WORLD SECURITY REPORT

Official Magazine of

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

WINTER 2020/21
www.worldsecurity-index.com

PRIORITY OF PROTECTING DIGITAL CRITICAL INFRASTRUCTURE WILL GROW IN 2021

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.12


» p.16


» p.26

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 100,000 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.

2020 – A YEAR TO REMEMBER

2020 has certainly been a year to remember, some might say a year to forget.

COVID19 has affected everyone to some degree or another but especially those of us lucky enough to be living in advanced economies. For those who live in parts of the world where the availability of clean water is more of a problem or where religious or ethnic violence is a part of daily life, COVID19 is just another problem.

As vaccines become available and we head for what we hope will be the control of the virus, and a return to normal, the long-term economic effects of the crisis are yet to play out, and what that might mean for security.

Already, we have seen the UK reduce its overseas aid budget to 0.5% of gross national income, and if the economy shrinks as a result of a COVID19 recession, that figure in real terms will shrink further. OK, so the UK is just one country. But this reduction is significant, given that the UK is second only to the US in terms of overseas aid. If other countries, struggling to balance their budgets follow the UK's lead, we could see a huge overall reduction in overseas aid.

Whilst aid money is not directly linked to security, foreign aid helps to generate prosperity and create the political and economic stability that leads to peaceful societies.

As budgets tighten, we may also see reduced levels of direct security assistance, such as President Trump's recently announced drawdown of US military assistance to the Afghan government. Although this is more to do with domestic US politics than budget, other cash-strapped NATO nations may decide to follow suit.

Only this week, General Mark Milley, Chairman of the US Joint Chiefs of Staff, admitted that after twenty years of war, NATO has only achieved a modicum of success, i.e., that another 9/11 type of terrorist operation that has been prevented. But militarily the situation is a strategic stalemate and negotiations with the Taliban are the only way forward.

READ THE FULL VERSION

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

In the middle of peace negotiations, withdrawing US troops is another mistake.. The message to the Taliban is clear. All they have to do is wait.

In the Sahel, French-led operations may also come under pressure at a time when sub-Saharan Africa is fast becoming the centre for ISIS affiliates activity.

According to the Global Terrorism Index report by the Institute for Economics & Peace (IEP), Sub-Saharan Africa has been hit the hardest, with seven of the ten countries with the largest increases in terrorism deaths residing in the region. ISIL affiliates are mainly responsible for the increase, with 41 per cent of all ISIL related deaths occurring in sub-Saharan Africa.

Thomas Morgan, a Senior Research Fellow at IEP, explains: "There are serious concerns that the deteriorating economic conditions will lead to more people becoming alienated and susceptible to extremist propaganda."

This is reflected in another phenomenon of recent years, the rise of the far-right in Western democracies. Whilst we are not likely to see widespread terrorism, on the scale of Islamic extremism, it is a reflection of a shift to the right of mainstream opinion, where economic conditions mean that elements of the population feel disenfranchised by globalisation and, become more xenophobic and isolationist. This is then reflected in more populist policies adopted by democratic governments.

It is difficult to predict what will happen to the global economy as the pandemic is brought under control. But what is certain is that the financial cost of it so far will put governments, policies and, budgets under severe pressure for the foreseeable future. It would be easy, and frankly popular, to reduce overseas aid and security assistance, but it is highly likely that this would have very negative outcomes in the long term.

Tony Kingham

Editor

Priority of Protecting Digital Critical Infrastructure Will Grow in 2021

In 2021 we will be facing a new and more sophisticated array of physical security and cybersecurity challenges that pose significant risk to global critical infrastructure (CI). A difficult challenge will be keeping up with the increasing sophistication of cyber threats and the expanding digital attack surfaces.

Last year, The 2020 World Economic Forum's Global Risks Report listed cyberattacks on critical infrastructure as a top concern. WEF noted that "attacks on critical infrastructure have become the new normal across sectors such as energy, healthcare, and transportation." www.weforum.org/reports/the-global-risks-report-2020

Global Cybersecurity Critical Infrastructure Attacks

In the past decade, there have been many cybersecurity attacks focused on breaching CI. There have been thousands of cyber attacks and several have been successful information technology (IT) operation technology (OT),

and industrial control system (ICS) infrastructures.The new reality is that almost all of our critical infrastructures operate in a digital environment that is internet accessible. The trends of integration of hardware and software combined with growing networked sensors are redefining the surface attack opportunities for hackers across all digital infrastructures.

The threats are growing along with the attack surfaces associated with CI. The types of cyber threats include phishing scams, bots, ransomware, and malware and exploiting software holes. The global threat actors are many including terrorists, criminals, hackers, organized crime, malicious individuals, and, in some cases, adversarial nation states.

Globally, a variety of industries related to CI have been targets of attack, including healthcare, financial and transportation. The energy sector has been a top focus of attacks. Historically, cyber threat actors have targeted the energy sector with various results, ranging from cyber espionage to the ability to disrupt energy systems in the event of a hostile conflict. According to a Ponemon Institute report, three-quarters of energy companies and utilities have experienced at least one recent data breach. A major reason for why the sector has become more vulnerables is that Adversaries have gained a deeper knowledge of control systems and how they can be attacked and can employ weaponized malware against power stations and other energy related CI assets.

Also expanded connectivity has added to an expanded attack surface that includes IT, OT, ICS,

system vulnerabilities and the Internet of Industrial Things (IIoT). Corporate networks, onshore wells, offshore platforms, and oil and gas pipelines all constitute the energy critical infrastructure. Moreover, In the case of energy infrastructure, many of the OT systems involve legacy systems over 25 years old (no security built in) and are in the early stages of digital transformation. Because of legacy equipment, there is often a visibility problem of the lack of telemetry data on many OT systems and devices.

There have been some frightening episodes involving critical energy infrastructure. In 2014, a computer in the control room at Monju Nuclear Power Plant in Tsuruga, Japan, was subjected to malware, but possibly by accident. And in 2015, South Korean hackers targeted Korea Hydro and Nuclear Power Company, but luckily to no avail. Most cyber experts believe that North Korea was behind the attempted cyberattack. These incursions are a wake-up call as there is a very real and growing fear that a future cyberattack on a nuclear plant could risk a core meltdown.

Non-nuclear power plants have also been subjected to intrusions and breaches. A hack in Ukraine was held up as a prime example. In December 2015, hackers breached the IT systems of the electricity distribution company Kyivoblenergo in Ukraine, causing a three-hour power outage.

In 2017, Hackers used Triton, a specialized malware to compromise critical safety systems at Schneider Electric. The malware is still being used to target industrial systems. According to Israel Barak, CISO at Cybereason, ;most countries are still vulnerable to cyber-attacks on critical infrastructure because the systems are generally old and poorly patched. Power grids are interconnected and thus vulnerable to cascading failures."

For a detailed list of attacks, please see Significant Cyber Incidents Since 2006 by The Center for Strategic and International Studies (CSIS):

https://csis-website-prod.s3.amazonaws.com/s3fs-public/201106_Significant_Cyber_Events_List.pdf

Cyber Vulnerabilities of Critical Infrastructure Systems

The World Energy Council says countries must raise their game in combating cyberattacks on nuclear

and other energy infrastructures. They note that the frequency, sophistication and costs of data breaches are increasing. The expanding cybersecurity focus on energy infrastructure by both the public and private sectors is certainly a welcome development. See: https://www.worldenergy.org/assets/downloads/World_Energy_Issues_Monitor_2020_-_Full_Report.pdf

An economic impact of a breach can be calamitous to critical infrastructure. A cyber-breach is not a static threat and is always evolving in tactics and capabilities. Many organizations do not know if an attack has occurred. Hackers often seek out unsecured ports and systems on industrial systems connected to the internet. IT/OT/ICS supply chains in CI can be particularly vulnerable as they cross pollinate and offer attackers many points of entry and older Legacy OT systems were not designed to protect against cyber-attacks. Protecting critical systems from cybersecurity threats is a difficult endeavor. They all have unique operational frameworks, access points, and a variety of legacy systems and emerging technologies. And a lack of trained skilled workforce is a continual issue in IT, OT, ISC cybersecurity.

The U.S. Approach To Protecting Critical Infrastructure

With all the IT, OT, ICS cybersecurity risks and challenges, protecting CI is not an easy task for any country, especially democratic societies that are by their nature open and accessible. In the U.S., most of the critical infrastructure, including defense, oil and gas, electric power grids, health care, utilities, communications,

transportation, education, banking and finance, is owned by the private sector (about 85 percent) and regulated by the public sector.

Created as a civilian counter-terrorism agency back in 2003, The Department of Homeland Seceurity (DHS) has become the lead U.S. agency on the civilian side of government for cybersecurity. Also, the DHS role has significantly evolved in correlation with the growing and complex threat to critical infrastructure. Largely because of that responsibility and cybersecurity threat to CI and the need to coordinate with the private sector, the Department of Homeland Security (DHS) embarked on creating the Cybersecurity and Infrastructure Security Agency (CISA) in 2018 as an operational component.

CISA's stated role is to coordinate "security and resilience efforts using trusted partnerships across the private and public sectors, and delivers training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide" A fundamental aspect of that role for CISA is to protect 16 critical infrastructure sectors deemed 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, or any combination thereof. They are:

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, and Water and Wastewater Systems Sector -- https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19

The DHS CISA model is a good one for any country to emulate, particularly from a risk management perspective.

