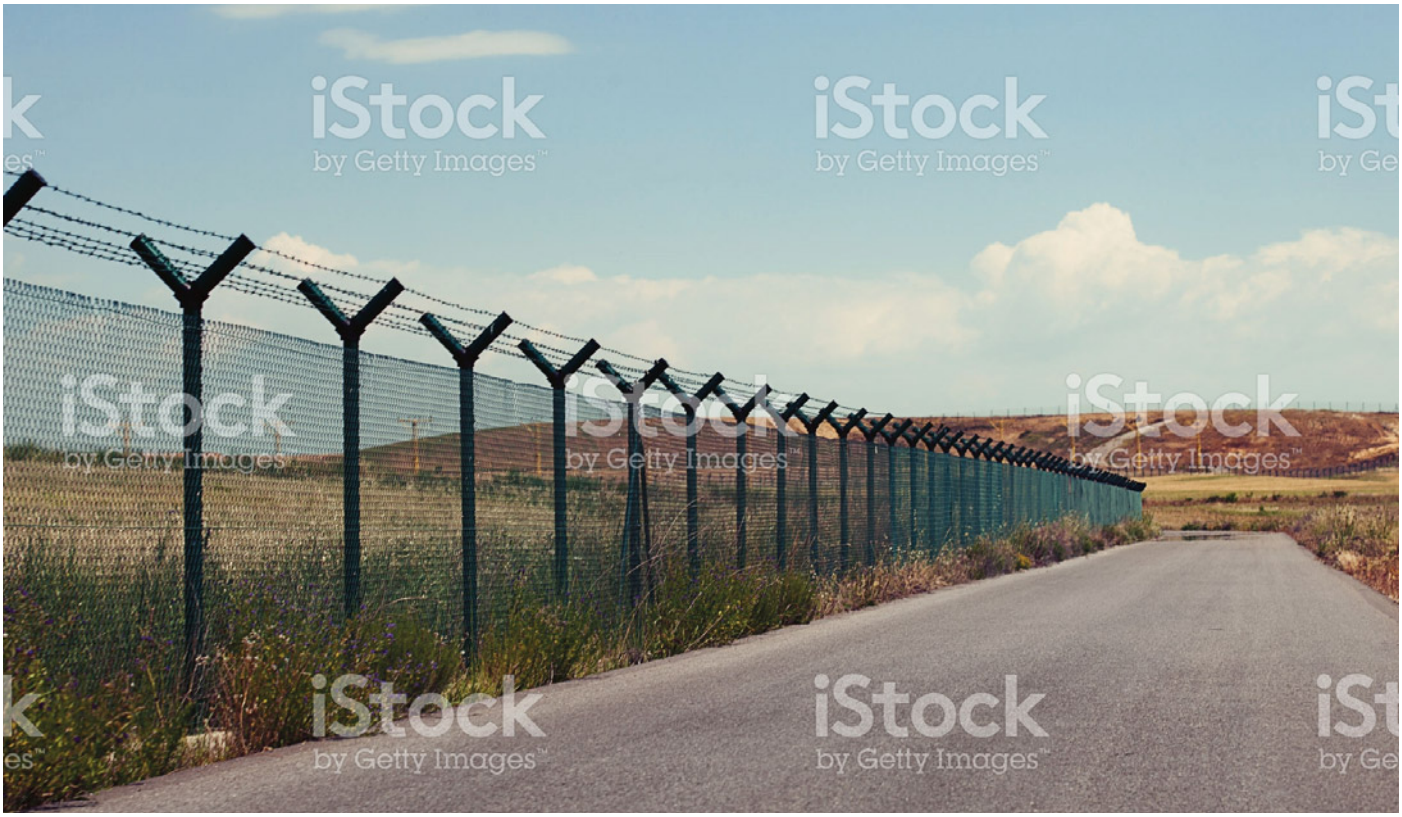
You don't take charge of a border agency if you want to win a popularity contest. We are expected to clear queues at borders very quickly, whilst ensuring that full checks are made upon everybody crossing, and woe betide us if somebody gets through that shouldn't get through. In the trade, we call it balancing faciliation with control – a principle that applies universally in any border agency mission statement. But, it is easier said than done.

