WORLD SECURITY REPORT

Official Magazine of

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

SPRING 2020
www.worldsecurity-index.com

THE SPY WHO HACKED ME?
SECURING A COUNTRY'S CRITICAL NATIONAL INFRASTRUCTURE

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

April 28th-30th, 2020
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.

Registration Today

and save with Early Bird Rates

All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure need to be addressed in the plans and executed to the requirements of the National Continuity Policy.

Join us in New Orleans, LA for the premier event for operator/owners of CI, government establishments and agencies and the CI industry tasked with the regions Critical Infrastructure Protection and Resilience.

The conference will look at developing on the theme of previous events in helping to create better understanding of the issues and the threats, to help facilitate the work to develop frameworks, good risk management, strategic planning and implementation.

For more information and online registration visit www.ciprna-expo.com




Confirmed speakers include:

- ***Keynote Speaker:*** Brian Harrell, Assistant Secretary for Infrastructure Protection, US Department of Homeland Security (DHS)
- Leslie Millet, Safety Agency Risk Manager / FSO Workgroup Chairman, Port of South Louisiana & Infragard Louisiana President
- Harrison Andrew Pierce, Head of Operational Compliance and Security, Aerial Systems, San Diego Homeland Security Office
- Dr. Christopher Rodriguez, Director of Homeland Security and Emergency Management for the city of Washington, DC, USA
- Stephanie Murphy, Assistant Vice President, Resiliency and Critical Infrastructure Programs, Tidal Basin Government Consulting
- Jeff Gaynor, President, American Resilience
- Sam Cohen, Cybersecurity Consultant – Risk Group, Deloitte Canada
- Alessandro Lazari, Regional Director – Mediterranean, International Association of CIP Professionals & KPMG Advisory, Italy
- Steve Povolny, Head of Advanced Threat Research, McAfee
- Tim Klett, Cybersecurity Researcher, Idaho National Laboratory
- Frédéric Petit, Principal Infrastructure Analyst, Argonne National Laboratory
- Ben Eazzetta, CEO , ARES Security Corporation

For speaker line-up visit www.ciprna-expo.com

The premier discussion for securing America's critical infrastructure

Supporting Organisations:

Media Partners:

CONTENTS

WORLD SECURITY REPORT


» p.5


» p.8


» p.17


» p.24

LONDON'S LONE WOLF ATTACKER

On 29 November in central London, a lone perpetrator, Usman Khan, stabbed five people, two of them fatally.

In addition to two knives taped to his wrists, he was wearing a fake suicide vest.

Khan was restrained by brave members of the public and ultimately shot by armed police.

This was yet another example of a low-tech lone wolf attack; the type of attack which the most difficult to detect and to stop.

They are challenging to detect because the would-be terrorist may be unknown to law enforcement or have no links to known radical groups or individuals.

So, if they keep their plans to themselves, the authorities are unable to pick them up via their electronic footprint; communications, social media, internet search activity and so on.

Nor can they be detected trying to acquire weapons or the materials necessary for bomb-making, because their weapon of choice is a knife or a truck or a car.

But this case was different. Why?

Because as low-tech as this attack was, Khan had been released from prison in 2018 on licence after serving just eight years of a sixteen-year sentence for terrorist offences.

In prison, Khan had completed the Healthy Identity Intervention Programme, the U.K.'s principal rehabilitation scheme for terrorism convicts. Following his release, he participated in the Desistance and Disengagement Programme, which is designed to "address the root causes of terrorism".

Being on probation, he needed permission to go to London and he was wearing an electronic tag.

So, this lone wolf case asks different questions.

Why was somebody convicted of terrorist offences released early?

Do these rehabilitations and deradicalization programmes work?

What went wrong, if anything with his post-release monitoring?

And finally, how many more Usman Khan's are planning to bring death and suffering to the streets?

Tony Kingham
Editor

READ THE FULL VERSION

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

www.worldsecurity-index.com

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

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

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

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

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

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

The Spy Who Hacked Me?
Securing a Country's Critical National Infrastructure

The recent failure of the UK's National Grid has emphasised the crucial importance of a country's Critical National Infrastructure (CNI) to its citizens' everyday lives. The event occurred when a power surge left parts of the country in chaos, London's transport and road network ground to a halt, and a million homes and businesses temporarily lost power.

Though the issue was resolved in a short space of time, it demonstrates the importance of CNI and the impact a single weak link in the chain can have on vital resources, such as energy, food & water supplies, emergency services and transport. Although it's hard to estimate the likelihood of an attack, the continual diversification of threats, and the ambition and capabilities of terrorist groups (and state actors) is likely to continue to evolve. Which means organisations must be equipped to deal with every eventuality.