A Cybersecurity Strategy & Framework to Defense Against Cyber-Attacks

A CI cybersecurity strategy to meet growing challenges needs to be both comprehensive and adaptive. As in physical security,

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

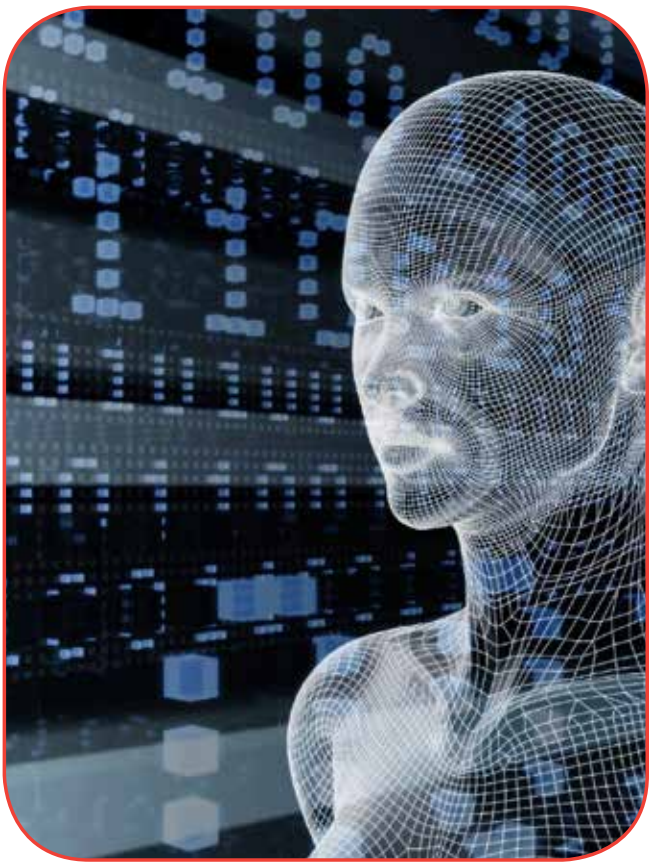
Paul Gloc
(UK and Rest of World)
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

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:



cybersecurity relies on the same security elements for protection as physical security: layered vigilance, readiness and resilience. Meeting the challenges also requires public/private cooperation on sharing threat information, best practices, incident response, and emerging technology solutions to help mitigate attacks.

Defined by the most basic elements in a cybersecurity strategy & framework for cybersecurity CI should be constitute:

• Security by Design: SCADA networks and IT networks for industrial systems, and need to be designed, updated and hardened to meet growing cybersecurity threats. Security by design requires building agile systems with operational cyber-fusion to be able to monitor, recognize, and respond to emerging threats. Segmenting of vulnerable networks and remote connectivity should be a priority. Security by design can also identify system and operational dependencies up front of the process to remove risk.

• Layered vigilance: Vulnerability Assessments need to be instilled up front in the process. This should include mapping of the control systems, communication flows, and all connected devices in the network should be prioritized. Encryption of data flowing from sensors and segmentation of OT and IT should be included in a layer. The vigilance should incorporate best practices for industry cybersecurity standards and processes, including NIST, IEC 62443,ISO 2700, and the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) for Industrial Controls Systems (ICS) framework, .and others according to verticals. Also, identity access management and control tools are vital considerations.

• Situational Awareness: there is a need to continually surveil, analyze and game the critical infrastructure cyberthreat landscape. There is no substitute for good intelligence.

• Information sharing: The specifics of a security approach may vary according to circumstances, but the mesh that connects the elements is situational awareness combined with systematic abilities for critical communications in cases of emergency. Cooperation within industries and with government (Public/Private /Partnerships) are a proven model to follow. Preparation and commitment from both government and industry leadership is critical to help thwart threats.

• Readiness and incident response: There is a high chance of being breached and if so operational capabilities need to be maintained for CI. What works in Cybersecurity IT may pose risk to OT cybersecurity where patching may not be an option. There are many available CI readiness monitoring tools to test and validate in a SOC visual command center.

• Incident response. Protecting industrial control systems used by utilities from both physical and cybersecurity threats is a component of the dynamic threat environment and response matrix that constitutes their security environments. Real-time on-the-scene intelligence and operational alarms to relay critical information to the appropriate response personnel are an essential part of that response matrix. The ability to disconnect CI from the internet and continue to operate should be a part of any incident response. Assigned roles and training on how to respond to a breach need to be incorporated into incident response planning.

• Resilience: This also requires strategy, training (table top exercises) for a coordinated response in the event of a breach, and a plan for communicating and enabling recovery. Management, legal, and public affairs need to be prepared.

For a more in depth look at protecting OT systems from cyber-attacks see:

https://www.hstoday.us/subject-matter-areas/infrastructure-security/nsa-and-cisa-recommend-immediate-actions-to-reduce-exposure-across-operational-technologies-and-control-systems/

Protecting critical infrastructure will have enormous security challenges as we adapt to the technological and cultural changes taking place in 2021. Every country, governmental jurisdiction, industry, company and individual has their own unique CI threat landscape to address. A security strategy based on the pillars of vigilance, readiness and resilience needs to be actualized against those threats. This is not only critical for risk management and incident response, but it is an imperative for mitigating harm in an increasingly connected and precarious world.

About the author: Chuck Brooks, President of Brooks Consulting International, is a globally recognized thought leader and evangelist for Cybersecurity and Emerging Technologies. LinkedIn named Chuck as one of "The Top 5 Tech Experts to Follow on LinkedIn." Chuck was named as a 2020 top leader and influencer in "Who's Who in Cybersecurity" by Onalytica. He was named by Thompson Reuters as a "Top 50 Global Influencer in Risk, Compliance," and by IFSEC as the "#2 Global Cybersecurity Influencer." He was named by The Potomac Officers Club and Executive Mosaic and GovCon as at "One of The Top Five Executives to Watch in GovCon Cybersecurity. Chuck is a two-time Presidential appointee who was an original member of the Department of Homeland Security. Chuck has been a featured speaker at numerous conferences and events including presenting before the G20 country meeting on energy cybersecurity.

www.linkedin.com/in/chuckbrooks/
@ChuckDBrooks

Europe deploys 7Shield – cybersecurity from space?

SHIELD – Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats.

The project gives an innovative boost to the protection of earth segments and satellite data resources. Protecting critical infrastructures from cyber threats. From IoT to machine learning, here are the advanced technologies integrated into the framework.

7SHIELD

The overall concept of 7SHIELD is to provide to the European Ground Segment facilities a holistic framework enable to confront complex cyber and physical threats by covering all the macrostages of crisis management, namely pre-crisis, crisis and post-crises phases.

The Copernicus era has created a new market with the massive amounts of satellite data that the ground segments of space systems receive serve to the market and governmental bodies.

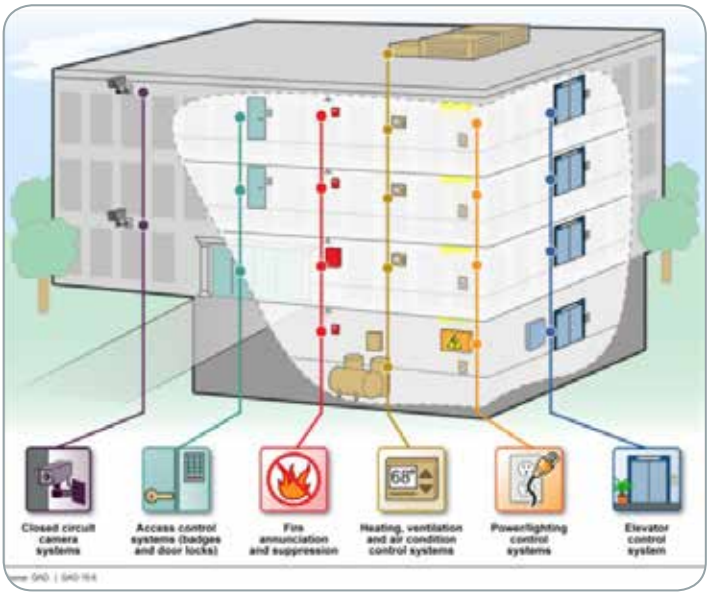
A physical/cyber-attack to their installations or communication networks, respectively, would cause debilitating impact on public safety and security of EU citizens and public authorities. A physical attack on a space ground segment makes the distribution of satellite data problematic and, on the other hand, a cyber-attack in its data storage, access and exchange affects not only the reliability of space data, but also their FAIR standards: findability, accessibility, interoperability and reusability. Current approaches do not fully exploit the recent advances in surveillance mechanisms with robotic technologies and AI.

A view of Facility Industrial Control System Security

A 2019 US Department of Energy Inspector General Report found that physical and logical access security controls did not always provide sufficient restrictions over information technology (IT) resources. (Energy OIG 2019 p 2) This statement is an illustration of the environment facing critical infrastructure protection (CIP).

Technology is advancing in the system-use and connectivity within buildings, facilities, and complexes. The Edith Cowan University research team in their 2017 building automation and control (BAC) system (BACS) report found that BAC is "… embedded into the contemporary building environment…" (BACS 2017 p i). The proliferation of interconnected systems brought about by the internet-of things (IoT) will enhance the facility's ability to become "system-smart." A system-smart facility from an infrastructure perspective is dependent of other systems within its architecture. This architecture will access and use local and external systems. To acquire the secure access to external system facility owners must have agreements to assure the security of the external system's access and connectivity.

The BAC Report found the building's environment must be flexible, adaptable, and sustainable. The building's vulnerability from threats and interconnectivity security issues. Secure local and remote access to devices, networks,



and software applications is paramount (BAC2017 p i). The BAC Report recommends

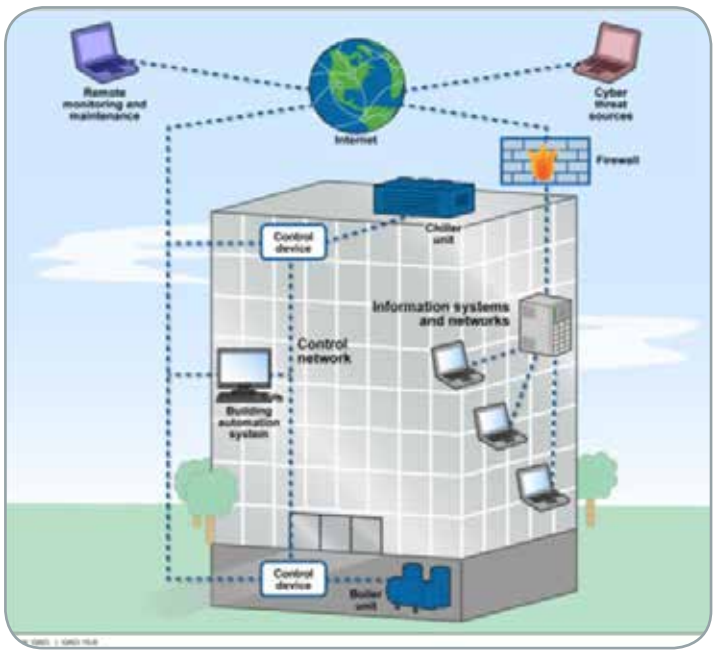
- The facility owners promote awareness of threats and risks
- Improve organizational cross-department liaison
- Build partnerships among BACS experts, in-house, and external third-parties
- Provide a guideline to aid the stakeholders to achieve the security of the BACS

The BACS Guideline is a governance tool to promulgate a common language among the facility's stakeholders (BAC 2017 p iii).