9/11 became a watershed for border agencies when 19 terrorists breached the US visa system to carry out the worst terrorist attack in history. Problems in the US government over governance, authority, data sharing, and even culture, were exploited by terrorists to deadly effect. The attacks on the London Metro system on 7/7 took this to a new level – terrorism was no longer just a foreign threat, but a domestic threat.

Identifying threat

You can't identify terrorists by their nationality or background. Yes, there are indicators, but indicators can only be identified by intelligence. Intelligence needs to be manipulated in such a way that it provides the maximum capability to find the needle in the haystack, which – in turn – takes us to technology.

One would hope we would learn lessons from the past. Yet, when we look at the terrorist attacks in



Paris in November 2015, we see a different story. At least seven of the Paris attackers are believed to have travelled to Syria to fight for Islamic State of Iraq and the Levant (ISIL), and returned to the EU undetected. All the attackers were known to the police – some for crime, some for terrorism, some for both. Two of the attackers were fingerprinted at the Greek border six weeks earlier, posing as refugees in the migrant crisis. Most of the attackers lived in residential areas in Paris and Brussels, of which were known to be breeding grounds for ISIL.

Many of the factors we saw in the USA on 9/11 re-emerged in France 14 years later. Vital intelligence was not being shared with the right people in the right places at the right level, and certainly not with border agencies.

So, how to de stop it happening again?

The short answer, of course, is that we can't. There are no guarantees against human behaviour. But there are some things we can do, in the context of securing our borders. So – in considering the issues of border controls in Europe – what does this mean?

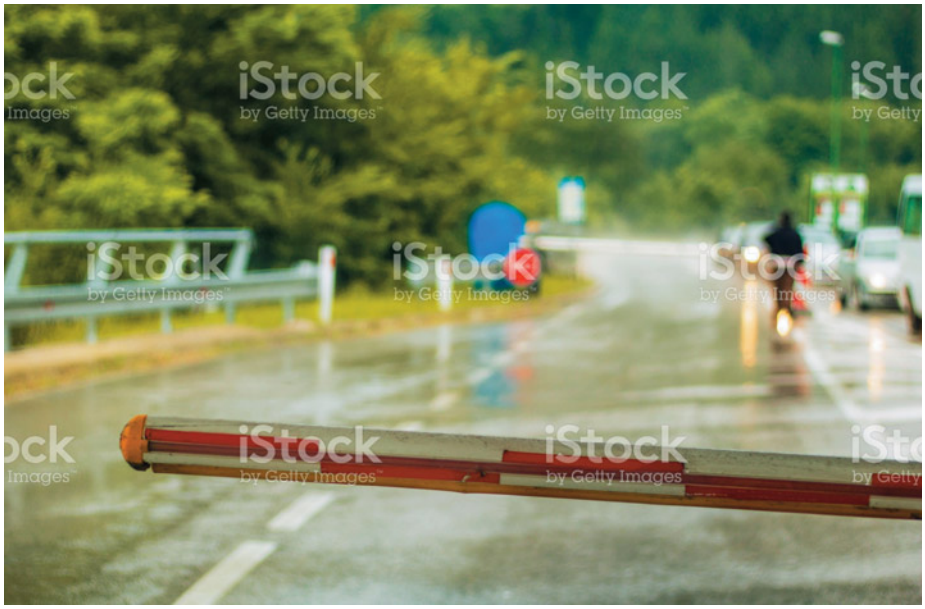
There are three fundamental and enduring principles to border management all border agencies should aspire to uphold that have stood the test of time. These are known as:

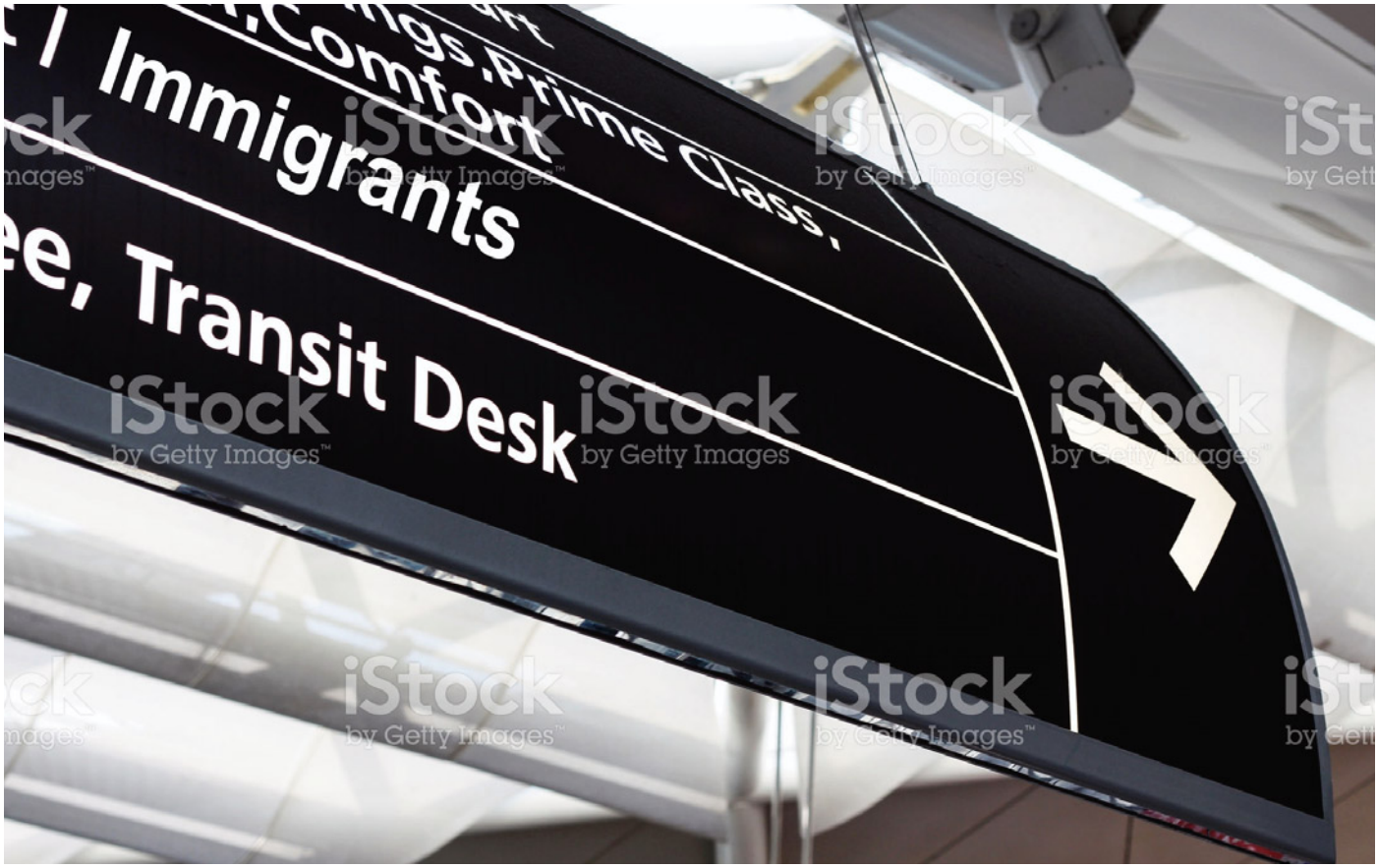
- the multiple borders strategy;
- integrated border management; and
- end to end identity.

Firstly, the multiple borders strategy demands that borders are constructed by transaction rather than physical inspection, and transactions take place as early as possible in the traveller continuum. For air traffic, this means getting data in advance of travel, performing a pre-arrival risk assessment, and – assuming all is well – allowing a seamless arrival upon landing with minimal queues. For maritime traffic, the same principle applies.

A strategy for air and sea

To deliver this strategy, there needs to be strong collaboration between the air and sea operators that transport people, and the border agencies that admit them. This is where technology comes in. Visa systems, electronic traveller authorities, advanced passenger information, passenger name records, and other national and international data sources need to combine with national and international watch lists and warnings systems. This synergy will ensure that only those who are entitled to travel – and those who do not harbour harmful intent – are able to do so. This means building a data eco system in Europe which has the necessary depth and breadth of capacity to do this. Thus, people who are non-compliant and/or those who pose a





threat cannot board the ship or aircraft in the first place.

