WORLD SECURITY REPORT

Official Magazine of

International Association of CIP Professionals
www.cip-association.org

AUTUMN 2020
www.worldsecurity-index.com

IMPACT OF THE COVID-19 PANDEMIC AND CRISIS ON THE OPERATIONS OF CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES OPERATORS IN SOUTH EAST EUROPE

critical infrastructure PROTECTION AND RESILIENCE EUROPE

11th-13th May 2021

Bucharest, Romania

www.cipre-expo.com

CALL FOR PAPERS

Abstract submittal deadline - 30th November 2020

Securing the Inter-Connected Society

UN Member States need "to share information [...] to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks."

The 7th Critical Infrastructure Protection and Resilience Europe brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing Europe's critical infrastructure.

Submit your abstract online today at www.cipre-expo.com.

To discuss sponsorship opportunities contact:

Paul Gloc
(UK and Rest of World)
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

Sam Most
(Mainland Europe & Turkey)
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

Paul McPherson
(Americas)
E: paulm@torchmarketing.us
T: +1-240-463-1700

Leading the debate for securing Europe's critical infrastructure

Owned & Organised by:

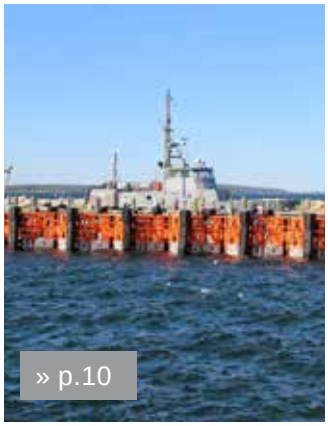
Supporting Organisations:

Media Partners:

CONTENTS

WORLD SECURITY REPORT


» p.5


» p.10


» p.24


» p.16

www.worldsecurity-index.com

Editorial:
Tony Kingham
E: tony.kingham@knmmedia.com

Assistant Editor:
Neil Walker
E: neilw@torchmarketing.co.uk

Features Editor:
Karen Kingham
E: karen.kingham@knmmedia.com

Design, Marketing & Production:
Neil Walker
E: neilw@torchmarketing.co.uk

Subscriptions:
Tony Kingham
E: tony.kingham@knmmedia.com

World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to over 130,000 organisations globally. It tracks the full range of problems and threats faced by today's governments, armed and security forces and civilian services and looks at how they are dealing with them. It is a prime source of online information and analysis on security, counter-terrorism, international affairs, warfare and defence.

ENVIOUS EYES, SLOWLY AND SURELY DREW THEIR PLANS AGAINST US

Yet across the gulf of space, minds that are to our minds as ours are to those of the beasts that perish, intellects vast and cool and unsympathetic, regarded this earth with envious eyes, and slowly and surely drew their plans against us.

War of the Worlds by H.G Wells

One of the greatest starts to a book ever written, but after a career in security, I'm afraid it always puts me in mind of something other than Martians. Those malignant minds out there, that are, as we speak, watching, waiting and drawing their plans against us!

And what lessons will those malignant minds have drawn from 2020?

Well, the obvious one is that if you really want to bring down the system, cause mass casualties, financial meltdown, spread fear and terror around the world, then bioterrorism is the way to go!

Conventional wisdom is that Bacillus anthracis, the bacteria that causes anthrax, is the most likely biothreat.

Why?, because according to the US Center for Disease Control (CDC) Anthrax spores are easily found in nature, can also be produced in a lab, and can last for a long time in the environment. Anthrax spores can be released quietly without anyone knowing, because you may not be able to see, smell, or taste them. They can be put into powders, sprays, food, and water.

Anthrax has been used as a weapon around the world for nearly a century. In 2001, powdered anthrax spores were deliberately put into letters that were mailed through the U.S. postal system. Twenty-two people, including 12 mail handlers, contracted anthrax, and five of these 22 people died.

Whilst it is, and always will remain a threat, Anthrax is not the sort of biothreat that is going to turn on your really committed, genocidal religious zealot. This is because the impact will always be relatively localised, as it requires the victim to touch, ingest or inhale the spores.

The really committed, genocidal religious zealot wants a virus that spreads, like COVID-19, but more lethal.

One of the early big stories at the start of the current pandemic were

READ THE FULL VERSION

The full version of World Security Report is available as a digital download at www.torchmarketing.co.uk/WSR

accusations that the pandemic started in a Chinese epidemiological laboratory. Now, this is almost certainly nonsense, but there are indeed epidemiology laboratories all over the world working hard on cures for infectious diseases, including COVID-19, as we speak. Meaning of course, that they legitimately store a whole range of deadly viruses for research purposes. This poses the question, how good is their security? especially with regard to insider threats?

Maybe, another viable source of a deadly virus is Ebola.

In June, the Democratic Republic of the Congo (DRC) announced a new outbreak of Ebola in Mbandaka, in its Équateur province. Whilst Ebola is not an airborne disease like COVID-19, so not as easily spread, it is much more deadly and available to any potential suicide bioterrorist. The disease has a high risk of death, killing 25% to 90% of those infected, with an average of about 50%. Symptoms typically start between two days and three weeks after contracting the virus, so time for a 'host' to transport the disease and spread it through liquid contamination.

The DRC's home-grown terrorist group, the Allied Democratic Forces (ADF) established ties with ISIS in late 2018, so the idea is not so far fetched as it might seem.

I would be the first to admit that my knowledge of epidemiology is based on what I have seen on the news and some limited research.

So, if I am way off the mark, I invite any readers who are experts, to share their thoughts in the next issue.

Tony Kingham
Editor

Impact of the COVID-19 pandemic and crisis on the operations of critical infrastructure and essential services operators in South East Europe

By mid-2020, COVID-19 pandemic (referring the period of writing this analysis) has caused a large number of deaths, significant economic damage and the collapse of many companies around the world, and surprisingly highlighted the considerable unreadiness of international organizations and the vast majority of countries to achieve timely and coordinated responses to the challenges they faced. That has additionally complicated the situation, intensified the effects of the crisis and created numerous cascading effects in all sectors.

Referring to the European continent, due to the delayed reaction, insufficient cooperation and concrete plan of both the European Union and the member states at the beginning of the crisis, borders were closed, economies slowed down and great uncertainty regarding all important political, business and social processes has emerged. Over time, the situation has partially stabilized – cooperation, coordination and solidarity has manifested but we are still in a state where we are

chasing COVID-19 consequences, the crisis is still unbridled and still insufficiently managed.

In relation with all that has been mentioned, great pressure was placed on critical infrastructures and essential services operators, who in circumstances of big uncertainty, closed borders, reduced cooperation and exchange of information had to ensure continuous operation of their business processes, protect themselves and their investments and ensure uninterrupted delivery of goods and service to its customers as well as other critical infrastructures. Where, referring to the text in the previous issue of the World Security Report (Summer 2020) „At the same time, it's necessary to point out that the pandemic threat wasn't among the ones properly addressed by critical infrastructures' business continuity plans." This has put critical infrastructures operators in the position of great stress and the need for vigorous action.

This analysis has the purpose to show in general how the operators of critical infrastructures and essential services from Southeast Europe have faced the COVID-19 pandemic and crisis, while the aim is to point out certain specifics in their response and identified lessons from the current part of the crisis. The methodology used in making the analysis consisted of three cross-cutting levels. At the first level, a desk top survey was used, through which the official websites of a number of critical infrastructures and essential services operators from Southeast Europe were reviewed and analyzed with the information they published related to business activity in this crisis. At the second level, electronic correspondence was used with a number of experts with executive functions within critical infrastructures (directors and security coordinators) who are directly responsible for the operation of critical infrastructures. Multiple responses were received from Northern Macedonia, Montenegro, Serbia, Bosnia and Herzegovina and Croatia (colleagues in other countries were contacted but their responses were not received until this text was written). At the third level, oral interviews were conducted with subject matter experts from Croatia and interviews by telephone with experts from Bosnia and Herzegovina. So this qualitative research primarily relates to the analysis of the impact of the COVID-19 pandemic on the operations of critical infrastructures operators in Southeast Europe viewed from the perspective of operators where some of them have asked to remain anonymous.

For the purposes of this brief analysis, we decided to focus on three questions: What are the consequences of the COVID-19 pandemic and crisis on your company's business? What measures have you taken in dealing with the pandemic and crisis to protect and secure your business as much as possible? What situations "surprised" you during the pandemic and crisis, and what do you see as the procedures and processes that needs to be changed both within your company and at the level of the overall national critical infrastructure protection system?

The COVID-19 pandemic and

crisis caused a number of the same or similar reactions from critical infrastructures operators, while in some situations they reacted differently. In the first place, all operators emphasized the care for their employees, which are a key resource in the successful implementation of their activities. They tried to adapt as much as possible to the recommendations of state authorities and their guidelines on health care, which directed them to reorganize working hours, ways of working and business processes at both the operational and management level. All the work that can be done from home is organized in this way and all possible epidemiological measures have been taken in the companies. Some respondents stated that in the first weeks of the pandemic it was very difficult to obtain the necessary protective equipment (protective masks and disinfectants) in the required quantities because they were simply not on the market to buy. Some operators have limited access to their facilities and administrative buildings to the maximum, by limiting contacts, meetings, deliveries and scheduled maintenance to the minimum of necessity. Almost all respondents stated that the pandemic and the crisis affected their business, delivery of goods and services and their billing, which in the short and long term is a business disruption and challenge. Some operators, such as Sarajevogas (Bosnia and Herzegovina's leading gas distribution company), have decided to extend capital plans and investments for another part of the year. Some operators were surprised by the crisis, and some, such as INA Group (Croatian company for refining and

distribution of oil and oil products, part of the Hungarian MOL Group) had a very fresh experience of crisis management due to cyber-attacks to which they were exposed for weeks and step in this crisis with a high level of operational readiness. As issues, some operators occasionally pointed out insufficient coordination with the competent institutions in exchanging information and informing about important activities that they plan to undertake and/or undertook and directly affect the business, provision of services and workspace of the operator. The second challenge, pointed out by some operators, is that the normative framework for critical infrastructure protection in their countries has not been established, thus the system of critical infrastructure protection and coordination of all key actors has not been implemented, and some existing documents that could be acted upon have not been activated, which put them in a situation of great uncertainty and were mostly left to their own devices.