The BAC Report is definitive in its research findings and recommendations. The implementation of key parts of the report will take time. The international implications of BACS is a CIP imperative. Systems and devises can be accessed from any where there is connectivity. In the United States the US Department of Homeland Security (DHS) provided guidance to the CIP community in the form of the National Infrastructure Protection Plan (NIPP). The NIPP provide guidance to the 16 industry categories or sectors. "Our national well-being relies upon secure and resilient critical infrastructure—those assets, systems, and networks that underpin American society. To achieve this security and resilience, critical infrastructure partners must collectively identify priorities, articulate clear goals, mitigate risk, measure progress, and adapt based on feedback and the changing environment." (NIPP 2013 p 1) From this governance each industry sector interprets the NIPP guidance to develop specific sector guidance in the form of sector specific plans. The Commercial Facilities sector-plan (CFSP). The Sector plan provide general guidance to the industry that is based on the guidance provided by the NIPP. "…this plan represents a collaborative effort among the private sector; Federal, State, local, tribal, and territorial governments; and nongovernmental organizations to reduce critical infrastructure risk…" (CFSP 2015 p iii). To serve the sector's need to provide cybersecurity guidance to the industry, DHS released the Commercial facilities sector cybersecurity framework (CFCSF) implementation guidance of 2015. This document "…recommends an approach that enables organizations to prioritize their cybersecurity decisions based on individual business needs without additional regulatory requirements…" (CFCSF 2015 p 1). The CFS cybersecurity release in 2015, provided provides an approach that will enable sector stakeholders to frame and prioritize their cyber security decisions (CFS-Cyber 2015 p 1). This cybersecurity guidance was based on the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, which was issued in February 2014. The current version is Version 1.1 of 2018. "… Version 1.1 of this Cybersecurity Framework refines, clarifies, and enhances Version 1.0, which was issued in February 2014. It incorporates comments received on the two drafts of Version 1.1…" (Framework 1.1 (2018) p ii). The CFS Cyber release of 2015 is a use-case implementation of the NIST Cybersecurity Framework.

Given this guidance at the national level there remain an implementation void. Throughout the BACS Report instances were cited that highlight these voids. Before the release of the BACS Report in 2017, the US Government's Government Accountability Office (GAO) released a report citing that the United States need to address the cybersecurity risk to BACS (GAO-15-6 2015). To graphically show a portion of the facility situation figure 1 is from the GAO report. It lists some of the BACS in a building.

As shown in figure 1, some types of building and access control systems in federal facilities include:" • closed circuit



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

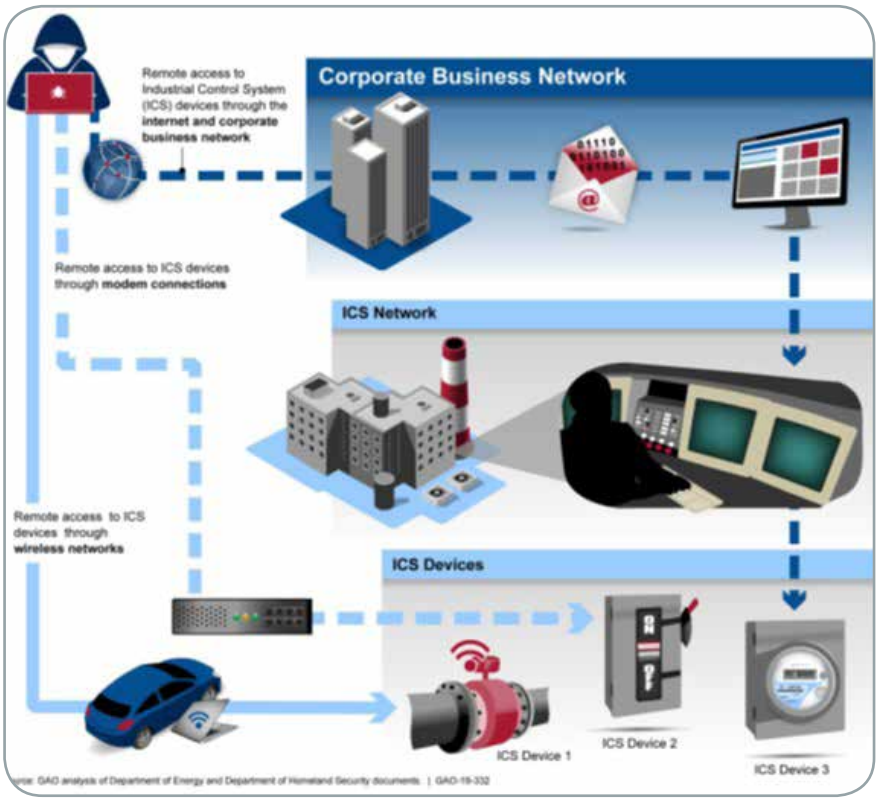
For further details and to join, visit **www.cip-association.org** and help shape the future of this increasingly critical sector of national security.

We look forward to welcoming you.

John Donlon QPM, FSI
Chairman
IACIPP

camera systems include cameras, televisions or monitors, and recording equipment, and provide video surveillance capabilities; • access control systems include card readers, control panels, access control servers, and infrastructure such as door actuators and communications lines, which restrict access to authorized persons only; • fire annunciation and suppression systems include fire alarms, emergency communication equipment, and water-based or non-water-based suppression systems, designed to prevent, extinguish, or control a fire or other life safety event; • heating, ventilation, and air conditioning (HVAC) systems include equipment for heating, cooling, moisture control, ventilation or air handling, and measurement and control, often managed through a building automation system13 • power and lighting control systems include lighting devices and their controls, advanced-metering controls, power distribution systems, and emergency power or lighting systems, which are also often managed through a building automation system; and ; • elevator control systems include operating machinery, safety systems, and a control system or panel." (GAO 15-6 pps 9-10)

As mention previously, the BACS are reliant on the on the interdependence of the facility's cyber architecture. GAO report 15-6 also, provide an example of the connectivity of a HVAC System. Figure 2 is an example of the connectivity of a HVAC System connect to the internet. This graphic represents the evolution of BACS. This implementation increases the efficiency of the HVAC throughout the building. Placing these systems with the information technology enterprise present



many cybersecurity challenges. Cyber intrusions and insider threats through the HVAC system is a reality that can cause an improperly installed and maintained system to traditional cyber threats.

In another GAO report threats, vulnerabilities and impacts are outlined. The report focuses on the US Electric grid. The vulnerability to a BACS is relevant to the identification of an attack profile. Figure 3 from this report is a graphical depiction of potential ways an attacker could compromise an industrial control system on a corporate network. (GAO-19-332)

Here the intruder gains access to the corporate network via the internet. From there the attacker moves to access the control system network and devices.

To illustrate an actual attack on a BACS, the Target stores is one such intrusion. on November 15, 2013, hackers broke into a contractor system to gain access to Target's HVAC system (INL/CON-18-44411 p 12). The attackers First stole the login credential of a third-party HVAC contractor with a phishing attack. They then uploaded malicious credit card-stealing software to cash registers throughout Target's chain of stores. 70 Million customers were affected. Target had $309 Million in lawsuits and the financial institution incurred an additional $200 million.

Dr. Ron Martin, CPP, CPOI is a Professor of Practice at Capitol Technology University

The Need for Higher Level Strategic Approaches to Cyber Security

Multiple factors are driving the need for higher-level strategic approaches to cyber security, as states and communities adapt to ubiquitous technological advancements, globalized platforms, and digital economies that are affecting nearly every aspect of our lives, our communities, and the global interactions among states and economies, which have become increasingly complex and intertwined

New and additional players are involved in cyber security, such as cyber lawyers, cyber insurance providers, regulators, and law- and policy-makers, at multiple levels of government. IT and security disciplines themselves are maturing and professionalizing, and are adapting to automation and technological advances, one such example is the introduction of AI into fraud and forensic investigation. Additionally, new security and cyber security disciplines are emerging, such as security convergence, and cyber security economics. The proliferation of unique interests, influences, and objectives among cyber security professionals and disciplines may result in different, and even conflicting, directions being taken in cyber security. This conflict may be reduced or managed through cross-discipline awareness and engagement, and a more strategic approach that transcends individual disciplines and actors.

One example of such conflict is that

the security community in general is trending toward greater regulation, and specificity in standards and certifications, while the business community is trending toward a demand for less regulation and specificity, to stimulate innovation, reduce barriers to sector entry, and to foster competition that drives innovation. Another example is that law enforcement and intelligence communities may resist encryption as an enabler of threats, while the cyber insurance sector may encourage encryption as a reasonable measure that businesses may take to protect data and reduce liability risk. Additionally, social media platforms, largely privately owned, are facing increasing pressure in the public interest to monitor and attribute content to limit social harms, which may in turn risk limiting anonymity and freedom of speech, which are also in the public interest, and have traditionally been public sector responsibilities.

Coherence will require more than collaboration and consultation; rather, it will require careful strategic balance and interdisciplinary consideration to ensure coherent momentum forward in cyber security efforts.

Attempts to achieve such balance are increasingly reflected in the proliferation of National Cyber Security Strategies (NCSS's), which are focused at the strategic level, rather than at lower levels, where much of the innovation and risk management in cyber security are occurring. NCSS's are to a certain extent political in nature, factoring in national interests and cost considerations for taxpayers, which may compete with traditional risk management and focus within organizations, which have their own strategic planning, risk tolerances & cultures, and stakeholder interests, among other. Traditional risk management approaches in cyber security may not working as effectively as expected. New risk management models and better data sets may need to be developed, including from the new 'cyber security economics' discipline. Similarly, NCSS's alone may not capture the full complement of considerations in cyber security, even at the strategic level, and may require the gap to be bridged more effectively between NCSS's and risk management within organizations.