Managing borders on the ground

This is of course more difficult to apply at land borders. These are easier to manage if there is collaboration on either side, and preferably a pre-clearance agreement. The arrangement under the Le Touquet treaty enables UK officers to work in Calais, and French officers to work in Dover. Similar arrangements apply along the 5,000-mile-long border between Canada and the US.

By working together, both countries can intercept threats before they enter their territory. Conversely, they can identify common risk assessment factors which would enable seamless travel in both directions for pre-approved travellers through registered and trusted traveller programmes. Again, this means deploying state of the art technology which is capable of refining and analysing data – often in different languages and formats – across a single platform.

An alternative approach

Secondly, integrated border management means that the various actors involved in the border management process must work together in collaboration to facilitate genuine traffic, and interdict harmful traffic. History points to systemic failures in this area, including 9/11, 7/7, and the Paris attacks. Of course, politics plays a role here.

Some countries are more prepared to demand and share personal data than others; whilst some agencies are more inclined to be open with their counterparts than others. There are legitimate concerns about privacy and data protection, but there is no point in holding secret information upon a high-risk individual in one part of government, if that information is not made available to other parts of government with an opportunity to intervene. In particular to border agencies, who are probably best equipped to do so. The very concept of integrated border management was devised by the European Union and promoted by them as best practice in other countries. It is therefore more important than ever that they practice what they preach.

Technology *versus* threat

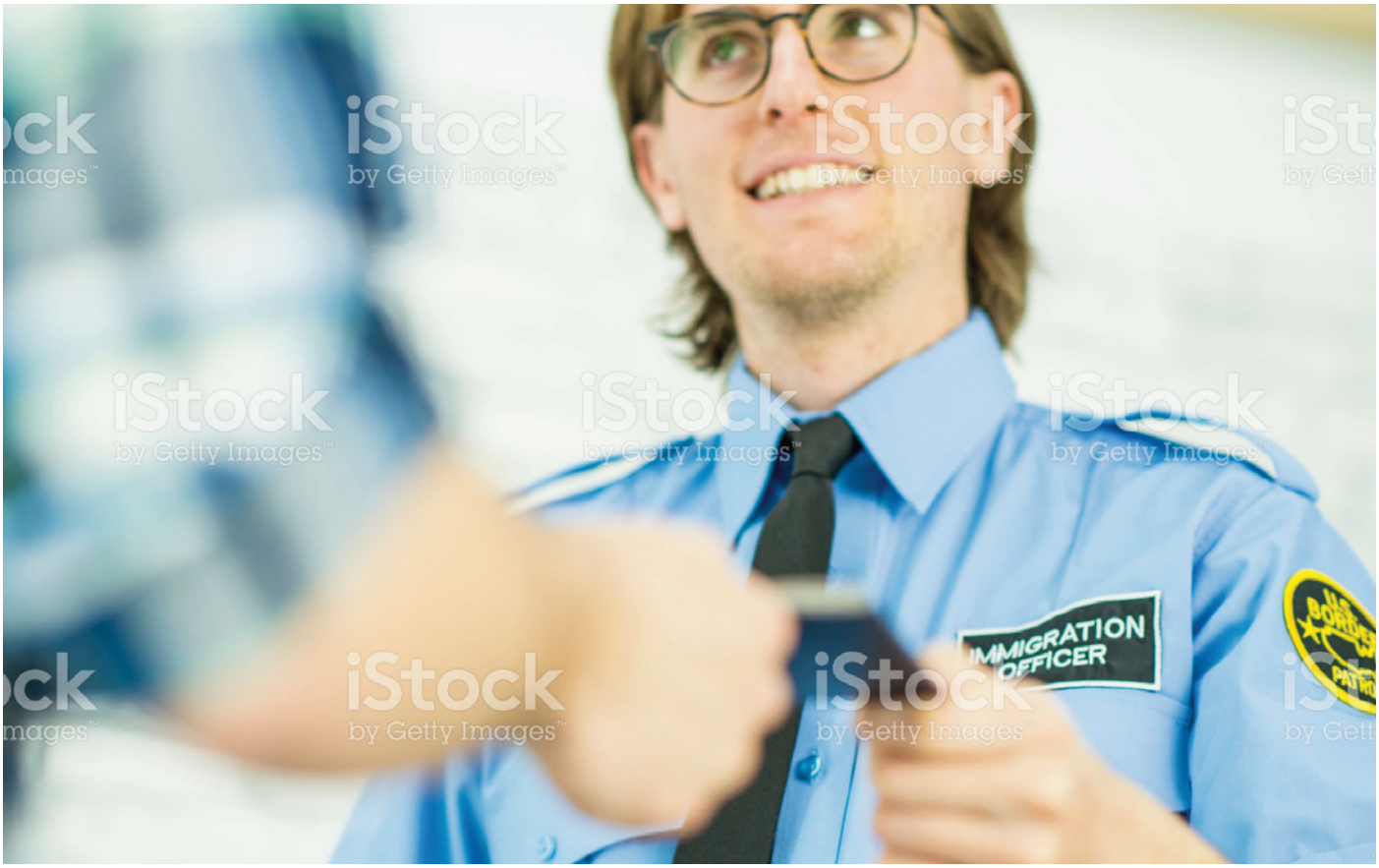
Thirdly, the rapid development in biometric technology opens huge opportunities for border agencies in the end to end continuum. By capturing biometric indicators (such as face, finger, and iris) at a first point of contact, border agencies enable the biometric to become the key token for identification at borders, and increasingly, for entitlement to services.