Regarding the measures taken by the operators in dealing with the pandemic and the crisis in order to protect and ensure business as much as possible is continuation of the previous question and answers. Montenegrin Electric Enterprise AD Niksic stated that in addition to all the recommendations of the competent authorities that they have implemented and constantly monitor them – they have strengthened internal communication between management and employees in terms of occupational safety standards, providing support to employees working from home, introduction of new (modern) communication systems for internal and external communication, implementation of technological systems for payment of bills via payment cards through the corporate portal and mobile application, and on-line coordination of key business processes. In addition to all this, the Elektrani na Severna Makedonija (ELEM) (Northern Macedonian electricity production company) operator, has increased contacts and interviews with its own employees to help them as needed. While MEPSO (state-owned electricity transmission system operator of North Macedonia) has taken special measures regarding the operation of the national dispatching center, as it is an essential point

in maintaining the security and stability of the electrical system. The usual system of work of the employees was changed and organized in shifts of 14 days each during which they were isolated within the center to avoid any possibility of their infection. JANAF (Croatian managing an oil pipeline system company) has produced brochures for all its employees on how to act in a crisis and for business partners on how to cooperate with the company during a crisis. Sarajevogas, in addition to all the above, organized reserve (alternative) work positions if the basic ones were "endangered" by the infection, and organized external training of employees by the epidemiological service.

For third question of the analysis, regarding the situations during the pandemic and crisis that "surprised" the operators and what they see as procedures and processes that need to be changed both within the company and at the level of the entire state critical infrastructure protection system – we will not list operators individually to protect their interests but we will present collective answer. Regarding the companies themselves, our interlocutors very sincerely pointed out certain areas that they believe need to be improved and changed. Some believe that it is necessary to reorganize the IT structure and increase the use of digital platforms and tools. Then, harmonization of existing and introduction of new internal processes and procedures for acting in crisis situations that will be adjusted to the needs of the company. Related to the above, is the proposal to introduce new work processes in the organization of work in order to facilitate remote work, because so far it has been an ad hoc measure and administrative regulation of such work. Flexibility as a principle has been highlighted as a need because crises often cause a number of unforeseen situations and conditions, so it would be necessary to introduce more flexibility into certain processes. In the part of public-private partnership with the state, the need for a higher level of cooperation and coordination, adoption of missing laws and bylaws, implementation of existing ones and open dialogue were emphasized, because they manage national critical infrastructures and ensure delivery/maintenance of essential services and therefore the partner relationship is necessary so their business processes could be implemented effectively.

This research has shown the great readiness and efficiency of operators of critical infrastructures and essential services in Southeast Europe in dealing with the COVID-19 pandemic and crisis, which according to the author of this text is higher than what countries have shown so far, but also there is a large room for improvements in a number of areas that are dependent and only feasible in public-private partnerships. The crisis has affected and still affects the business, but according to this research, it is visible that the operators used the crisis as the opportunity to change part of their own business processes as well as detect an additional number of identified lessons, which, if converted into lessons learned can enable a higher level of preparedness, readiness and effectiveness in dealing with future crises.

by Robert Mikac – Director for the South East Europe Region – IACIPP

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

October 19th-21st, 2021
New Orleans, LA, USA
A Homeland Security Event

Are you sure your national infrastructure is secure?

The ever changing nature of threats, whether natural through climate change, or man-made through terrorism activities, either physical or cyber attacks, means the need to continually review and update policies, practices and technologies to meet these growing demands.

Call for Abstracts

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure.

The 3rd Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing America's critical infrastructure.

You are invited to submit an abstract for consideration for inclusion in the conference programme - visit **www.ciprna-expo.com/call-for-papers** for further details.

Join us in New Orleans, LA, USA for the premier event for operators and government establishments tasked with the regions Critical Infrastructure Protection and Resilience.

For further details visit **www.ciprna-expo.com**

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

To discuss exhibiting and sponsorship opportunities contact:

Paul McPherson
(Americas)
E: paulm@torchmarketing.us
T: +1-240-463-1700

Paul Gloc
(UK and Rest of World)
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

Sam Most
(Mainland Europe, Turkey, Israel)
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

The premier discussion for securing America's critical infrastructure

Supporting Organisations:

Media Partners:

Threats to CNI - Annual Assessment – Focus on Ports

In this article, Editor of World Security Report and worldsecurity-index.com, Tony Kingham, gives his annual assessment of current physical threats to CNI, with a special focus on ports and waterside facilities.

Islamist terrorist group, Islamic State's Central Africa Province (ISCAP), a group with links to ISIL, recently seized the seaport of Mocimboa da Praia, in the north eastern corner of Mozambique. The attack was reportedly launched from both sea and land, and over one hundred members of the security forces were reported killed during the assault and the remainder were forced to withdraw, leaving the port in the hands of the terrorists.

Only 40 miles north, and currently under construction, is the US$20billion, gigantic Mozambique LNG export terminal project run by the French oil giant, Total.

Although ISCAP is part of the Cabo Delgado insurgency, intent on establishing an Islamic state, the attack is a reminder, if one were needed, that ports and their infrastructure are vital strategic targets for both state and non-state actors.

90% plus of the world's trade moves by sea and ports are the economic life blood of any nation, or any would-be nation. It is not just the dockside facilities themselves that are vital, oil

terminals, power stations, water desalination plants and even airports are located in or very near ports.

But waterside sites are especially vulnerable.

What makes ports and waterside CNI so vulnerable is the multi-dimensional nature of their threat environment. Attacks can be launched from land and sea, both surface and subsurface, and increasingly from the air by attack drones. Or all of them at once!

I am not suggesting that a terrorist attack on the scale of Mocimboa da Praia is likely elsewhere, anytime soon, but it does illustrate how vulnerable ports are and that they are considered high value targets.

Ports are, by their very nature, busy bustling places with vehicles and marine traffic coming and going continuously. Making security incredibly challenging!

So, what are the threats?

From the air

In recent years, a combination of technological developments and geopolitical circumstances has made attacks on CNI, not just a threat but a reality.

The terrorist use of drone technology to attack coalition forces in Syria and Iraq was pioneered by ISIL and continues, with regular reports of attacks against Syrian and Russian forces. More recently Iranian backed Houthi separatists have deliberately targeted airports and oil and gas facilities in both Saudi Arabia and the UAE with drone attacks.

The Qasef1 UAS's systems used by the Houthi's are based on Iranian Ababil-2 airframe and are a technologically significant step up from the off-the-shelf systems available to other terrorist organisations (unless they are affiliates of Iran), but that doesn't lessen the threat from drones.

During the war in Afghanistan, the average Improvised Explosive Device (IED) weighed in at around 23 kilos and was usually of the Home Made Explosive (HME) variety i.e. primarily made of cheap and freely available substances like ammonium nitrate fertiliser and sugar (ANS) plus a small detonating charge and a trigger mechanism.

HME IED's of that size have the power to destroy 18-ton armoured vehicles throwing them several feet into the air.

There are plenty of off-the-shelf drones that can carry that sort of payload and more, such as the GAIA 190MP-Heavy Lift Drone, which claims to lift 35kg, and fixed wing systems like the GATH-y007 that claim up to a 40kg payload. They are both available for purchase on the internet.

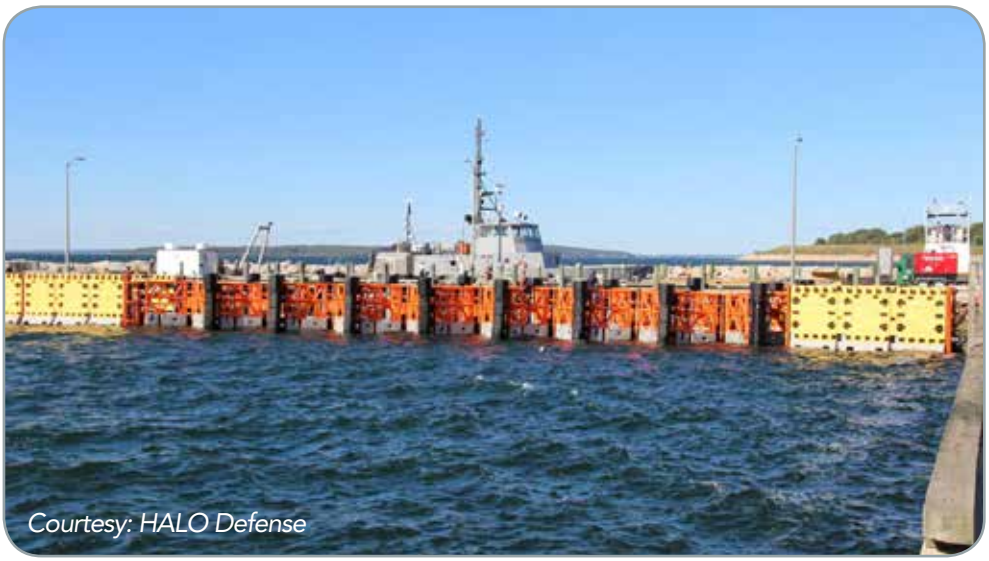
These systems carrying explosive payloads are effectively cruise missiles.

We all recently witnessed the devasting explosion in the port city of Beirut, caused by the accidental detonation of stored ammonium nitrate. How many more ports deal with bulk shipments of ammonium nitrate, or store it, even temporarily? These stores, or the vessels themselves during loading and unloading, could be deliberately detonated by a drone attack. All you need is a little inside knowledge about what, where and when these cargoes are delivered.

Drones are difficult to detect anyway, but in the cluttered environment of a busy port it is even more problematic. Many port facilities are surrounded by commercial buildings and suburban homes, which is what made the Beirut blast so devasting, not just to the port and city but to the whole Lebanese economy.

This urban clutter makes detecting drones before they reach the port or CNI perimeter extremely difficult.

Many anti-drone systems rely on RF signals for detection and jamming but the terrorist may use autonomous drones using GPS or inertial navigation systems (INS) to counter RF. GPS spoofing systems can jam or seize control of drones relying on GPS for guidance, but won't work on INS guided systems once it is in flight. Other drawbacks of these systems are that they are typically short range, and both can interfere with legitimate signal traffic in the area, so cannot be used in a continuous mode in urban areas.



Courtesy: HALO Defense

However, both systems are valuable

International Association of CIP Professionals

www.cip-association.org

Join the Community and help make a difference

Dear CIP professional

I would like to invite you to join the International Association of Critical Infrastructure Protection Professionals, a body that seeks to encourage the exchange of information and promote collaborative working internationally.

As an Association we aim to deliver discussion and innovation – on many of the serious Infrastructure - Protection - Management and Security Issue challenges - facing both Industry and Governments.

A great new website that offers a **Members Portal** for information sharing, connectivity with like-minded professionals, useful information and discussions forums, with more being developed.