Cyber security may require not just a strategic-level approach, but a grand-strategic approach, once reserved to great powers. Grand-strategy involves greater than military resources, and applies in peacetime, and within domestic space - consistent with the ubiquitous nature of cyber security challenges of today. Middle and even smaller powers may require comprehensive, and more than basic strategic efforts when it comes to cyber security challenges, even beyond cyber-specific or cyber-focused NCSS's. While dedicated NCSS's are becoming more common, outside of national security and foreign policy strategies for example, stand-alone cyber security strategies may not be sufficient, particularly in the absence of recognized international cyber law. Larger geostrategic considerations may also need to be factored into strategy, as well as international trade and investment, and larger economic considerations.

Risk management and risk tolerances are related to organizational culture. State-level 'cyber security cultures' may be slowly emerging, including as the global regulatory and legal landscape is becoming increasingly 'staked-out' in terms of jurisdictions and state preferences. For example, in relation to cybersecurity, the EU has been notably privacy-focused, and favourable to individuals with personal information (as reflected in the General Data Protection Regulation - GDPR), the United States has been notably business focused (reflected in the rollback of privacy protections and internet neutrality), and Russia's approach has been informed by its unique international law doctrine and security posture that has favoured strategic independence and sovereign decision-making among states (consistent with Russia's recent 'Internet Isolation Law').

As regulators and law-makers

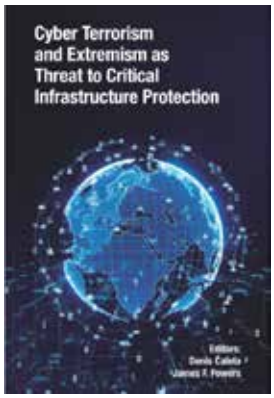
are pressed to address rapid advances in technology and the associated risks and effects of same on societies and communities, these new laws and regulations may be 'baking-in' the preferences and/or characteristics of the current leadership and trends, further shaping in enduring ways these emerging 'cyber security cultures'. For example, the current U.S. President Donald Trump has a personal background in business, while Russian President Vladimir Putin has a personal background in international law, and Europe's Cold War history has arguably made current leadership more sensitive to privacy rights - all of which are reflected in their respective laws and regulations, which are unlikely to be easily changed. Emerging cyber security cultures may in turn affect both how risk is managed and how strategic approaches are formed and evolve.

In the short- to medium-run, cyber security may benefit from enhanced strategic treatment, to address and mitigate the uncertainty and instability that currently characterizes the cyber security landscape, due to rapidly changing technology, uncertainty in relation to laws & regulations, significant liabilities & compliance penalties, jurisdictional variations, and conflicting state approaches, in the context of more frequent and severe threats and risks. Excessive uncertainty may be an obstacle to sector development, and may exacerbate the talent gap, disincentivize investment, and inhibit the ability of businesses to innovate, grow and scale-up.

Greater stability through enhanced strategic approaches may foster a more predictable and hospitable cyber security landscape over the long-run.

By Bonnie Butlin is the Co-Founder and Executive Director of the Security Partners' Forum

The book Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection has been published



The modern world is pervaded with complex risks and threats to the values that people, various organizations and states seek to protect. The set of threats that need to be taken into account are extremism and terrorism and their direct and indirect effects on endangering critical infrastructure. This is precisely the goal of the book that we are presenting here, which deals with these challenges.

The aim of the book Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection is to provide an insight into existing levels of risk and threats and available response options by analyzing the above from different theoretical frameworks, methodological discourses and social circumstances. This valuable work was created as a result of long-term cooperation between the Ministry of Defense of the Republic of Slovenia, Joint Special Operations University from Tampa, USA and the Institute for Corporate Security Studies, Ljubljana, Slovenia.

The editors of the book are Denis Čaleta, Ministry of Defense Republic of Slovenia and James F. Powers Jr., Joint Special Operations University from Tampa. While the chapter contributors are experts from Europe and the US.

After the Introductory part, the book is divided into two sections: the first, Extremism, Radicalization and Cyber Threats as an Important Security Factors for Countering Terrorism Processes; and the second, Cyber Terrorism and Security Implication for Critical Infrastructure Protection.

In total, the book has 204 pages, 11 chapters, Index, Summary of Contents, Biographical Notes about Editor and Contributors.

The first section of the book brings very interesting analyzes related to various forms of Extremism, Radicalization and Cyber Threats with special reference to: Re-assessing online Jihadi Extremism, European security challenges of return foreign fighters, Russian cyber operation, Radicalization as cause of terrorism with case study from Bosnia and Herzegovina, and Cyber threats in Kosovo.

The second section is specifically dedicated to protecting critical infrastructure from cyber terrorism and other various forms of cyber threats. Out of a total of six chapters, three are thematically devoted to the analysis of the situation in South-Eastern Europe, while the remaining three chapters deal with the analysis of historical and legal aspects of cyber-attacks on critical infrastructure, cyber threats to maritime critical infrastructure, and the possibilities of using artificial intelligence in anticipating threats towards critical infrastructure.

This book represents an extremely significant achievement written by practitioners and academic researchers and represents the 'state of art' of current knowledge of the analyzed areas. The book is intended for a wide audience of interested readers from students, analysts, public officials of various profiles, security experts, opinion and decision makers, and especially all those engaged in strengthening resilience and protecting critical infrastructure.

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

Critical Infrastructure Protection Starts at the Perimeter

Critical infrastructure sites are constantly at risk of vandalism, theft and attack. There are also concerns for regulatory compliance and for liability associated with trespassing. By adding deterrence and detection measures at the perimeter, such as fence sensors, intelligent lighting, and video analytics, intruders can be stopped before they cause damage to property or hurt themselves.

Deployed on their own or in multi-layered combination, perimeter security solutions can protect critical infrastructure sites of all sizes.

Detect Intruders Before They Get Inside

Perimeter intrusion detection systems are a first line of defense against intrusions. While there are many types of sensor technologies that protect perimeters, some are more suitable for critical infrastructure protection than others. When looking at different systems, consider these factors:

- Coverage – Does the system protect the entire perimeter (e.g. no blind spots)?
- Probability of detection (Pd) – Does the system quickly and accurately detect attempts to breach the perimeter every time?
- Nuisance alarm rate (NAR) – Does the system only generate alarms for real or simulated intrusion attempts? If the system generates alarms during normal conditions or high winds, security may start to suffer because of responder complacency.
- Ease of installation and

A high-security fence enhanced with a fiber optic perimeter intrusion detection sensor. Any attempt to cut, climb, or lift the fence fabric is immediately detected

configuration – How easy is the system to install and configure? Can the system be configured remotely from an equipment room so maintenance staff can avoid travelling out to the perimeter whenever an adjustment is required?

• Integration with Security and Video Management Systems (SMS/VMS) – Can the information generated by the system be presented in a way that improves situational awareness? For example:

o Can the SMS/VMS display the precise location of intrusion attempts on a map?

o Can the alarms be integrated with the VMS for automated camera control?

o Is there full logging of activity so that incident reports can be generated?

• Cybersecurity concerns – Can the system be hardened to keep physical security systems safe against computer-based attacks?

Fence-Mounted Sensors

Fence-mounted sensors turn existing fences into smart fences by detecting and locating attempts to cut, climb or lift the fence fabric. They are durable, cost-effective, field-proven, difficult to defeat, and work reliably in all weather conditions. When an intruder is detected, the generated alarm (which includes the intrusion zone or precise location) can be used to trigger other on-site security resources, including PTZ cameras, as well as deterrence devices like sirens, loudspeakers, and/or security lights. The system can be managed by security personnel at a centralized monitoring station, enabling them to assess the situation remotely and respond appropriately.

Fiber optic-based fence sensors are a popular choice for critical infrastructure sites, especially those with longer perimeters. These sensors are non-conducting, intrinsically safe in explosive atmospheres, and immune to lightning and EMI. Often with support for extended coverage distances, a single unit installed indoors in a safe location can protect a facility's entire perimeter. Using advanced sensing techniques like Coherent Optical Time-Domain Reflectometry (C-OTDR), the systems offer high-value security features such as precision ranging, environmental compensation algorithms, and cut immunity.

Precision ranging, a major technology improvement over previous generation "block" sensors, provides many benefits. Not only can intrusion location information be used to direct surveillance

cameras, but it also enables sensitivity levels to be adjusted for specific areas of the fence (for example, to accommodate for changes in fence construction). Ranging capabilities can also reduce nuisance alarms, as the system can distinguish between site/area-wide disturbances caused by high winds and a legitimate intrusion attempt. Finally, ranging reduces operational costs by enabling maintenance staff to quickly locate and resolve issues.

A common concern with fence-mounted sensors is what happens in the event of a cable cut. When this happens, either accidentally or in an attempt to defeat the sensor, the system immediately reports the incident, including its exact location. Moreover, systems based on time-domain reflectometry technology retain the ability to detect and localize intrusions up to the point of the cut. When installed in a redundant-loop configuration,

the sensor becomes cut-immune and continues to provide detection on the full perimeter even after a cable cut.

Gates along a perimeter fence, typically equipped with electronic access control and closely monitored via surveillance cameras, can also be enhanced with perimeter sensors. Swing gates can use the same fence sensor protecting the perimeter by routing the cable onto each moving panel (the cable is trenched from one side to the other). For sliding gates other technologies are more effective. If the area can be viewed from a clear, overhead location, virtual detection zones can be monitored via outdoor people and vehicle tracking video analytics. Another solution is wireless gate sensors, where an embedded accelerometer analyzes gate movement in three-dimensions, enabling the sensor to distinguish between gate activity, intrusion attempts, and environmental conditions. The sensor communicates with a nearby processor over an encrypted and monitored wireless link. If a suspicious event occurs – intrusion attempt, communication link failure, or an attempt to remove the sensor from the gate – an alarm is immediately generated.

Intelligent Lighting

Intelligent, low-voltage lighting is a new trend in perimeter security. Installed on fences outside of designated hazardous areas, LED-based luminaires provide uniform, targeted wide-spectrum illumination along the fence line. This improves the quality of video feeds by avoiding hot spots while a high Color Rendering Index (CRI) value means colors are accurately

Intelligent lighting system illuminates the fence line, detects intrusion attempts, and deters intruders by strobing or increasing intensity at the intrusion location

shown, greatly assisting security personnel with identification. LED-based lighting also dramatically reduces electrical consumption while a 10-year-plus lifespan virtually eliminates maintenance.