Putting knowledge into practice

In my time as Director of UK Ports of Entry, I was frequently criticised because serious criminals who had recently been deported were soon back on the streets of London committing crime again. This was because they had been able to secure a new identity and a fresh passport, which concealed their previous misdemeanours in the UK.

The biometric visa

By introducing a biometric visa we were able to identify them from fingerprints, regardless of the name on their travel document and thus, refuse entry. More recently, I presided over the "biometric Olympics" in 2012, where we required all games family members from visa countries to undertake biometric checks against our criminal and terrorist watch lists before they were allowed entry.



Nowadays advancements in facial recognition technology enables border agencies to recognise vast numbers of travellers with e-passports at automated border controls, without the need for physical inspection by an officer. More forward-thinking countries are already looking at the next generation of automation, where passengers will pass seamlessly through border control without needing to stop at all. Biometric technology must therefore be a key component of any modern-day border system.

The EU has not been idle in recognising these principles, or in using technology to address them. The EU Smart Borders Programme has been working on data integration for some time and plans for biometric entry and exit at the EU Frontier are well underway.

Technology continues to accelerate at an alarming rate, with new initiatives such as artificial intelligence, the Internet of Things (IoT), blockchain, and others, are becoming increasingly common language in modern day border management.

How important is collaboration across countries?

All of this is fine, but none of it will work without one key factor. Collaboration is the critical factor to success. When I was a leader in borders – whether in Canada or the UK – I had only limited knowledge or exposure to the art of the possible in developing technology. Since joining the private sector, I have found it difficult to bring the latest innovations to the attention of my successors.

I have addressed numerous conferences and events around the world where technology and border leaders come together, but invariably there is little or no ongoing dialogue between events about new and emerging trends, and how we can build stronger safer borders together in the future.

Therefore, I have founded the International Border Management and Technology Association. Our aim is to bring together border agencies, technology suppliers, ports and airports, transportation companies and academics into a single non-competitive community to discuss the latest trends in border management, and how to manage these. In addition to running regional events and workshops, we want to create a communications platform which enables these communities to come together in a spirit of collaboration.

Some of my best experiences in government were those where collaboration was at its best. We developed:

- joint passenger analysis units;
- border targeting centres; and
- integrated border enforcement teams in North America between the various US and Canadian enforcement agencies.

In the UK we built and implemented the CONTEST strategy, which brought together the UK law enforcement and other communities to counter the threat posed by home-grown terrorists. In 2012 we staged a hugely successful Olympic Games in London, bringing together government agencies from the UK and beyond to build a multi-agency risk assessment process to manage threats in an environment where the national threat assessment told us that a terrorist attack was highly likely.

If we are to manage the borders of tomorrow, we must learn lessons from the borders of yesterday. As a result, industry and government must work in collaboration to apply tried and tested border management principles to the very best new and emerging technology we have at our disposal.

Tony Smith CBE
Chairman
International Border Management and Technologies Association (IBMATA)

http://www.ibmata.org