The ever changing and evolving nature of threats, whether natural through climate change or man made through terrorism activities, either physical or cyber, means there is a continual need to review and update policies, practices and technologies to meet these growing and changing demands.

Membership is currently FREE to qualifying individuals - see **www.cip-association.org** for more details.

Our initial overall objectives are:

- To develop a wider understanding of the challenges facing both industry and governments
- To facilitate the exchange of appropriate infrastructure & information related information and to maximise networking opportunities
- To promote good practice and innovation
- To facilitate access to experts within the fields of both Infrastructure and Information protection and resilience
- To create a centre of excellence, promoting close co-operation with key international partners
- To extend our reach globally to develop wider membership that reflects the needs of all member countries and organisations

For further details and to join, visit **www.cip-association.org** and help shape the future of this increasingly critical sector of national security.

We look forward to welcoming you.

John Donlon QPM, FSI
Chairman
IACIPP

as counter unmanned aerial systems (CUAS) because they are passive, so no licence is required, and they can be turned on in the event of a confirmed threat. Some can also triangulate to identify the drone and controllers' position.

That means radar detection, coupled with electro-optical and infrared systems (EOIS) are a necessity, as radars and EOIS provide continuous, long-range identification and tracking of multiple targets, whether they are autonomous or guided.

However, no system is fool proof and a clever attacker will have reconnoitred the target and may choose a low-level approach through busy streets to avoid detection, or at least delay detection and reaction times. So, careful positioning of sensors is critical and requires a detailed threat assessment to establish likely attack routes, identify dead ground etc.

When it comes to interdiction there are a whole raft of technologies, including RF and GPS jamming, anti-drone nets fired from launchers or other drones, capture drones and even birds of prey. In fact, too many to list here.

At the national security end of the spectrum there are, High Power Microwave (HPM) devices, that are designed to generate an Electromagnetic Pulse (EMP) to disrupt a drone's electronics and lasers that again destroy electronics. And as the last resort, there are kinetic systems such as guns and missiles.

Not for the first time in this article will I say that there is no single technological solution to the drone threat, so a layered approach with each technology being used to its strengths is optimal, integrated into one overall security system.

On the ground

In terms of landside security threats, nothing much has changed. Still the most likely terrestrial threat comes from the terrorist's old favourite, the vehicle borne improvised explosive device (VBIED). Why? Because of their potential payload and mobility, and their ability to blend in with regular traffic, until it is too late.

So, the key to security is limiting access points. Ensuring authorised access and VBIED mitigation methods such as serpentine barriers and vehicle stoppers like pop-up vehicle barriers, and inspections technology such as Under Vehicle Inspection Systems (UVIS) , Non-Intrusive Large Scale, X-Ray Detectors and Motion Detection Technology.

The extended perimeters of ports are a problem in that regular fences do not pose much of a problem to heavy goods or construction vehicles. To mitigate against a VBIED attack on the perimeter, old technology is probably best, such as a ditches, bunds, or concrete barriers.

Although it may not seem a high probability, single or teams of saboteurs should not be discounted, especially in the wake of Beirut blast. Terrorist groups cannot have failed to have noted the devastation and publicity the blast generated. It may start them thinking about the sheer number of flammable and explosive goods passing through ports that could potentially be detonated by a relatively small IED.

So, as well as fences and bunds, radar, CCTV, IR, radio frequency monitoring, seismic ground sensors, proximity sensors and microwave sensors, could all form part of that layered security approach.

Waterside

The waterside security environment in ports is incredibly complex. There is a surface, sub-surface, river and/or seabed and waterside environment, that may not only include the port facilities themselves but many miles of estuary and/or coastline. All of which must be secured.

Ports raison d'être is to facilitate the free flow of maritime trade, which means keeping the goods, commodities and people moving, which makes for a difficult balance. Ports are often public facilities, meaning, in addition to merchant vessel traffic there could be numerous ferries, fishing boats, pleasure boats and workboats, constantly coming and going.

So, what are the threats?

Attacks from small craft has a long history. Probably the most famous of which was in October 2000, when the USS Cole, an American guided missile destroyer berthed alongside in the port of Aden, was attacked by two suicide bombers in a fibreglass boat. The explosion left a gaping hole in the port side and 17 sailors dead.

Since then, the number of attacks using small craft are again too numerous to mention but in May 2019, four commercial ships were damaged in the Fujairah anchorage in the Gulf of Oman. The ships were anchored in UAE territorial waters for bunkering in Port of Fujairah.

The findings of an Emirati-led international investigation into the attacks stated that a sophisticated and coordinated operation by divers from fast boats utilized limpet mines to breach the hull of the ships, concluding that a "state actor" was the most likely culprit.

A month later two oil tankers were attacked near the Strait of Hormuz while they transited the Gulf of Oman. They were attacked allegedly with limpet mines or flying objects, sustaining damage.

The use of divers in the May attack clearly demonstrates that divers remain a real threat, whether that is by attaching limpet mines directly to vessels or by laying mines on the seabed. In a port or estuary, the impact of an attack like this would be huge, especially if the perpetrators are able to "hole" the vessel below the water line and sink it in an estuary or port entrance.

Use of explosive-laden unmanned surface vessels (USV's) launched by the Iran-backed Houthi's has been a new feature of the current conflict in the Yemen. According to a 2015 U.S. Army assessment on threats from unmanned craft, "utilizing suicide drones is an asymmetric strategy which both allows Iran to compete on an uneven playing field and poses a risk by allowing operators to pick and choose targets of opportunity" and by extension, their proxies. Information about their success or otherwise is difficult to assess, but as with all such innovations, it will not have gone unnoticed by other terrorist groups.

The last category of threat are submersibles and semi-submersibles, both manned and unmanned. The US Coast Guard and partner organisations in the region, are almost routinely interdicting narco-subs heading for the US. Most of these are of the semi-submersible variety but are still very difficult to detect in that transition zone between surface and sub-surface. Most of them are made in crude jungle workshops in Central and South America, which puts them well within the capabilities of most terrorist organisations. According to a report in Forbes magazine, last November the first documented 'transatlantic' narco-submarine reached Europe. This marks a significant step up in capability and given the known links between organised crime and terrorists, it is a worrying development.

Once again, a layered approach to security including radar, sonar, electro-optics and diver detection systems are essential for high risk ports. It may prove necessary to segregate especially sensitive or vulnerable areas of the port, so floating security barriers, anti-diver nets and gates may be required. Halo Defense in the US have been particularly successful with sales of their waterside security barrier to the US Navy and most recently to the Bahrain military complex. Companies like Sonardyne and have successfully deployed diver detection sonar worldwide but other systems include Armelsan and Echorium Diver Detection from Koç Information and Defense Technologies.

Once detected, non-lethal and lethal mitigation measures need to be rapidly deployed, such as acoustic systems like WG Enforcer, which is designed to bring the diver to the surface, and of course depth charges.

The combined small craft and diver attack in May 2019, also illustrated another difficulty facing port security professionals. An innocent looking small surface craft being monitored by radar may not be flagged as a threat,

however if a diver covertly goes over side or a mine is dropped and is picked up as a sonar threat, that surface vessel should automatically be flagged as a surface threat, because it may contain more divers, mines or be packed with explosives. But that only happens if both systems, radar, and sonar are properly integrated. The transition between environments and systems is a key difficulty, especially as port authorities procure multiple systems and technologies, air, land, and sea from different OEM's and attempt to integrate them with legacy systems.

One company, MARSS Group specialises in solving this problem with their NIDAR Command and Control System. Developed in collaboration with the European Union, defence agencies and NATO, it is already deployed protecting high-risk ports. NiDAR is an open architecture C2 system that can integrate a number of new and legacy systems and sensors; air land and sea, surface, and sub-surface, into one touch screen smart system to manage a whole facility. AI and software algorithms autonomously and intelligently detect, classify, and respond to multiple air, surface and underwater objects determining potential threat levels, triggering alerts and controlling threat mitigation measures.

Finally, it must be said that there are any number of other possible threats, but we do not have time to cover them all within the confines of this article. However, as I mentioned at the beginning of this article, the threat to ports and CNI is no longer theoretical, but a clear and present danger. So, if you are involved in national security or directly involved in port and CNI security and haven't undertaken a major security review of your facility in the last couple of years. Perhaps it is time!

Transnational Tentacles - Global hotspots of Western Balkan Organized Crime

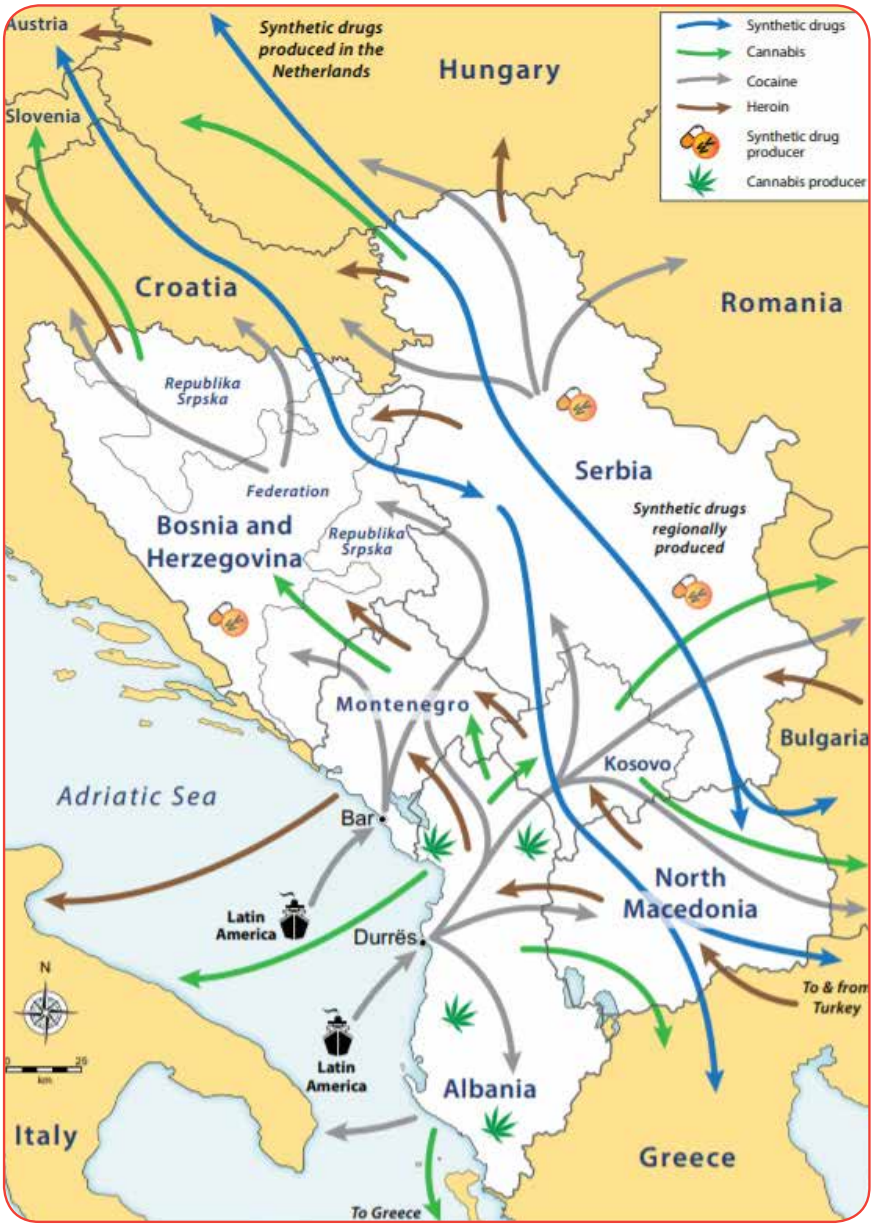
by Walter Kemp

The following is an extract from a recent report published by the The Global Initiative