These benefits are useful but how do they relate to perimeter sensors? This is where "intelligent" comes into play. Sensors embedded in the luminaires themselves detect the fence vibrations caused by someone attempting to cut, climb or lift the fence fabric. In addition to notifying the SMS/VMS, the luminaires in the immediate area can instantly switch to full power or strobe. Knowing they are detected, potential intruders may rethink their actions.

Video Analytics

The effectiveness of video analytics has greatly improved over recent years, benefiting from today's higher performance/lower cost computing resources, as well as HD cameras with impressive low-light, infrared and thermal capabilities. Advances in computer vision research have led to the development of sophisticated video analytic software optimized for outdoor/indoor people tracking, left/removed object detection, PTZ auto-tracking, face and license plate recognition, crowd detection, and more. These software modules may be included as part of a VMS or embedded on individual cameras.

Rather than being an alternative to traditional fence-mounted sensors, video analytics offer a new set of technologies that greatly enhance perimeter security at relatively low cost. For example, video analytics can leverage a facility's existing camera infrastructure to detect and track people near both sides of perimeter fences, providing early warning of potential security events before they can occur.

Video surveillance footage showing a site protected by both an outdoor people tracking video analytic and an intelligent lighting system.

Building Trust and Co-operation through Discussion and Dialogue

Co-Hosted by:

HELLENIC REPUBLIC
Ministry of Migration & Asylum

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
NS&RC

Media Partners:

BORDER SECURITY REPORT
WORLD SECURITY REPORT
World Security-index.com

Cybersecurity of Physical Security Devices

Whenever physical security devices are deployed, they themselves have the potential to become cybersecurity targets, often with the intension to be used as a springboard for targeting other critical systems. To keep physical security devices from introducing new vulnerabilities, site owners and integrators should ensure:

- Security devices are physically protected against tampering, as well as being configured to generate alarms if tampering does occur
- Inter-device communications are separate from external network connectivity
- Software applications use encrypted communications
- Software vendors conduct Penetration Testing (PEN Testing) by reputable third parties

Increased Security, Increased Public Safety

Perimeter intrusion detection technology, including fence-mounted sensors, intelligent lighting, and integrated video analytics can help meet the goal of reliably detecting attempts to bypass perimeter fencing and gates. The key concerns when evaluating these systems for use at critical infrastructure facilities is to ensure they reliably detect intrusion attempts while avoiding false alarms, avoiding blind spots and other security gaps, are cost-effective for sites with long perimeters, and can be properly integrated to enhance overall security response capabilities while not exposing the organization to additional cybersecurity risks. Implementation of the appropriate physical technology along with security practices can help mitigate risks to environmental and public safety.

Video surveillance footage showing a site protected by both an outdoor people tracking video analytic and an intelligent lighting system

Senstar Product Manager Stewart Dewar discusses how fence sensors, intelligent lighting, and video analytics can provide early warning of potential security events before they occur.

Call to action on international standards

The Riyadh International Standards Summit concluded with the call to action for "each country to recognize, support, and adopt international standards to accelerate digital transformation in all sectors of the economy to help overcome global crises, such as COVID-19, and contribute towards the achievement of the United Nations Sustainable Development Goals (SDGs)".

The Call to Action emphasizes international standards' important role in the implementation of the United Nations' Global Agenda aimed at achieving all 17 SDGs by 2030. "Today's global health crisis has highlighted the need to continue investing in our digital future, through investments to drive infrastructure development, connect the unconnected, and build confidence and trust in digital technologies: elements which are all crucial to the achievement of the SDGs."

Reflecting on the issues addressed, ISO Secretary-General Sergio Mujica saw a strong common spirit shared by all participants. "This recognition raises the bar on supporting international standards and illustrates the critical role each country can play in overcoming our common challenges and boosting synergies for all. We look forward to the international community answering the call to recognize, support and adopt international standards as a key instrument for economic and social development."

A word from the Chairman

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

International Association of CIP Professionals

Try not to be distracted….

It is probably an understatement to say that this year has been both unique and extremely concerning for everyone across the globe. Something as all-consuming and complex as a pandemic, brings about a host of challenges and presents a breadth and depth of vulnerabilities across all aspects of life that would have been difficult to imagine some 12 months ago. It is at times like these, when our attention can be diverted, and we must strive to remain ahead of the curve when seeking to ensure the protection and resilience of our critical infrastructure systems.

November is Critical Infrastructure Security & Resilience Month (NCISRM) in the United States. A time when the USA as a nation review their commitment to protecting and securing their essential systems and services. They use this as an opportunity to undertake a range of initiatives and to highlight examples of the work that they are doing within the Department of Homeland Security(DHS) and with industry, responders, international partners, and other stakeholders to keep their critical infrastructure systems on the cutting-edge.

The International Association of Critical Infrastructure Protection Professionals (IACIPP) is very supportive of initiatives such as these. Initiatives which bring into focus the range of threats and vulnerabilities that continually need to be considered and provides good practical advice to the infrastructure community.

Having looked at some of the NCISRM examples of activities it was pleasing to note that preventing terrorist acts remains an absolute focus and is not being (too) distracted by the complexities and challenges that the coronavirus pandemic has placed upon them. Protecting Critical National Infrastructure from terrorism must remain as a key focus for all involved, whether it be through policy development or security and resilience implementation.

This month (November) provides us with a distressing reminder of the devastation and impact that terrorism has on individuals and society as a whole. It marks five years since the co-ordinated terrorist attacks that took place in Paris, which claimed 130 lives and left 350 people injured. We continue to hear the details of the horrendous attack that took place at the Ariana Grande concert at the Manchester Arena in 2017 through the public inquiry. Then, more recently, the incidents across Europe (6 since the end of September) are a stark reminder that acts of terrorism remain a key issue for many countries even during the Covid-19 pandemic.

Such is the concern over the series of European attacks the United Kingdom's threat level was raised to 'Severe' by the Joint terrorism Analysis Centre at MI5. This action was taken immediately following the shootings in Vienna on the 2nd November and means 'An attack is highly likely' within the UK. This is not a decision that would have been taken lightly. It will have been based on the careful analysis of a range of information and intelligence and sends a clear message to the UK's business communities and the population in general, about additional and sustainable protective security measures being put in place and the need for an increased level of vigilance from all.

The Results Are In...

The IACIPP Poll

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

Q. How often does your security officer program receive budget and financial pressure from your senior executives?

- Never - 56%
- On an annual basis - 33%
- Sometimes (eg. six-monthly) - 0%
- Seldom (eg. quarterly) - 0%
- Very frequently (eg monthly) - 11%

Even though the attacks mentioned may not have been directly focused on our critical national infrastructure it is a timely reminder that the threat of terrorism remains a reality.

So, while we all continue to try to keep each other safe from the spread of the coronavirus, adhering to the governments mantra of 'Hands – Face & Space' - let us all remember not to be (too) distracted, as terrorism has not gone away, and will not be fixed by a vaccine in the new year.

I hope that you and yours stay safe and healthy as we move into the festive period and that you all, no matter what restrictions you may face, manage to get some quality time with your families and loved ones.

John Donlon QPM FSyI
Chairman IACIPP

Brian Harrell Welcomed as Strategic Advisor to IACIPP

The International Association of Critical Infrastructure Protection Professionals (IACIPP) is delighted to announce the appointment of Brian Harrell as Strategic Advisor to the Board.

In 2018 Brian was appointed by the President of the United States to serve as the sixth Assistant Secretary for Infrastructure Protection, at the Department of Homeland Security. He also served as the first Assistant Director for Infrastructure Security at the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

Brian currently serves as the Vice President and Chief Security Officer (CSO) at AVANGRID, an energy company with assets and operations in 24 states. He is responsible for the companies physical and cybersecurity, security compliance, enterprise risk governance, and fire protection units.

His breadth of experience spanning both the private sector and his involvement at the highest levels of governmental/ policy positions will no doubt add great value to our Association.

Brian is nationally recognized for his efforts on critical infrastructure protection, continuity of operations, and enterprise risk management. Advising corporations throughout North America, Brian has worked to increase physical and cybersecurity mitigation measures designed to deter, detect, and defend critical systems.

Brian is also a Senior Fellow at Auburn University, McCrary Institute For Cyber and Critical Infrastructure Security where he serves as an advisor on infrastructure protection and cybersecurity policy initiatives.

Brian has spent time during his career in the US Marine Corps and various private sector agencies with the goal of protecting the United States from security threats.

John Donlon QPM, Chairman of the IACIPP said, "I am delighted that Brian has accepted the position as Strategic Advisor with us. He has a wealth of experience both as a security practitioner and in an oversight capacity, so will be a tremendous asset to the and the global CNI community. "

"The IACIPP continues to welcome new members who share the desire to engage with likeminded individuals seeking to enhance the protection and resilience of infrastructure across the globe." Concluded Mr Donlon.

Latest Resources from IACIPP

Members of IACIPP can enjoy benefits including access to a range of online resources including video presentations, conference papers and magazine back issues, as well as a whole range of White Papers.

Latest White Papers include 'Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection book' by Denis Caleta, James F. Powers and 'Indication of Critical Infrastructure Resilience Failure' from Assoc. Prof David Rehak, Ph.D., VSB – Technical University of Ostrava, Faculty of Safety Engineering.

More details and access to the Resources and White Papers can be found at www.cip-association.org.

Effective Security Options for Healthcare Facilities

The police recorded a 4% decrease in crimes across England and Wales in the 12 months ending June 2020, attributed to the ongoing Coronavirus pandemic. Crimes such as general theft have reportedly dropped overall by 15%, with the most significant change year on year seen in April to June 2020, when there were 43% fewer theft offences.

However, sadly the effects of the pandemic mean that healthcare facilities have become even more vulnerable to attack. Restricted visitor guidelines, and increased demand for critical PPE items such as masks and gloves, meant these institutions were exposed to opportunistic criminals. Staff cars and bikes have been stolen, ambulance tyres slashed, hand gel dispensers ripped from walls, and defibrillators and oxygen canisters were key targets for burglars. Given the constant, essential work carried out by health services, the security of staff and physical assets must be fully considered to protect them from opportunistic criminals.