The report has set out to show where there are global hotspots of activity by criminal groups from the Western Balkans. It has looked at case studies in Latin America, Western Europe, Turkey and South Africa, and touched on Australia. There are some similarities between these hotspots, but also important differences. Many of the hotspots are linked to a legacy of the dramatic events that took place in Yugoslavia and Albania in the 1990s, but others have more to do with more recent developments and opportunities that have opened up because of political changes and globalization.

Most hotspots have sizeable diasporas of people from the Western Balkans, but some do not (such as those in Latin America). Some hotspots have relatively weak institutions and criminal-justice systems, or were attractive to criminal groups during a time of transition, but others (such as Western Europe, Australia and Turkey) do not.

Almost every hotspot identified is linked to the drug economy; either supply (in Latin America), transit (Turkey) or distribution and retail (Western Europe and Australia). Smuggling of migrants and cigarettes has also been highlighted, particularly in the case of Turkey. South Africa is an



outlier. It seems to have been a hotspot in 2018 and 2019 because of a settling of old scores among a small group of people somehow connected to the assassination of Arkan.

Yet there are indications that it is becoming a hotspot for the trafficking of cocaine, including with the involvement of groups from the Western Balkans. In most hotspots, the criminal groups from the Western Balkans have moved up the value chain in the past 20 years. Men from small towns in the Western Balkans (including from hotspots identified in an earlier report by the GI-TOC) are now organizing multiple-tonne shipments of cocaine from the jungles of Latin America through some of Europe's busiest ports to the streets of its capitals. Sailors from small Balkan ports are using yachts to ship drugs to South Africa and Australia, or migrants from Turkey to Western Europe. Brokers from the Western Balkans are cutting deals with some of the biggest Latin American cartels, the Italian mafia and well-established Turkish criminal groups. They are now in the premier league of crime. Most of the criminal activity in the hotspots is non-violent.

Again, South Africa is the outlier, but that seems to be because of bloody infighting related more to vendettas than competition over a criminal market. There has also been some recent violence in Italy, which suggests competition with groups that may be taking issue with the ascendency of Albanian networks in major cocaine markets such as Rome. The other notable exception is violence associated with the bloody feud between the Škaljarski and Kavacki clans.

But with the exception of a few hits in Western Europe, this violence mostly occurs in Serbia and Montenegro rather than the hotspots abroad.

Characteristics of the groups

It is difficult to make generalizations about the criminal groups from the Western Balkans operating in global hotspots, partly because there is no uniform model and partly because of a dearth of information. It is clear, however, that there is no Balkan cartel or even an Albanian mafia.

Such descriptions suggest a degree of organization and cohesion that does not exist. Rather, there are a number of groups and networks that sometimes cooperate with one another and/or with local partners. Western Balkan criminal groups operating in global hotspots are seldom ethnically homogeneous, although Albanian groups have traditionally preferred to work with people from their own clan or community. There is also still a tendency for criminals from the Western Balkans to work with others from the region. But cases examined in this report suggest that criminal groups from the Western Balkans operating abroad are highly adaptive and are willing and able to work effectively together with people of a wide range of nationalities.

The lack of violence displayed by

groups from the Western Balkans suggests that they are either pragmatic and have found ways to get along with local partners and other groups, or they feel confident in their ability to control certain markets. The latter can be attributed in some cases to alliances with powerful partners, a reputation for violence, sufficient resources to ensure impunity in countries with weak criminal justice systems, as well as a protective umbrella back in their home country.

Some members of these groups – particularly from Serbia and Montenegro – still have a legacy from the Yugoslav wars of the 1990s, but many of that generation of criminals are either dead, in jail or out of the game. The exception is in South Africa, where there happened to be a cluster of people (mostly over 50 years old) with connections from the early 2000s who, paradoxically, wanted to escape their past. There are others who are part of a 'second generation' who either left the Western Balkans as children, or who were born abroad. In some cases, they have links to groups from the Western Balkans, but in other cases they are branded as Balkan criminals, even though their only link to the region is their family name.

Today there is a generation of younger, professional criminals who have good language skills, are adept at using technology, park their money offshore or in cryptocurrencies, and profit from globalization. They have gone from the Yugosphere to being citizens of the world. They are the global equivalent of what used to be referred to in the Balkans as 'controversial businessmen'. The new generation of traffickers have become tech savvy to avoid law-enforcement surveillance. For instance, they use GPS for deliveries of drugs or to navigate trafficking routes. They use satellite phones, Voice over Internet Protocols (VoIP), and encrypted internet-based communications that are hard to intercept. And they are active on the darknet and increasingly use cryptocurrencies, such as Bitcoin, that are hard to trace.

An unbeatable business model

One of the most striking conclusions of the report is the upward mobility of criminal groups from the Western Balkans. Within 20 years, they have gone from being small-time couriers or crooks trying to escape instability and underdevelopment to becoming big-time distributors in some of the biggest drug markets in the world. They have positioned themselves close to the source of the world's biggest supplies of cocaine and heroin, and – in the case of Albanians – are sometimes even the producers of cannabis. They are also active in the retail trade, particularly in Western Europe due to access to various ports in the EU such as Antwerp, Amsterdam, Hamburg, Valencia, Algeciras and Piraeus. They also have links to street-level distributors, including compatriots from the Western Balkans. This allows them to drive down prices, pass the savings on to consumers, deliver good quality at a fair price, and thereby knock out the competition. As a business model, it is unbeatable. If they continue to play it right, this business model will continue to be lucrative because supply and demand for cocaine, heroin and cannabis are high.

The development of this niche as an end-to-end service provider has not developed by chance. Criminal groups from the Western Balkans have shown a willingness to take risks and to seek out and exploit opportunities, for example using new routes and new technologies. They have built the respect of local partners on both ends of the supply chain. They have shown themselves to be innovative, entrepreneurial and adaptive.

Enabling factors

The report has highlighted a number of factors that have enabled criminal groups from the Western Balkans to operate abroad. As noted, in some cases it is weak governance and corruption in countries where they operate. Another factor is their ability to use several identities and therefore avoid detection.

Limited container security is a problem, either due to corruption or the sheer volume of containers going through some ports. It is quite possible that some of the illicit goods are being shipped through free economic zones: this makes them hard to interdict. In some cases, weak border and customs control, as well as lax maritime security, are making smuggling relatively low risk.

As mentioned, technology is an enabling factor for the groups described in this report: for example, the use of encryption, cryptocurrencies and GPS tracking. The financial system also seems to be an enabler for the flow of money of some of these groups. How else could it be possible to move and invest so much

World Border Security Congress

24th-26th November 2020

ATHENS, GREECE

www.world-border-congress.com

Building Trust and Co-operation through Discussion and Dialogue

REGISTER TODAY

Register for your Delegate Pass online Today

Greece lies at the crossroads of East and West, Europe and the Middle East. It lies directly opposite Libya so along with Italy is the primary destination for migrants coming from that conflict zone and is a short boat trip from Turkey, the other principal migrant route for Syrians fleeing there conflict there.

Greece has over sixteen thousand kilometres of coastline and six thousand islands, only two hundred and twenty-seven of which are inhabited. The islands alone have 7,500 km of coastline and are spread mainly through the Aegean and the Ionian Seas, making maritime security incredibly challenging.

The sheer scale of the migrant crisis in late 2015 early 2016 had a devasting impact on Greek finances and its principle industry, tourism. All this in the aftermath of the financial crisis in 2009. Despite this, both Greece and Italy, largely left to handle the crisis on their own, managed the crisis with commendable determination and humanity.

With their experience of being in the frontline of the migration crisis, Greece is the perfect place re-convene for the next meeting of the World Border Security Congress.

The World Border Security Congress is a high level 3 day event that will discuss and debate current and future policies, implementation issues and challenges as well as new and developing technologies that contribute towards safe and secure border and migration management.

The World Border Security Congress Committee invite you to join the international border security and management community and Apply for your Delegate Pass at **www.world-border-congress.com.**

We look forward to welcoming you to Athens, Greece on March 31st-2nd April 2020 for the next gathering of border and migration management professionals.

www.world-border-congress.com

for the international border management and security industry

Confirmed speakers include:

- Jim Nye, Assistant Chief Constable – Innovation, Contact & Demand & NPCC Maritime Lead, Devon & Cornwall Police
- Dr Olomu Babatunde Olukayode, Deputy Comptroller of Customs, Nigeria Customs
- Sanusi Tasiu Saulawa, Deputy Superintendent of Customs, Nigeria Customs Service
- Heiko Werner, Head of Security Group, Federal Office for Migration and Refugees, Germany
- Gerald Tatzgern, Head of Joint Operational Office, Public Security Austria
- Peter Nilsson, Head of AIRPOL
- Wayne Salzgaber, Director, INTERPOL Washington
- Tatiana Kotlyarenko, Adviser on Anti-Trafficking Issues, OSCE
- James Garcia, Assistant Director, Cargo & Biometrics – Global Targeting Advisory Division National Targeting Center – U.S. Customs and Border Protection
- Valdecy Urquiza, Assistant Director – Vulnerable Communities – INTERPOL General Secretariat
- Hans Peter Wagner, National Expert, Senior Chief Inspector, Federal Police
- Mile Milenkoski, Senior adviser, Department for borders, passports and overflights, Ministry of Foreign Affairs, Republic of North Macedonia
- Manoj Kumar, Second in Command, Indian Border Security Force
- Rear Admiral Mohammed Ashraful Haque, Director General, Bangladesh Coast Guard Force

Supported by:

OSCE Organization for Security and Co-operation in Europe

European Association of Airport and Seaport Police

AFRICAN UNION

ISIO

International Association of CIP Professionals

NSeRC

Media Partners:

BORDER SECURITY REPORT

WORLD SECURITY REPORT

World Security-index.com

money? Do banks and real-estate companies really know their customers?

A key consideration is that some of the underlying factors that made people from the Western Balkans vulnerable to organized crime in the 1990s still exist: lack of employment opportunities, corruption, inequality, frustration with the domestic political situation and the slow process of EU accession. If these are not addressed, there will continue to be a pool of young people in the Western Balkans or the diaspora willing to risk a life of crime.

Law-enforcement cooperation

While criminals from the Balkans demonstrate the benefits of transnational cooperation, the report also shows that law-enforcement agencies can work effectively together. Operation Balkan Warrior was a joint operation between the DEA, the Serbian intelligence agency and police in Uruguay and Argentina that helped take down Darko Šarić in 2010.

There have been several other successful operations involving law-enforcement agencies from the US, Western Europe, Latin America and the Western Balkans. SELEC has proven to be a useful coordination mechanism for carrying out joint investigations. Part of SELEC's added value is that Turkey is a member. There has also been good cooperation at sea, such as the drug bust in February 2020 off the coast of Aruba that was part of a joint operation between Serbian, Montenegrin, Dutch and British law enforcement agencies. Indeed, between 2018 and 2020, the number and size of drug busts seemed to be increasing, either as the result of greater cooperation between law-enforcement agencies or as a reflection of an increased volume of trafficking, or both.

EUROPOL plays a key role. On 11 March 2020, for example, EUROPOL announced that it had helped to dismantle a large Balkan criminal network that was trafficking drugs, mainly cocaine, from Latin America to Europe. A complex international investigation, launched in 2017, intercepted a catamaran smuggling 840 kilograms of cocaine being shipped from the Caribbean to Europe. Four crew members of Bosnian, Montenegrin and Serbian nationalities were arrested in 2018, and several other members of the group were arrested on 10 March 2020.

This shows how EUROPOL can facilitate the exchange of information, provide coordination support and analyze operational information against its databases to give leads to investigators. This approach has also been applied to countering the trafficking of human beings and cigarettes, as well as smuggling of migrants in the Western Balkans.

Eurojust is helping countries of the Western Balkans to strengthen capacity and provides assistance in prosecuting cases. More generally, since prosecution is often the weakest link when dealing with cases of serious organized crime, the support of other countries can be helpful, including extradition. In some cases, liaison officers from police departments in the Western Balkans have been placed in countries of origin to help identify suspects and help with analysis. Such cooperation has proven successful.

Bilateral cooperation is also necessary. A good example is the cooperation between Italian and Albanian law-enforcement agencies, including joint operations. Italy, together with the US and a number of EU countries, has also been supportive of the process of reforming the Albanian criminal-justice system. There has also been cooperation in the context of the EU's Instrument for Pre-Accession Assistance, which provides EU candidates with financial and technical help. In some cases, this has led to successful operations against organized-crime groups as well as seizures of criminal assets. The investigations carried out have covered the entire spectrum of organized-crime manifestations – from trafficking in human beings, arms and drugs to terrorism and money laundering – and have been conducted both in the Western Balkans and in the countries of the EU, as well as sometimes in other countries. Cooperation with the EU could be even more effective if countries of the Western Balkans had access to the Schengen Information System. This would enhance and speed up the ability of police and border guards to

identify persons of interest.

INTERPOL plays a key role in terms of coordinating joint actions. For example, in January 2020 it led a major operation against human trafficking and the smuggling of migrants in the Balkans called Operation Theseus. As a result, 72 suspected traffickers and 167 migrant smugglers were arrested, 89 victims of human trafficking were rescued and 2 000 migrants identified. INTERPOL's Red Notice system is also crucial for identifying criminals. It is interesting to note that INTERPOL had an entire project devoted to tracking the Pink Panthers.

More could be done, particularly in terms of enhancing cooperation between law-enforcement agencies in countries of supply and demand, and also by involving colleagues from the Western Balkans. There is also a need for a greater focus on maritime security (particularly through intelligence-led operations), and tackling container security, for example, by making more effective use of the UNODC–World Customs Organization Container Control Program. And there is an urgent need to improve mutual legal assistance between countries of the Western Balkans and global hotspots where criminal groups from the Western Balkans are active.

Since criminal groups are financially motivated, and given that money is the source of their strength, more needs to be done to look at the financial flows of Western Balkan groups operating abroad. To increase risks and reduce benefits, greater cooperation is needed in tracking money laundering and recovering stolen assets. The legal frameworks exist in the UN Convention against Transnational Organized Crime (UNTOC) and the UN Convention against Corruption (UNCAC).

The key is practical cooperation. Otherwise this money could be used to buy power, or pervert national economies. Indeed, if there will be a liquidity crisis as a result of the COVID-19 virus, the leverage of criminals with significant amounts of cash could have a major influence on business and politics.

In short, if Balkan crime has gone from the inside out, a large part of the solution will have to come from the outside in – through international cooperation. As an Italian prosecutor said, 'just as they ally themselves with each other, so we must cooperate together'.

A multi-layered approach

Dealing with the impact of criminal groups from the Western Balkans operating abroad will require responses at different levels. Within the Western Balkans it is important to strengthen the resilience of society against the factors that enable crime to prosper. This would reduce hotspots of crime at home and abroad. The reform of the criminal justice system in Albania is a good example. It may be slow and arduous, but this is an opportunity to bring in a new generation of criminal-justice officials, and to build greater integrity and trust in the system.

More broadly, in all countries of the region, it will be important to have effective institutions, not only good legislation. And it is vital to create more jobs and viable livelihoods, particularly among vulnerable groups (such as the youth) in vulnerable regions. Here donors have a role to play as well in addressing the factors that cause underdevelopment, marginalization and brain drain. This could become even more acute in relation to the economic fallout of COVID-19.

Western European countries have a key role to play in reducing demand for the goods and services that are fuelling crime in the Western Balkans. Indeed, with the exceptions of Australia and South Africa, all of the trafficking flows that criminal groups from the Western Balkans are profiting from are directed at the EU and the UK. While some critics and sections of the media may sound the alarm about criminal groups from the Western Balkans, few point out that they are the delivery service for

Western Europe's illicit markets.

Furthermore, leaving countries from the Western Balkans without a European perspective is not going to improve the situation. People from the Western Balkans who wanted to move to the EU are already there – including criminal groups, as highlighted in this report. If some of them turned to a life of crime because of a system that they feel let them down, why deepen the vulnerabilities of that system? Instead, the challenge should be to address the conditions that created the vulnerability in the first place.

It is a tall order, but more should also be done to strengthen resilience in countries of supply. Countries that are major markets for Latin American cocaine have a self-interest in strengthening criminal-justice systems and sustainable development in countries such as Ecuador, Colombia and Peru. Furthermore, addressing the issue of criminal groups from the Western Balkans without reducing the market forces that keep them in business will simply see them replaced by groups from somewhere else. Indeed, as noted in many of the hotspots examined in this report, they are not the major players in the drugs trade.

The role of civil society

Civil-society actors both in the Western Balkans and abroad have a key role to play. They should continue to push for effective governance and institutions, and promote a culture of lawfulness. And they should work with governments to ensure that there is space and freedom to give a voice to those – particularly in the media, civil society and concerned citizens – who believe in a society free of crime and corruption.

Otherwise, disillusionment with politics and a lack of faith in future opportunities in the formal economy will continue to make young people across the Western Balkans vulnerable to either going abroad or joining criminal groups (or both). Co-nationals in the diaspora have a stake in promoting a culture of lawfulness because the activities of criminal groups in their midst gives them a bad name too. Most members of the diaspora do not benefit from the criminal activity of their compatriots, and some even suffer from it. Indeed, many of them left the Western Balkans because of crime and instability – they do not want it on their doorstep again.

Violence and silence

Finally, it is important to keep the spotlight on the issue. Criminal groups profit more by silence than violence. Although attention is often focused on criminal groups when there is violence, this is usually a sign of competition or disruption in a market, whereas a highly efficient market is one that operates smoothly in silence.

Thus far there has been little understanding of the role of Western Balkan groups outside of their home region, as well as the links between them. This report has had the advantage of being based on information from experts (including journalists, academics and members of civil society) in the global hotpots, and a wide range of sources.

That said, in many cases the providers of that information noted that there is a lack of data and analysis about the role criminal groups from the Western Balkans play in organized crime. Problems include a lack of disaggregation of data on the basis of ethnicity, limited knowledge of the Western Balkans, the use of multiple identities by the perpetrators (including through passports from EU countries), and the view that criminals from the Western Balkans are not a major threat to the country in question.

Nevertheless, perhaps this report can contribute to a greater understanding of the roots, characteristics and impact of this problem in order to help stimulate remedial action.

In conclusion, this report shows the role of groups from the Western Balkans in hotspots around the world. More action is needed to reduce the supply and demand of the goods that these groups deliver, and to disrupt their activities. Otherwise the tentacles of criminal groups – including those from the Western Balkans – will continue to wrap themselves around the globe.

Download the full report at https://globalinitiative.net/wp-content/uploads/2020/07/Transnational-Tentacles-Global-Hotspots-of-Balkan-Organized-Crime-ENGLISH_MRES.pdf

This report is published by The Global Initiative, a network of more than 500 experts on organised crime drawn from law enforcement, academia, conservation, technology, media, the private sector and development agencies. It publishes research and analysis on emerging criminal threats and works to develop innovative strategies to counter organised crime globally.

A word from the Chairman

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

International Association of CIP Professionals

National Preparedness Month - USA

In the United States the Department of Homeland Security (DHS) have various months of the year dedicated to focus on their various missions. The month of September deals with the subject of Preparedness (October will be Cybersecurity and November, Critical infrastructure Protection).

National Preparedness month is recognised each September in the USA to promote family and community disaster planning now and throughout the year. It is also a time for government's, organisations, and emergency planners to reflect on their preparedness for the disasters they may face in the future whether they be natural or man-made.