The ongoing COVID-19 pandemic has placed enormous pressure on our essential healthcare services, adding additional risks and complexity. Facilities managers and specifiers now need to consider these factors to provide adequate protection for patients, visitors, property and assets.

One new issue involves securing additional sites. Additional, temporary areas, built specifically for Coronavirus patients are now

common across many hospitals to enable them to cope with the excess demand on their services. Often entirely disconnected from the main hospital, these sites require their own physical security measures to ensure they are adequately protected.

Facilities managers are seeing the benefit of combining fencing, gates, storage enclosures and access control as part of a complete solution to secure such buildings. With the right combination of security measures in place, it's possible to operate effectively 365 days a year, through the pandemic and beyond.

Robust Access Control

Hospitals are fast-paced environments where life and death outcomes are often time-critical. The promptness of patient admittance and staff movement around the site is hugely important. As such, efficient, seamless access is vital. All gates and access points around the perimeter need to be assessed and considered, and each of the access points should be installed and controlled centrally, or regularly monitored.

Another principal consideration is the diverse range of vehicles that require access, including ambulances entering and exiting at speed, lorries carrying crucial medical supplies, and staff and visitor vehicles. The appropriate solution should ensure that all visitors, including site staff, should have access to secure parking, while also allowing emergency vehicles to get in and out of the site unhindered, and without ever compromising the safety of pedestrians.

When designing pedestrian and vehicular access: gates should be DDA (Disability Discrimination Act) compliant. It is important to note that the design of fencing and gates specified needs to accommodate rapid evacuation and access for emergency services.

Secure Parking Solutions

Multi-storey car parks provide an effective way of parking cars, using far less ground area than conventional parking solutions. Commonly used alongside healthcare facilities, they provide low building costs per vehicle space and a greater degree of flexibility, which ensures faster parking and retrieval times.

These structures need specialist fencing to secure them effectively. Jacksons has worked on several multi-storey car park sites, including one at Lister Hospital, Hertfordshire. Over 1,000 metres of steel welded mesh panels were specified for this development. They created an ultra-secure barrier to stop members of the public from falling through open gaps in the car park's steel structural framework, yet also delivering an aesthetically pleasing solution which did not impede surveillance.

The security in hospital car parks can be strengthened via rising arm barriers or bollards. These solutions control access and actively separate pedestrians from vehicle traffic once inside the multi-storey structure, thus reducing the risk of accidents.

Promoting Wellness through Aesthetics

Creating a welcoming environment is extremely important when specifying security options for hospitals. Razor or barbed wire may be effective deterrents to potential trespassers, but they create an intimidating and harsh aesthetic, far removed from the sense of wellbeing these developments should promote.

Vertical bar security fencing or welded mesh panels both offer visual appeal and a high level of security. These options deliver strong boundary protection and, crucially, excellent visibility for surveillance, surpassing any alternatives.

For recreational or recovery areas requiring a delicate appearance, such as gardens, timber fencing is a good option. Timber has a natural, welcoming appearance and promotes a sense of wellbeing and privacy. Wood, in the form of acoustic fencing, can also provide a high level of noise protection,

transforming gardens or terraced areas into little oases of calm, ideal for recovery and relaxation.

Outdoor Storage Areas

Hospitals and other medical facilities produce a large amount of hazardous medical waste which requires secure storage on-site before it's taken away. Hospitals have a responsibility to ensure these areas are secured using risk-appropriate fencing to avoid potentially dangerous materials getting into the wrong hands.

Risk assessments are also vital to ensuring an appropriate solution is installed effectively. For facilities at risk of criminal activity, products accredited by standards including Secured by Design or the Loss Prevention Certification Board's LPS 1175 have been shown to reduce the likelihood of crime. It's also best practice to assess any climbing

aids such as lamp posts or trees located near the storage areas. The surrounding fence should also be high enough to deter any attempts at climbing.

The market is brimming with a wide variety of robust, and easy-to-install security options, suitable for healthcare facilities. The most crucial factor is to ensure each institution is considered on a case-by-case basis, as a unique project, as each site is different and will require a tailored plan to keep everyone safe.

by Peter Jackson, Managing Director, Jacksons Fencing

African Terror Groups 'Rebrand' as Islamic State

Ituri, in the far north east of the Democratic Republic of the Congo is almost capable of being a paradise on earth, the combination of being virtually on the Equator coupled with being over 1000 metres above sea level means that it's possible to grow two, or even three, crops a year. It also possesses an almost obscene wealth in precious metals ranging from gold to cobalt.

Alas, though, it is also an area plagued by insecurity with unending conflict between the forces of the far-away government in Kinshasa and local armed opposition groups who all seek, in some measure, autonomy if not absolute independence.

One of these groups in particular, the Allied Democratic Forces, has been responsible over the years for numerous attacks on the government army, FARDC(Armed Forces of the Democratic Republic of the Congo) at their various bases not just in Inturi but also in the neighbouring provinces of Beni and the Kivus, North and South. Their attacks have also targeted the United Nations peacekeeping force in the Congo, MONUSCO, since in the case of the Congo the UN has interpreted its' role as one of support to the national government .Although the ADF began life primarily as a Ugandan resistance to the authoritarian regime of Yoweri Museveni over recent decades it has recruited increasingly from within the eastern Congo.

However it is now clear that the ADF has established increasingly close ties with ISIS over the last couple of years, starting with online posts referring to themselves

as the Madinat Tauheed Wal Mujahadeen and this resulted in ISIS publicly recognising the ADF as an affiliate in late 2018 and thus claiming responsibility for ADF attacks starting in April last year on a FARDC base near Kamongo and continuing also into this year with frequent attacks on the government army and UN peacekeepers, with the result that well over 300 civilians are reported also to have been killed in the ensuing operations.

However these attacks have been conducted tactically in the same way as always, using small arms and machetes ,and this prompts one to wonder whether the 'rebranding' as ISIS is thus purely an attempt to 'cash in' on greater public awareness of ISIS ? Certainly the ADF do not seem to have adapted their tactics to fall more in line with those of IS, for example a copy of an Arabic textbook produced by the Islamic State's Research and Studies Office was found by Congolese troops on the body of an enemy combatant killed in a firefight, so the ADF are clearly aware of alternative tactics.

Certainly, though, they have received some financial support via their links with the Islamic State, including payments from sources in the UK, South Africa and Syria being sent to the ADF via a contact in Kenya and certainly captured ADF combatants over the last 18 months have included a South African, a Tanzanian, Kenyans, Rwandese, Burundians, one Brit and a South Sudanese, all a far cry from the movement's roots as a local opposition to remote central governments.

This pattern of what can only be called 'rebranding' has also been observed in Mozambique

the author and colleagues inspect surrendered weapons at the United Nations base in Bunia, D.R.Congo

recently as well as in Mali, where a plethora of insurgent groups have morphed into Jama'at Nasr al Islam wai Muslimin (JNIM), whose numbers were recently increased by about ten percent when the new government, in a gesture of conciliation, released amongst others, fighters suspected of involvement in terrorist attacks on hotels in Mali, Ivory Coast and Burkina Faso that killed many Westerners. Alas the government's hopes may be thwarted not least because the JNIM does not want to be seen as less Islamic than its' main hearts-and-minds rival the Islamic State in the Greater Sahara (see WSR for March/April 2019). A particular concern in the case of Mali is the presence of European troops with a large EU mission training the army , along with military assistance from the USA, plus some 5,100 French troops avowedly fighting jihadists. The UN also has some 15,000 'peacekeepers ' in Mali.

Like their counterparts in the D. R. Congo and elsewhere these peacekeepers have suffered from their association with the government in power. Over the last twenty years we have seen politicians in the Security Council attempt to tweak the words peace keeping to mean , in practice, peace making – which is a vastly different undertaking, requiring not only a different mind set but also enhanced training and equipping. Whereas the traditional role of UN forces in a conflict zone was to protect the civilian population from depredations by any and all armed groups, increasingly they find themselves being used to support the faction in power who are supposed to have legitimacy. This then means that UN forces are seen by the indigenous population not as guarantors of their safety but as supporters too often of their oppressors. It is a very long way from Ituri and the Kivus to Kinshasa just as it is from Timbuktu to Bamako. The people are different and so are their aspirations. We in the West need to be more flexible in our approaches to conflicts in Africa and, indeed, elsewhere in the world, perhaps seeking to understand before we seek to condemn.

Transnational Access to Electroni Evidence for Crimial Cases: Trends and Latest Developments within EU and Beyond

Europol, Eurojust and the European Judicial Network publish today the second annual edition of the SIRIUS EU Digital Evidence Situation Report. The report outlines the status of EU authorities in retrieving electronic data held by foreign-based online service providers (OSPs) in 2019. Cross-border access to digital information is paramount to an ever-increasing number of investigations, ranging from economic crimes and drug trafficking to terrorism, cybercrime and child sexual exploitation. In one case mentioned in the report, law enforcement officers were able to find an abducted child after requesting GPS data from a social media platform.

This report encompasses extensive information gathered from over 325 surveyed officials of EU Member States' law enforcement and judicial authorities, together with relevant input coming from a dozen major OSPs and reference to national legislation.

The volume of cross-border requests submitted by EU authorities to OSPs increased significantly in 2019 with a large majority of them issued by Germany (37.7% of requests), France (17.9%) and the UK (16.4%). Requests to access electronic data doubled in Poland and nearly tripled in Finland. Furthermore, emergency disclosure requests increased by nearly half in one year.

In order to better inform authorities and advance future investigations and prosecutions, the report focuses on the most important types of data in criminal cases. However, the acquisition of basic information on users (such as IP addresses used at registration, email addresses or phone numbers) suffers specific challenges. These relate for example to the length of the procedures in place, the very limited amount of time in which data is available and the fact that companies have different standards when cooperating with authorities.

Officers Foil Fraudsters from Stealing €40m in Payment Card Scam

Carding Action 2020, an operation led by law enforcement agencies from Italy and Hungary and supported by the UK and Europol, targeted fraudsters selling and purchasing compromised card details on websites selling stolen credit card data, known as card shops, and dark web marketplaces.