In the last edition of the World Security Report I spoke about how the scale of the current coronavirus situation seems to have caught us all by surprise (even though warnings about a looming pandemic have been there for decades) and how we should delve deeply into the lessons that have been learnt and those that are continually emerging. We need to ensure, at a global level, that those lessons are both shared and acted upon. There is, in my opinion, no better way to prepare for the future than that of learning from the past.

2020 continues to be an incredibly difficult year for the world. Just as a number of countries were emerging from national 'lockdowns' and parts of the economy were showing some signs of recovery, there were some small green shoots of hope on the horizon. Then we started to see an increase in cases, those testing positive for coronavirus, not just in one country but across many and this has obviously caused concern triggering new restrictions to be put in place.

In many cases, disasters don't come with much warning, but I would like to think that we are ready, properly prepared even, for a second wave, particularly, as on this occasion we do have a degree of notice. Coronavirus is, as commentators suggest, the most significant international public health challenge faced in a generation. If we look back in history the last such occurrence was the influenza pandemic in 1918. At that time nations recorded between one and three waves and notably evidence suggests that the second and third waves were more impactful than the first.

That is not to say that will be the case this time. As an international community great effort is being made to develop a vaccine and to understand how to manage such a pandemic within our daily lives. But we must be prepared for that next stage, anticipate its impact, and seek to reduce, if we cannot fully prevent, the harm that it will cause.

Coronavirus is today's emergency management challenge and I think future reviews on the management of this emergency will be less than complimentary on our preparedness for this first wave of the pandemic. Let us hope that as those reviews move into looking at the response to any subsequent occurrence it will highlight that governments and experts came together and both shared and acted upon lessons learnt and demonstrated a more significant level of preparedness.

I hope that you and yours stay safe and healthy and wish you all the best during these troubled times.

John Donlon QPM FSyI
Chairman IACIPP

The IACIPP Poll

The results are in! Responses to the recent poll give the following insight.

Q. How Often Does Your Organization Conduct Background Screening on Employees?

- We don't check employee backgrounds - 0%
- We currently don't conduct background screening, but have plans to do so in the future - 9%
- Only upon the hiring process - 27%
- Less frequently than once a year - 55%
- Every six months - 0%
- Once a year - 9%

Security Industry's Master Disablement Plan for CV-19

The HIM method and Tools that this work is based upon, were conceived, researched, and are presented herein by Juan Kirsten (HIM). These methods are based on four manuscripts and/or e-connect tools which have been reviewed by Prof. Larry Barton/ Emergency Management and Disaster Planning (USA), Prof. Rommel Manwong/Criminology and Security Studies (Philippines), Dr Katerina Poustourli Pre-normative Security Research (Greece), Dr Declan Garrett/Security Training (United Kingdom),and Dr Gavriel Schneider (Australia), and other seasoned non-academics.

This work is a simple solution to disabling COVID-19. COVID-19 is in theater and will be an active biological threat until such time a cure is discovered, and the population is inoculated. Therefore, the infectiousness of the disease dictates that many people will be infected to the extent that all people must be tested, monitored, and managed daily. This calls for mass mobilization and focused concentration by all stakeholders using the same methods and working in sync to limit the level of collateral damage.

Situation

- The Health department have set protocols to 'chemically' test and in addition for hygiene and social practises for cv-19.
- Mobile phone cv-19 awareness tech in theory may work however, the length of pandemic life- time

plus the known and unknown impacting issues may not derive the desired results.

• The Security Industry views the situation differently and considers that [they] are dealing with an active biological threat and therefore are conscious of unique challenges that could influence increased infections. Therefore, they have a different comprehension of the situation, the specific objectives to be achieved and security protocols that must be used. The security sector and industry can electronically 2nd tier test millions of people. Furthermore, they have the semi-and skilled manpower to orchestrate the managed flow of people for quarantine.

Security success depends on the level of situational awareness of the decision-makers (people) on the ground and their reaction speed. When the situation talks to a pandemic, then reaction speed must be highly proactive with distinctive objectives.

It is impossible to 'chemically' test each person every day because of the infectiousness of the virus. However, the security sector can assist with millions of people that must be tested many times a day for cv-19, which could easily be activated and achieved. This means that once a person has a high temperature then we are aware of the situation.

Both the health and security sector must be working in sync together towards the same goals, whereas the private security industry (with no policing powers) assists with 2nd tier testing, identifying people of concern and directing them towards the authorities (medical and mental institutions or quarantine centres)

When people leave their homes and use public transport then their temperature will be monitored, when they walk into a store or a building or anywhere – their temperature will be taken. Specific protocols for the instruments must come into session because the instruments are only as good as the users. Furthermore, not all equipment and technology may be advertised authentically or is reliable.

The problems are in the management and containment of the people that are in a state of anxiety and despair, meaning that they could react differently from their norm. This situation must consider using distinct protocols by the security departments because cv-19 is considered as an active biological threat in theatre with life impacting and deadly outcomes. For example, the layering of the manpower must be by layering appropriate soft and hard skills using relevant and unique skill-protocols.

Identify - Contain - Isolate - Rejuvenate

The objective for the security sector is simple, to identify a person that is infected, direct them to an isolation area and summon the appropriate authorities to assist the person in their quarantine.

Stated earlier, to identify the person of concern, technology and equipment is used. Companies must purposely purchase relative, reliable, and authentic equipment and technology. The manufacturers are running onto the market with temperature, fever detection, etc. Major issues are being currently discovered (such as false advertising) therefore it is vital to check before purchasing or upgrading verify the authenticity of equipment and technology.

There must also be consideration for where best to place certain technology/equipment. It does not help anybody if the users are not obtaining the desired results or achieving specific objectives by using the equipment or technology. This information must be considered when compiling the protocols.

Decision-making in this pandemic does give leeway to reaction speed. Decisions made during a pandemic is quite unlike other scenarios where decision-making may be timeously introduced. There is no room for emotional issues regarding fears of failure, egos, or any other irrelevant

agendas. Reaction speed takes precedence and one would have to live with the consequences. Do rather do something than nothing at all!

When a person of concern is identified then they would need to quarantine. Some will voluntarily participate while others will be reluctant, unable or be unwilling to do so. The crowd reactions overall would be unlike any other before which calls for specific protocols by layering the skills accordingly.

The biological threat must be isolated and contained until such time it is not a threat. Consequently, the faster infected people are isolated and healed the better. When the person is infected and refuses to be contained then that person is a high threat that is weaponized and must be into forced quarantine.

The biggest nightmare is not knowing what is truly happening on the ground therefore, security related investigative thinking applies more so than criminal investigation methods, simply because crime investigators are only called in after the fact. If incident management software will be used then the incident management software will only be as good as the critical thinking management of such, besides collection of reliable and all-the-truthful information considered and must be speedily uploaded.

Security issues impacted by cv-19 considered in a world depression and in-turn create larger issues to contend with

The Security Industry must consider the implications on crime and security that took place in the 1930's during the great depression. The manufacturing industry took a

major blow during the depression, the banks had their issues along with other sectors in the economic machine took its toll. Now, with the 4th industrial revolution is on the rise and will have its own unique issues and crime related.

In 1929 the great depression brought the world into a time of despair that lasted 10 years. COVID-19 is the root cause which surmounts the issues even more so. This dynamic of the 'perfect storm' will create calamities and shifting crime into different directions causing the security industry to shrink in some areas and grow in others.

This is the time when the security sector must play an important and productive role so that the globe does use these skills to disable COVID-19. Any form of riot or acts of aggression will trigger increased physical contact thus stimulating the number of infections.

This period in the 1930's gave rise to certain types of crime and stimulated the birthing of the transnational and local organized crime gangs besides the empowerment of the pro-nationalist extremists that participated with the mass murder of millions.

Physical security will now have to contend with issues that will increase dramatically. The lack of jobs and lower buying-power specially from low paying jobs could stimulate pro-nationalist extremists to do once again unspeakable things. Furthermore, the pro-nationalist and migrant reactions could turn to some towards radicalization and using methods of terror. We comprehend that there has been a distinctive increase in migration over the past few years, whereas, the vulnerability landscape has changed dramatically. Polarized neighbourhoods have grown in size and various countries experienced increased support for pro-nationalist parties. The crime related in cross cultural attacks of grievously bodily harm, rape and murder has increased along with demonstrations and riots breaking out periodically. This physical retaliation will speed up the number of infections in specific locations and feed into neighbouring locations. This work is not going to discuss right now the crime and damages related besides other issues but, declares that one cannot fathom

the possible outcomes related to this scenario in theatre that could impact the landscape dramatically. [Ref Critical Thinking the X Factor in Criminology, Security & Risk by Juan Kirsten 2018]

The loss of revenue could drive humankind even more towards using desperate measures. Man's basic need of food, shelter and drink [alcohol – (prohibition crime in the 30's)] besides medicine or medical support will be heightened and calling for all related buildings and logistic services related as soft targets. It must be considered that additional needs form part of man's basic needs and is discussed in the research of this article. This comprehension of this knowledge will give direction to the security industry whereas, security consultants, companies, risk managers, investigators and trainers must comprehend their position, predict the changes in their location and field of interest to survive this debilitating period

The perfect storm

As suggested above, the outcomes of cv-19 have led to the economic meltdown which in-turn, will present increased collateral damage with common and unique crime besides major factors concerning the human condition. COVID-19 influenced the human condition with heightened senses of fear, desperation, and anxiety. When we couple the cv-19 issues with unemployment leading to starvation then the human condition will become more desperate and lead to major challenges of increased mass violent outcomes to the extent of total anarchy in some countries.

The private security sector must protect the integrity of the supply chain besides contribute towards the disablement of covid-19. The supply chain will be tampered with by organized crime, gang crime, corruption, and very desperate people. This will cause major issues in delays of logistics, services or products required which will then cause even greater despair for the many.

Rejuvenate

There is a second part to this plan of action which must run parallel and refers to food security and securing 'community silos' (hybrid domains). This stage is already gearing into a major threat as food parcels and stamps are already being distributed in an attempt to feed the masses. If not addressed simultaneously then anarchy will prevail and destroy the lives of billions.

Solutions, Leadership, and Implementation

In this short overview, it clearly displays that there are multi-threats impacting simultaneously, and others that will come into theater at different times in various locations. The implementation of the leadership plan and method would be by orchestrating the global and regional infrastructure working in concert on the same foundation. as well as, at their own timing and rhythm relative to their location. Many countries have their structure in place the necessary methods to bring them onto the same page are being used with the current technology available. This all means, that the suggestions above could limit the level of collateral damage and offer a platform of solutions that can rejuvenate collateral damage already done and tackle the unknowns that are to follow.

The research, operational methodology and protocols are available from Juan Kirsten. Director General [ISIO] | International Security Industry Organization and Author HIM | Human Investigation Management, (Endorsed by ISIO and IFPO | International Foundation for Protection Officers)

ISIO - International Security Industry Organization

Juan Kirsten Author, Security Manager's Strategic, Operational and Protocol Guide to manage Covid-19, 2020,Master Investigator Critical Thinking in Investigation Vol 5, 2019.Criminology and Security Investigation Management Vol 4, 2019,Critical Thinking the X Factor in Criminology, Security and Risk Vol 3, 2018. *The operational methodology and protocols related is the intellectual property of Juan Kirsten.*

One of World's Biggest Online Piracy Groups Taken Down

An alleged criminal network of copyright infringing hackers, mainly responsible for pirating movies and hosting illegal digital content worldwide was dismantled in a coordinated action between US authorities and their counterparts in 18 countries around the world, with Europol and Eurojust support. Sixty servers were taken down in North America, Europe and Asia and several of the main suspects were arrested.

Streamed prior to release

The Sparks Group obtained DVDs and Blu-ray discs of unreleased content and compromised the copyright protections on the discs to reproduce and upload the content publically to online servers. It is believed that the piracy group, under investigation since September 2016, had successfully reproduced and disseminated hundreds of movies and TV programmes prior to their retail release date, including nearly every movie released by major production studios in the US. The Sparks Group has caused tens of millions of US dollars in losses to film production studios, mainly to the US movie, television, and supporting industries, from the copyright infringement.

False claims for free films

To get ahead, members of the Sparks Group made several material misrepresentations and omissions to wholesale distributors. On many occasions, they claimed to be DVD and Blu-ray discs retailers and promised not to sell the content prior to the retail release date. Once they received the products, the members of the group used special software to crack the copyright protections to then reproduce and encode the content in high-definition. The content was then disseminated and reproduced on streaming platforms, peer-to-peer and torrent networks from their platforms.

The servers were located around the world in Canada, Czechia, Denmark, France, Germany, Latvia, the Netherlands, Norway, Poland, Portugal, Romania, South Korea, Spain, Sweden, Switzerland, and the United Kingdom. These were taken down in yesterday's action and in the days preceding it, with the help of national authorities from these countries. Other measures were also taken in Italy, Romania and Canada. One of the members of the alleged criminal network was arrested over the weekend in Cyprus and another suspect was arrested yesterday in the US.

How 4 Million Victims of Ransomeware Have Fought Back Against Hackers

While the world is in the grip of a coronavirus outbreak, another virus is quietly wreaking havoc. Although this virus has been around for years, its cases have been rising alarmingly in the past few months and has brought critical activities such as hospitals and governments to a standstill. This virus is ransomware, but a free scheme called No More Ransom is helping victims fight back without paying the hackers.

Celebrating its fourth anniversary this month, the No More Ransom decryption tool repository has registered since its launch over 4.2 million visitors from 188 countries and has stopped an estimated $ 632 million in ransom demands from ending up in criminals' pockets.

Powered by the contributions of its 163 partners, the portal has added 28 tools in the past year and can now decrypt 140 different types of ransomware infections. The portal is available in 36 languages.

You can consult all the key figures in our dedicated infographic.

How No More Ransom works

No More Ransom is the first public-private partnership of its kind helping victims of ransomware recover their encrypted data without having to pay the ransom amount to cybercriminals.

To do this, simply go to the website nomoreransom.org and follow the Crypto Sheriff steps to help identify the ransomware strain affecting the device. If a solution is available, a link will be provided to download for free the decryption tool.

Three arrested in medical supplies fraud case

Three members of an international crime syndicate wanted for tricking an Italian company into making fraudulent payments for non-existent medical equipment were arrested in Indonesia, in a case supported by INTERPOL.

In May, an Italian company which was in discussions to purchase a large amount of medical supplies from a Chinese company, including ventilators and COVID-19 monitoring equipment, fell victim to a business email compromise (BEC) fraud.

The suspects infiltrated the email correspondence between the two companies

and convinced the Italian buyers to make three bank transfers totaling EUR 3.67 million to an account they controlled in Indonesia. Believing they were paying the legitimate supplier, the company made the transfers.

The fraud was quickly discovered, and INTERPOL's Financial Crimes unit was requested to assist with the case. INTERPOL swiftly facilitated communication between the Italian and Indonesian authorities via the INTERPOL National Central Bureaus (NCBs) in Rome and Jakarta, resulting in the timely interception and freezing of EUR 3.1 million of the fraudulent payments in early June.

To further support the investigation, in August INTERPOL held a virtual case coordination meeting where authorities from Italy (NCB Rome and the Postal Police Service) and Indonesia (NCB Jakarta, the Financial Intelligence Unit (PPATK) and the Criminal Investigation Department) shared critical investigative details and outlined the steps necessary for securing the frozen assets and locating the suspects behind the fraud.

Phone scams targeted in INTERPOL-coordinated operation

Two members of a criminal network engaged in telephone and email fraud have been extradited from China to South Korea, as part of an ongoing operation coordinated by INTERPOL.

Operation First Light, first held in 2014, targets telecom fraud and other types of social engineering scams, as well as money laundering of the illicit proceeds. Launched in September 2019, some 37 countries and territories are participating in the latest edition to identify and locate illicit call centres engaged in the fraud scams.

Under the auspices of the operation, INTERPOL facilitated a bilateral meeting between its National Central Bureaus (NCBs) in China and South Korea in November 2019 where the countries shared intelligence on transnational telecom fraud.

Following the meeting, police in Suzhou, China dismantled a criminal network engaged in telephone scams targeting victims in South Korea and arrested seven South Korean nationals, three of whom were the subjects of INTERPOL Red Notices. Two were extradited back to South Korea in July following extensive coordination between the two NCBs, with the remaining extraditions impending.

"The current wave of Operation First Light has faced unexpected challenges due to the pandemic, but we were still able to achieve a successful outcome thanks to close cooperation between the NCBs in Beijing and Seoul and the use of Red Notices alerting to the wanted individuals," said Duan Daqi, Head of NCB Beijing.

"This success demonstrates once again the strong determination of police in China and across the region to jointly fight against transnational crime, including telecom fraud," added Mr Duan.

Organized by INTERPOL's Financial Crime unit with support from regional policing bodies Europol and ASEANAPOL, the current wave of Operation First Light began in September 2019 and has been extended through March 2021 due to the COVID-19 crisis, to allow the participating countries sufficient time to exchange information, follow up on new intelligence and identify suspects.

US DHS Combats Potential Electromagnetic Pulse (EMP) Attack

The U.S. Department of Homeland Security (DHS) continues to prepare against ever evolving threats against the American homeland, most recently highlighting efforts to combat an Electromagnetic Pulse attack which could disrupt the electrical grid and potentially damage electronics. Today, the department is releasing the Electromagnetic Pulse (EMP) Program Status Report as part of an update on efforts underway in support of Executive Order (E.O.) 13865 on Coordinating National Resilience to Electromagnetic Pulses. E.O. 13865 establishes resilience and security standards for U.S. critical infrastructure as a national priority.

EMP weapons have the potential to disrupt unprotected critical infrastructure within the US and could impact millions over large parts of the country. Since the President's signing of the E.O. in March 2019, DHS, through the Cybersecurity and Infrastructure Agency (CISA), in coordination with the Science and Technology Directorate (S&T) and the Federal Emergency Management Agency (FEMA), has taken key actions to address known EMP-related vulnerabilities to critical infrastructure. The EMP Program Status Report highlights efforts taken across the public and private sector to foster increased resilience to EMP events. Through data analysis, vulnerability and risk assessments, testing and pilot programs, and government and industry engagement, the department is identifying critical infrastructure and associated functions that are at greatest risk from an EMP, and developing and implementing best practices to reduce the risk.

"EMP attacks are part of the emerging threats against our nation and demand a response," said Senior Official Performing the Duties of the Deputy Secretary Ken Cuccinelli. "That is why DHS is taking these contingencies very seriously, working diligently to mitigate our risks and equipping our state and local partners with the resources they need to do the same. We've made significant progress and look forward to the work ahead."

"As the Nation's risk advisor, one of CISA's priorities is understanding and mitigating threats associated with EMPs," said CISA Director Chris Krebs. "Over the past year, we have worked with interagency and industry partners to identify the footprint and effects of EMP threats across our National Critical Functions, and are developing sustainable, efficient, and cost-effective approaches to improving the Nation's resilience to EMPs."

In 2018, DHS released the Strategy for Protecting and Preparing the Homeland against Threats from Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD), which was the Department's first articulation of a holistic, long-term, partnership-based approach to protecting critical infrastructure and preparing to respond and recover from potentially catastrophic electromagnetic incidents.

46 arrested in France and Italy in a hit against the 'Ndrangheta

On Tuesday 15 September, the French Gendarmerie (Gendarmerie Nationale) and the Italian Carabinieri Corps (Arma dei Carabinieri), supported by Europol and Eurojust, arrested 46 individuals (33 in France and 13 in Italy) for their involvement in large-scale drug trafficking and money laundering.

This operation was enabled by an exceptional deployment of more than 550 police officers in France (in and around Paris and Provence-Alpes-Côte d'Azur) and Italy (Liguria). During the house searches, law enforcement officers seized weapons, a large amount of cash, counterfeited documents, drugs, vehicles and various assets from money laundering operations. The investigation also uncovered the transfer of weapons, some of them military. The suspects linked to the 'Ndrangheta were reported to play an active role in cocaine and cannabis trafficking between the Côte d'Azur in France and Liguria in Italy, with supply chains from Belgium, Spain and the Netherlands.

iProov has launched the world's first system of global threat intelligence for biometric assurance

The iProov Security Operations Centre (iSOC) combines technology, process and people to monitor and manage the rapidly evolving landscape of biometric cyber-crime. It further secures iProov's Genuine Presence Assurance technology and protects organizations and individuals against the growing threat of AI-driven cyber-attacks, including deepfakes.

Biometrics have become the technology of choice for digital user authentication, enabling individuals to securely and effortlessly unlock devices and access online services, such as bank accounts and health records. Face biometrics offer simplicity and ease for frequent user authentication, while delivering the highest levels of online security for Genuine Presence Assurance - is the user the right person, a real person, authenticating right now?