The operation sought to mitigate and prevent losses for financial institutions and cardholders. Group-IB and card schemes worked in close cooperation with police authorities from the countries involved. During the three-month operation, 90 000 pieces of card data were analysed and prevented approximately €40 million in losses.

Europol facilitated the coordination and the information exchange between law enforcement authorities and partners from the private sector. Europol's experts provided operational analysis on large volumes of data and supported with expertise in the field of payment card fraud.

"Cybercrime can affect all aspects of our daily life, from paying in the supermarket, transferring money to our friends to using online communication tools or Internet of Things devices at home. Cybercriminals can attack us in different ways and this requires a robust response not only from law enforcement, but also from the private sector," said Edvardas Šileris, Head of Europol's European Cybercrime Centre (EC3). "With more than €40 million in losses prevented, Carding Action 2020 is a great example of how sharing information between private industries and law enforcement authorities is a key in combating the rising trend of e-skimming and preventing criminals from profiting on the back of EU citizens," he added.

The expansion of e-skimming attacks targeting merchant point of sale systems and e-commerce merchants also influenced the significant increase of prevented losses. As reported in the iOCTA 2020, card-not-present fraud is a criminal threat in constant evolution, generating millions of euros of losses and affecting thousands of victims from across the EU.

Artificial Intelligence and law enforcement: challenges and opportunities

The disruption of AI-controlled systems, AI-authored fake news, and the use of driverless systems as weapons were identified as probable AI-enabled future crimes during the INTERPOL-UNICRI Global Meeting on Artificial Intelligence for Law Enforcement.

- The potential misuses of AI;
- Law enforcement use of AI, including special panels on the use of AI to combat online child sexual abuse and terrorist use of the internet and social media;
- Latest AI developments for law enforcement in the private sector;
- Developments in related areas such as the use of AI in the criminal justice system, AI and criminal liability and the interaction between AI and drones.

Case studies were shared by speakers from the Biometrics Institute, the World Economic Forum, the private sector and other international organizations, who highlighted the clear need for collaboration, the inclusion of interest groups, and diversity to develop widely-accepted and useable frameworks. These findings were echoed by informal polls conducted with participants during the week-long meeting.

There was a consensus that a more data-driven and scientific approach to criminal investigations would be crucial in tackling AI-related threats. These observations will be taken into account in the development of a "Responsible AI Innovation Toolkit for Law Enforcement". Transparency, accountability, and trust also emerged as crucial factors in the development of the AI Innovation Toolkit..

INTERPOL warns of organized crime threat to COVID-19 vaccines

INTERPOL has issued a global alert to law enforcement across its 194 member countries warning them to prepare for organized crime networks targeting COVID-19 vaccines, both physically and online.

The INTERPOL Orange Notice outlines potential criminal activity in relation to the falsification, theft and illegal advertising of COVID-19 and flu vaccines, with the pandemic having already triggered unprecedented opportunistic and predatory criminal behaviour.

It also includes examples of crimes where individuals have been advertising, selling and administering fake vaccines.

As a number of COVID-19 vaccines come closer to approval and global distribution, ensuring the safety of the supply chain and identifying illicit websites selling fake products will be essential.

The need for coordination between law enforcement and health regulatory bodies will also play a vital role to ensure the safety of individuals and wellbeing of communities are protected.

Shaping an international response against criminal finances and misuse of cryptocurrencies

Representatives from law enforcement and the judiciary, Financial Intelligence Units (FIUs), international organizations and the private sector have met virtually to shape international cross-sector solutions against the criminal use of cryptocurrencies.

Recent increases in the number and quality of investigations in the field of cryptocurrency-facilitated crime and subsequent money laundering means that law enforcement and other public entities are continuing to enhance their level of knowledge and expertise in this crime area. In this regard, the conference served as an opportunity to underline the need for countries and jurisdictions to increase the exchange of tactical information and best practices, so that lessons learnt by one entity can be useful to others.

With the conference underlining the need to extend capabilities on how to investigate virtual assets, and the necessity of applying rules to regulate virtual asset service providers to prevent money laundering, INTERPOL's Director Organized and Emerging Crime Ilana de Wild said:

"A multi-agency and multi-disciplinary approach involving both the private and public sectors is key to tackling criminal finances and the misuse of cryptocurrencies. By combining the expertise and data on financial crime held by the private sector with the investigative capabilities of law enforcement, we can enhance our collective capabilities and scale up efforts against criminal finances."

ENISA Report Highlights Resilience of Telecom Sector in Facing the Pandemic

ENISA is releasing its 'Telecom Security During a Pandemic' report at the 32nd meeting of EU telecom security authorities. Underlining the current strength of the sector in the face of the pandemic, the report also calls for increased cooperation, as telecommunications become more and more essential for Europe's society and economy.

the European Union Agency for Cybersecurity (ENISA) is releasing its Telecom Security During a Pandemic report, which gives an overview of initiatives and good practices in the telecom sector to mitigate the impact of the pandemic. The report highlights the resiliency of telecom networks and services during the pandemic, which sustained major fluctuations in usage and traffic. The report also points to the need for increased cooperation between the public and private sectors as the role of telecoms expands.

The COVID-19 pandemic triggered major changes in the use of telecom networks and services: employees are teleworking; students are learning online; people are communicating via video. Almost overnight, the telecoms sector became a lifeline for Europe's citizens and businesses. The pandemic put the telecom sector to the test with traffic peaks and spikes, combined with a national crisis and difficult working circumstances. Peaks followed major announcements about the pandemic; spikes occurred after news of lockdowns and closures. The diagram below shows the correlation between COVID-19 cases and fluctuations in network traffic on a single timeline. This is an example of one provider in one EU country, but it is representative of what other operators in Europe observed.

JRC proposes a new framework to raise awareness and resilience against hybrid threats

A new conceptual framework on hybrid threats designed by researchers aims to increase the understanding of hybrid threats and facilitate the development of effective measures to improve resilience against these threats.

The 'hybrid threats' concept refers to coordinated action conducted by hostile state or non-state actors with the deliberate goal to undermine or harm democratic states.

Although the topic is high on the political agenda, our understanding of hybrid threats is often limited to past experiences and known forms of interference, such as disinformation and terrorism.

Working together with the Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), the JRC has developed a conceptual framework, which describes the components of hybrid threats in terms of actors, their objectives, tools, the domains that can be compromised as well as the different phases of action.

The work aims to facilitate the early detection of hybrid threats, the identification of gaps in preparedness and response and the development of effective measures to counter this complex phenomenon.

The research teams call for a whole-of-society approach, which brings together all civil, military and political actors for a more effective response to hybrid threats.

CISA releases the insider threat mitigation guide

The Cybersecurity & Infrastructure Security Agency (CISA) has released their Insider Threat Mitigation Guide for organizations who have individuals entrusted with access to or knowledge of their organization, who represent potential risks, which includes current or former employees or any other person who has been granted access, understanding, or privilege.

Organizations of all types and sizes are vulnerable to insider threats. The CISA Insider Threat Mitigation Guide is designed to assist individuals, organizations, and communities in improving or establishing an insider threat mitigation program. It offers a proven framework that can be tailored to any organization regardless of size. It provides an orientation to the concept of insider threat, the many expressions those threats can take, and offers an integrated approach necessary to mitigate the risk. The Guide shares best practices and key points from across the infrastructure communities.

Canadian authorities recently conducted performance testing on the soon to be released SkyTrack system from OpenWorks

This follows the integration testing that was completed in Germany by ESG Elektroniksystem- und Logistik-GmbH, earlier this year.

Canadian authorities represent the first end-users to operate the system, as they stay at the forefront of C-UAS technology. Testing SkyTrack as part of their search for the latest generation of optical UAS detection and tracking technology.

Pilots flew Class 1 UAS such as the DJI Inspire and

Mavic UAS to evaluate the autonomous detect and classification ranges achievable in both day and night environments. SkyTrack was able to successfully detect and track the DJI Mavic out to 2km, showing world class performance. The DJI Inspire was tracked to 2.5km and the pilots could not out-manoeuvre the 'lock' of SkyTrack.

The system was manually cued onto the target during these tests which demonstrated a standalone operational capability. To achieve the greatest performance, SkyTrack is integrated using the proven SkyWall interface, receiving data from drone detection sensors, RF or radar, for a rapid handover to smooth target tracking. This has already been proven with Flir, Qinetiq and Robin Radar systems previously.

Kromek has launched the D5 RIID, the world's smallest high-performance radioisotope identification device ("RIID")

Kromek has launched the D5 RIID, the world's smallest high-performance radioisotope identification device ("RIID"). The ruggedised device, with ultra-low false alarm rate, is designed for homeland security, military and industrial use.

The D5 RIID was developed under a programme with the Defense Threat Reduction Agency of the US Department of Defense. It detects a wide range of sources, including special nuclear material and mixed, shielded and heavily masked configurations. It provides high accuracy dose measurement and has an industry-leading ultra-low false alarm rate of less than 1 in 24 hours. The D5 RIID combines this advanced

performance with being small, lightweight and easy-to-use – capable of being operated in one hand. It can also be used when wearing all levels of PPE, including gloves. It offers multiple modes of configuration, including being able to provide app-based training, and can be easily integrated into standard and custom networks.

It is the first device to be launched in Kromek's new D5 product range, which expands the Group's radiation detection portfolio to encompass devices specifically designed for more challenging use cases and harsh environments. This next-generation of product has a larger crystal, which enables higher accuracy and sensitivity – capable of detecting mixed, shielded and heavily masked configurations including special nuclear material – as well as being ruggedised.

Dr Arnab Basu, CEO of Kromek, said: "We are delighted to have launched the D5 RIID, which truly sets a new benchmark in radioisotope identification. The level of accuracy, combined with small size, far exceeds competing military standard detectors, enabling the rapid identification of radiological threats. As the first of our new D5 range, this device expands our portfolio to provide products ideal for use in harsh environments and for more challenging applications alongside our existing D3 solutions that are aimed at fleet deployment for large-scale networking across urban areas. We are proud to be continuing to drive innovation in this crucial area to enable rapid, informed decisions to be made in response to a radiation threat wherever it may appear."

CRDF Global Awarded a Department of State Grant to Support Cyber and Maritime Security in Cyprus and Lebanon

CRDF Global announced that is has been awarded a grant by the U.S. Department of State's Export Control and Related Border Security Program (EXBS) to improve cybersecurity defenses among maritime port authorities in Cyprus and Lebanon.

CRDF Global will work in partnership with maritime and cyber authorities in Cyprus and Lebanon to improve country-specific defense strategies against malicious, state-sponsored threats to cyber and port security. Through specialized training and action plan development to secure maritime operations from cyberthreats, CRDF Global will support Lebanon and Cyprus to prevent proliferation-related transfers and networks.

"Cyprus and Lebanon both play key roles in Eastern Mediterranean maritime affairs — Cyprus, due to its geostrategic location, and Lebanon as a critical transshipment hub and the resulting vulnerability as an entry point for dual-use materials. The recent horrific explosion in Beirut is a stark reminder of the importance of effective port security," said Susan King, Director of Strategic Trade Controls and Border Security at CRDF Global.

ODSecurity Sells First-Ever Body Scanner into Dominican Republic Prisons

Netherlands based, ODSecurity announces the sale and installation of their Soter RS body scanner into Las Parras Correction and Rehabilitation Centre, commonly known as "La Nueva Victoria" in Guerra, in the Dominican Republic.

The installation, the first of its kind in the Dominican Republic, was part of a tender alongside OD's partner for this contract, Smart Logistics International, for the supply of security and communication equipment to Direccion General de Prisiones, Dominican Republic.

On the 10th August 2020, the then president of Dominican Republic, President Danilo Medina delivered the first phase of the new penitentiary alongside the Attorney General of the republic, Jean Alain Rodrigues. The country's new President, Luis Abinader took office on the 16th August 2020. The new President has put police reforms at the top of his security priorities.

The Soter RS full body scanner, is an advanced security x-ray system that will detect anything on, or in a body. For the first time, in the history of prisons in the Dominican Republic, contraband hidden on a person, ingested or camouflaged whether organic, metal or plastic will be detected, providing the operator with a medical grade image showing the clear difference between human tissue and the contraband.

The Dominican Republic has, since 2003, developed a "New Prison Management Model" which aims to apply the international principles of human rights and the United Nations Mandela Rules – the focus of which is human rights and rehabilitation rather than repression.

The coordinator of the New Penitentiary Management Model, Hilda Patricia Lagombra said, "The Las Parras Penitentiary Complex is an enclosure in which we will have eight Correction and Rehabilitation Centers where approximately eight thousand inmates who are currently in the La Victoria prison will be housed, a great step within the Penitentiary Reform project, since the overcrowding, the violation of human rights and the mistreatment of inmates will become a thing of the past."

Radio Physics Solutions announce the global launch of Optracon, concealed threat detection solution

Radio Physics is pleased to announce the global launch of Optracon, stand-off threat detection solution. Optracon is a fully automated multi-sensor fusion solution for detecting concealed mass casualty threats at distances of up to 30m. Harvesting data from state-of-the-art radar, video analytics, LiDAR, machine learning algorithms and artificial intelligence to produce the world's leading concealed threat detection solution.

Following more than 18 months development, greatly aided with the support of European Commission funding from a Horizon 2020 SME instrument grant. The product has completed successful final trials, held recently at a sports stadium in Warsaw, Poland. Radio Physics is pleased to announce the performance

of the technology greatly exceeded expectations and that of previous generation products, and Optracon™ has been released to the general market.

Optracon tracks people in crowds by fusing modern 3D video analytics and LiDAR technologies to provide an intelligent multi-sensor digital understanding of groups and flows of people – as a collation of 3D objects with previous and forecast coordinate paths.

This contextual view provides both a human and machine-based view of people that can/should be, or already have been, scanned by Radio Physics mm-wave MiRTLE OM30 threat detection radar sensors. Each radar has its own boresight camera that uses the same video analytic software as the context setting overhead camera(s) to focus on relevant body areas for mm-wave scanning as well as post scan tagging. If necessary, a direct drive gimbal moves the radar unit through either small or large angular rotations at speed to target and scan individuals within a region of interest.

Mark Pritchard, CCO said: "We are delighted with the launch of Optracon, it is exciting times at Radio Physics and are looking forward to working with our partners in the coming months on the many already identified opportunities across Europe and globally."

Gary King, CEO added "we extend our sincere thanks to the European Commission and to our hosts and partners in Poland, without whose financial and logistical support this initiative would not have been possible".

Smiths Detection HazMatID Elite Command Systems expand MABAS-Illinois Hazmat response capabilities

Smiths Detection has fulfilled a multi-year $2.2 million contract with Mutual Aid Box Alarm System (MABAS) of Illinois to expand their hazardous materials response capabilities with HazMatID Elite handheld chemical identifiers.

SDI began supplying MABAS with HazMatID Elite identifiers in 2016 as part of a strategy to equip their regional HazMat teams with

Fourier-transform infrared (FTIR) technology to analyze suspicious substances on emergency scenes. In addition, the equipment has been upgraded with Smiths Detection's Command System solution, which provide responders with the ability to compare unknown substances to a database of more than 35,000 chemicals, including toxins, explosives and narcotics, helping them both accelerate response times and obtain critical, or life-saving, information quicker.

Don Davids, President of MABAS-IL commented, "HazMatID Elite continues to be a trusted tool that we use to safeguard our communities. Upgrading to the Command System not only improves our response ability, but also helps us build upon the expertise we have gained over the years."

MS Tech's Homeland Security and Defense Division Expands the Detection Capabilities of its Sensors Covering Now Emerging Homemade Explosives, Fentanyl and a Range of Synthetic Opioids to Meet with Current Global Threats

MS Tech has announced that its homeland security and defense division, expands its detection capabilities covering chlorates, perchlorates, fentanyl and a range of synthetic opioids, to meet with current growing threats around the world. The latest capabilities enable defense forces, HLS agencies and first responders to detect and identify dangerous chemical threats within seconds.

Fentanyl is a powerful synthetic drug similar, yet much more potent, to morphine and heroin. Law enforcement and first responders have a high risk in being exposed with such drugs, unknowingly, from its many forms and any breathing or direct contact exposure can be deadly and lethal. Chlorates and Perchlorates are very powerful oxidizers and were used in homemade explosives in past terror attacks.

Doron Shalom, CEO of MS Tech says: "The detection of these emerging and global threats is extremely difficult with the traditional analytical methods commonly used today; following an extensive R&D process, enhanced engineering and smart detection algorithms, our innovating HF-QCM nanotechnology sensors, are now able to detect and identify these threats."

3DX-Ray Brings Airport Security Technology to the Cabinet X-ray Market

In a world first, 3DX-Ray has launched the AXIS™-CXi, a cabinet-based x-ray screening system that utilises the same colour differentiating image technology used in airport baggage screening.

The AXIS™-CXi is a huge step forward in mail room scanning, as colour differentiated images enable operators to determine not just the shape but, the nature of the materials being scanned. Orange shows organics, such as; explosives, chemicals and drugs, as well as more innocent items such as foodstuffs. Blue shows metals, such as; guns, knives, and potential IED components. Green shows inorganic materials like those used in homemade explosives. Grey scale is used for recognition of shapes and the form of objects. This allows the operator, with very little training, to analyse items more accurately, quickly and easily.

This is a step change from the existing cabinet mail screening manufacturers who have relied on pseudocolourisation of images and powder detection algorithms to indicate to operators the potential of a threat – these tools do not have any independent standard accreditation or assessment unlike the materials discrimination 3DX-Ray has introduced which is assessed according to the transport and aviation sector standards.

A further major innovation is in the design itself. The AXIS™-CXi has an extra-large inspection chamber, whilst maintaining a small footprint. So, not only can it scan mail and parcels, but it can also scan bags up to and including aircraft cabin bags.

The system is mobile and aesthetically sympathetic, meaning that it can be used in corporate entrances and hotel lobbies in times of raised threat levels.

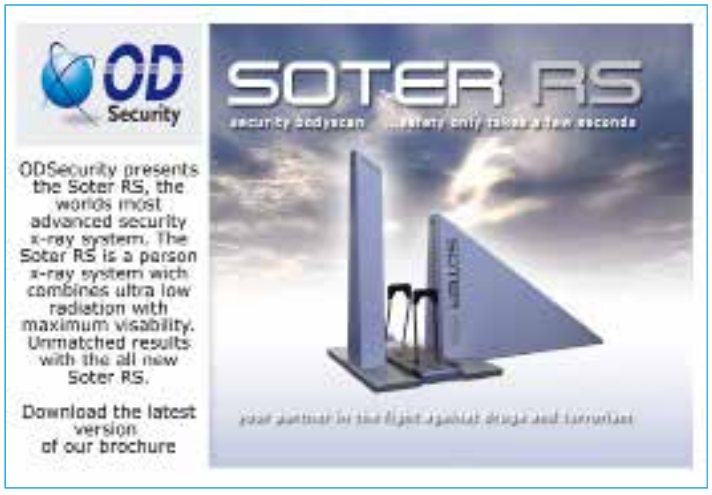
With user-friendly touch screen controls, unrivalled image resolution and industry leading image processing software, AXIS™-CXi is a unique product with unmatched functionality and utility.

World Security Report

World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to 100,000 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 34,000 border agencies, agencies at the borders and industry professionals, policymakers and practitioners, worldwide.



December 2020

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

17-18
ICAO Global Aviation Security Symposium 2020 (AVSEC2020)
Montreal, Canada
www.icao.int/Meetings/AVSEC2020/Pages/default.aspx

February 2021

2-3
International Exhibition Security & Safety
Monaco
www.psemonaco.mc/?lang=en

March 2021

9-11
Security & Policing
London, UK
www.securityandpolicing.co.uk

10-12
Secon Korea
Goyang, Korea
www.seconexpo.com

15-17
Milipol Qatar
Doha, Qatar
www.milipolqatar.com

15-17
Intersec Saudi Arabia
Riyadh, Saudi Arabia
www.intersec-ksa.com/frankfurt/18/for-visitors/welcome.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

June 2021

8-10
World Border Security Congress
Athens, Greece
www.world-border-congress.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