This makes it ideal for all types of organisations, including those most sensitive to security, like governments, banks and travel and health providers.

iProov's iSOC acts as the nerve center for its cloud-based Genuine Presence Assurance solutions. Cyber-criminality continues to grow, as fraudsters attempt to take over or manipulate legitimate customer accounts for financial gain, to compromise national security, or to cause disruption and social disintegration by impersonation. The lower cost of technology and improved processing power, combined with the explosion in publicly available deepfake technology, make it easier for criminals to create these attacks at scale, inexpensively and with minimal efforts, with potentially devastating implications.

iProov's iSOC combines advanced machine-learning technology with responsive processes to provide resilience against the emergence of ever more sophisticated attacks. iProov's Genuine Presence Assurance technology is providing governments and enterprises in financial services, healthcare, and travel with presentation attack detection (PAD), replay attack detection (RAD), and deepfake attack detection (DAD). iSOC's threat intelligence provides forewarning of major new attacks and enables iProov to prepare and defend against them. The world has seen how failure to prepare against threats in other sectors of cybersecurity has led to the phenomenon of sudden ransomware storms; iSOC will help prevent biometric attack storms.

iSOC has played a key role in enabling iProov to pass audit for certification against demanding security standards, such as eIDAS, conducted by stringent auditors like TÜV. These demand robust business processes for monitoring and management of attacks. Thanks to iSOC, iProov is the only provider of biometric assurance to have passed such audits.

Battlefield evidence increasingly used to prosecute foreign terrorist fighters in the EU

Battlefield evidence, such as photos depicting crimes committed against civilians, fingerprints on explosive devices and e-mails describing terrorist plots, is increasingly being used to prosecute suspects of terrorism and core international crimes, including returning Foreign Terrorist Fighters. The 2020 Memorandum on Battlefield Evidence, which was published today by Eurojust, the EU Agency for Criminal Justice Cooperation, shows that while there are many challenges in obtaining such data and making sure it meets the criteria for admissible evidence, it has paved the way for bringing terrorist suspects to trial.

Battlefield evidence can be considered as proof, similar to any other type of evidence, in criminal proceedings. Judicial authorities in ten EU countries report that, since 2018, they have increasingly received and used battlefield information in court proceedings – irrespective of whether the information came from national and/or foreign military forces, or from NGOs and UN entities. The evidence consists of both electronic data and physical items, such as mobile phone data, credit cards. Other examples are situational reports, letters describing potential terrorist plots, witness statements and administrative documents such as a payroll roster, a list of patients in a hospital, or a will.

CONTROP is to supply surveillance and observation systems for new ships currently being built for the Vietnamese Border Guard

CONTROP has been selected to supply iSea-25HD observation systems for installation on the new ships under construction at L&T's shipyards in India, and vessels being built for the Vietnamese Border Guard, by Hong Ha shipyards in Vietnam. The systems will be delivered during 2020 and 2021.

Easily interfaced with other onboard systems, the iSea-25HD offers a full solution for naval and maritime operations. Featuring a unique, cutting-edge gyro-stabilized system, it enables a stable, continuous and uninterrupted line-of-sight (LOS) view, ensuring a very clear picture, even in the roughest of seas, and is robust enough to withstand even the harshest environmental conditions including fog, moisture, salinity and excessive splashing.

Capable of maintaining boresight even in conditions where there are shocks and vibrations, the iSea-25HD incorporates digital and mechanical compensatory mechanisms developed by CONTROP to significantly enhance image quality.

The iSea-25HD lightweight system provides maximum range surveillance using highly sensitive sensors, including a high-performance thermal imaging (TI) camera using 3-5µ IR detector with a continuous zoom lens, a high-sensitivity color day camera, and an eye-safe laser range finder (LRF). Among its additional features are advanced image processing and video enhancement algorithms. Applications include search & rescue, law/coast guard enforcement, EEZ protection, counter piracy, illegal fishing and special ops.

The Panasonic i-PRO X-Series cameras run Deep Learning AI applications on the edge for lower TCO and faster processing

Panasonic today announced its collaboration with the software company A.I.Tech. It brings together i-PRO's industry leading security cameras with built-in AI capabilities and groundbreaking intelligent applications to provide a range of business solutions based on deep learning, many applicable to the current COVID-19 environment.

The deep learning applications run directly on the cameras themselves, eliminating the need for additional servers for analytical calculations whilst maintaining the same high levels of accuracy. The benefits include lower total cost of ownership of security infrastructure, as well as faster processing and more immediate alarms, notifications or information from the applications.

A number of the AI applications can be used in the current pandemic to help manage social distancing, occupancy levels and the wearing of face masks. Applications can also be used by retailers to enhance the customer experience; in smart cities for traffic monitoring and smart parking; and by event organisers and transports hubs to monitor and ensure safety.

They are completely integrated with the recently introduced Panasonic i-PRO X-Series camera range with AI engine, which includes six new models in total: The 5MP resolution cameras went on sale in July and the 4K resolution cameras come to market in November. All are available with vandal resistant indoor and outdoor dome or box configurations.

Axon's TASER 7 Conducted Energy Device Approved for Deployment Across UK Police Forces

UK's Home Secretary Priti Patel grants approval to use next-generation TASER device for increasing officer efficiency and community safety

TASER's Axon brand includes a growing suite of connected products and services from body cameras and digital evidence management tools to mobiles apps.

Axon has announced the approval for police forces in the United Kingdom (UK) to purchase and deploy its latest TASER Conducted Energy Device (CED). The TASER 7 is Axon's most effective less-lethal weapon to date and was

built to equip officers with the power to de-escalate dangerous situations. Following the approval to deploy the TASER 7 by the UK's Home Secretary Priti Patel, police forces can begin training on the TASER 7 before the end of the year.

The TASER 7 is Axon's first truly connected CED with services that are completely integrated into Axon Evidence (Axon's digital evidence management solution). These capabilities include wireless device management, self-reporting and general visibility into the health of the device or a full fleet of CEDs. The TASER 7 also provides enhanced reliability by offering optimized close-quarter and stand-off cartridges.

"We're excited to watch the adoption of this innovative device across the UK," says Axon UK Country Manager, Mike Ashby-Clarke. "We built this tool with community and officer safety in mind. With high-tech features such as automated usage logs and device management, officers will be able to spend less time physically managing their CED and can instead focus on what matters - protecting the public."

Videalert's CCTV new electric mobile enforcement vehicle (MEV) has masses of potential security applications

Bath and North East Somerset Council (B&NES Council) is extending its Videalert CCTV enforcement platform by deploying a new electric mobile enforcement vehicle (MEV). This multi-tasking vehicle will be used to enforce a wide range of civil traffic contraventions including digital resident parking permit zones, keep clears outside schools, bus stops and bus lanes. It will also help B&NES Council to carry out traffic surveys as well as monitoring and enforcing the new class C Clean Air Zone (CAZ) in the City of Bath which is expected to go live in early 2021.

According to Chris Major,

Group Manager for Transport and Parking at B&NES Council: "Videalert's hosted video platform is multi-purpose and allows us to quickly and easily extend the reach of our enforcement activities. We can now use fixed and mobile CCTV enforcement cameras mounted on electric MEVs, both cars and bikes, enabling us to achieve compliance whilst demonstrating that we are serious about driving through clean air initiatives."

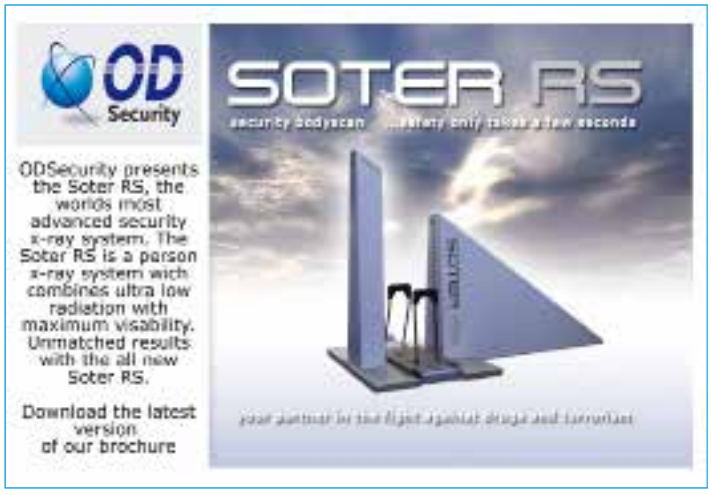
The new MEV is a Peugeot 208e with a 47kw battery giving a range of 170-200 miles from a full charge. The car is fitted with Videalert's full suite of traffic enforcement and management software. Two roof-mounted Stingray modules are installed front and rear, each with two ANPR cameras and upgraded infra-red lighting, which accurately capture crisp images of reflective number plates at distances of up to 40 metres. The MEV will deliver high levels of productivity as number plate read rates of over 98% can be achieved in a wide range of applications with vehicles being driven at normal road speeds and includes a full colour overview module to capture contextual images of contraventions.

World Security Report

World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to over 130,000 organisations globally. It tracks the full range of problems and threats faced by today's governments, security and armed forces and civilian services and looks at how they are dealing with them. It aims to be a prime source of online information and analysis on security, counter-terrorism, international affairs and defence.

Border Security Report

Border Security Report is the bi-monthly border management industry magazine delivering agency and industry news and developments, as well as more in-depth features and analysis to over 20,000 border agencies, agencies at the borders and industry professionals, policymakers and practitioners, worldwide.



October 2020

5-7
ICS West
Online
www.iscwest.com

5-8
Behavioural Analysis
Online
www.behaviouralanalysis.com

November 2020

24-26
World Border Security Congress
Athens, Greece
www.world-border-congress.com

30-5 Dec
International Security Expo
Online
www.internationalsecurityexpo.com

December 2020

8-9
Aviation Security Summit
Online
www.aaae.org/aaae/SecuritySummit

1-2
Sectech Denmark
Copenhagen, Denmark
www.securityworldmarket.com/sectech/dk/index.asp

8-9
ICAO Global Aviation Security Symposium 2020 (AVSEC2020)
Montreal, Canada
www.icao.int/Meetings/AVSEC2020/Pages/default.aspx

To have your event listed please email details to the editor tony.kingham@knmmedia.com

May 2021

11-13
Critical Infrastructure Protection & Resilience Europe
Bucharest, Romania
www.cipre-expo.com

October 2021

19-21
Critical Infrastructure Protection & Resilience North America
New Orleans, LA, USA
www.ciprna-expo.com

ADVERTISING SALES

Paul Gloc
UK & ROW
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

Sam Most
Mainland Europe &Turkey
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

Paul McPherson
Americas
E: paulm@torchmarketing.us
T: +1-240-463-1700