There are other factors that broaden the remit of security teams further. For instance, cities are becoming increasingly smart and connected. This connectivity is creating more avenues for cyber-attacks than ever. Furthermore, it's not only isolated hackers targeting organisations anymore, nation states are orchestrating well-funded and wide-ranging attacks. North Korea, for example, has been linked to disruptive malware like Sharpshooter and WannaCry. This leaves security administrators with the difficult task of assessing an ever-multiplying range of threats. Whilst it may be impossible to secure CNI networks completely – planning ahead, improving defences and resilience as new vulnerabilities arise can significantly reduce the potential impact such attacks could have. The disruption from a simple power-cut not only

showed us the fragility of the system that powers the UK, but also gave us a snapshot of the chaos that would ensue if an attack was ever successful.

The Fallout

In July 2019, an electrical provider in Johannesburg was targeted by ransomware. Once infected its IT systems were locked-down, leaving many of its customers across the city without power. Although this was more than likely an isolated hacker rather than a state backed cyber-attack, it highlights the fact that not all attacks on CNI are physical. Ransomware proved to be the easiest means of causing the most disruption and was therefore the preferred method of causing mayhem.

The most illustrative modern example of a state-wide cyber-meltdown was the Estonian cyber-attack of 2007. After city officials decided to relocate a soviet WW2 statue from the country's capital, Tallinn, there was a Russian backlash. Consequently, Estonian websites were overwhelmed when they were swarmed with bots. Bank, media and government websites were shut down. This left government workers unable to communicate remotely, people unable to withdraw money from ATMs or access their bank accounts, causing chaos for weeks. Precisely no one was surprised to learn that many of the IP addresses were based in Russia, so it's almost certain these attacks were orchestrated by the Kremlin. But regardless of who the instigator was, this incident showed that nations can exert an enormous amount of power remotely through digital means. A targeted attack on key services also illustrates just how brittle a countries' infrastructure can be and how quickly communications can break down.

Thankfully, there have been far fewer examples of physical security breaches on CNI, although when they have occurred, they - more often than not - have a higher chance of causing loss of life and devastation – like the 7/7 attacks that targeted London's transport network. But events like this show that regardless of the type of threat, cyber or physical, you must be prepared.

The ABCs of security

Within the context of international cyber-espionage and terrorism, the task of security can seem like a daunting one. Nevertheless, the scale of the organisations involved should make little difference – the fundamentals of cyber and physical security remain the same. The Centre for the Protection of National Infrastructure classifies effective security as "defence-in-depth". This concept is based on the principle that the security of an asset is not significantly reduced with the loss of any single layer of defence. A way of simplifying the management of this layered system of defences is by consolidating every security asset into a single unified platform. After all, every IP-connected device such as a video surveillance camera or access control that helps protect you in the real world can become a digital gateway into the organisation if not secured appropriately.

This kind of approach may seem rudimentary, but is an important first step that organisations can take towards a more resilient security system. Unified security links everything together to give administrators a complete, holistic view of their environments. This provides a single place for security teams to work from, providing them with all the information they might need from across the entire physical or digital environment. The ability to access all facets of security, like access control, surveillance or cyber in an instant provides huge operational advantages. For instance, it eliminates the need to search for information as it's at operators' fingertips. Having mission-critical information available at all times means you can drastically reduce incident resolution time – as assessing a threat, planning a resolution and fixing the problem all happens more quickly.

Furthermore, it also means that security teams will be less stretched when covering a large environment and can optimise available manpower accordingly – which is vital for protecting CNI, as these types of sites or installations often cover huge areas.

Another fundamental element of effective security is resilience. This not only means an organisation's ability to defend against external threats, but crucially, when an incident does occur -how they react and what measures are put in place to stop it happening in the future. Again, unifying security is a cornerstone of this approach as it provides operators a single place where data can be consolidated. In the aftermath of an incident, exporting raw data can help to start building a detailed report of what occurred, so that they can analyse how things were done and how they could be improved next time. By reviewing the process from incident detection through to resolution auditing, organisations are able to make predictive changes, create new best practices, plan for the unexpected, identify weak spots, determine areas that require extra staff training, and shore up defences.

Looking to the future

The security climate is growing more complex, fuelled by invasive cyber-strategies from the likes of China, Russia and North Korea, and the constant threat of terrorism – which presents more challenges for security teams than ever. This will no doubt lead CNI to become more like quasi-public sector organisations, leading to more stringent regulation and a necessity for improved security - on all fronts. General Nick Carter, of the British Army, perhaps characterised these circumstances best when he said distinctions between peace and war "no longer exist". This assessment certainly holds a lot of weight, highlighting the need for lasting security preparedness in a time where a wide-range of anonymous threats are always looking for vulnerability.

Dan Meyrick, Sales & Business Development Manager at Genetec

Shifting Global Energy Demands and its Impact on Arabian Gulf Energy Security

The Arabian (Persian) Gulf region sits on half of the world's oil reserves, which makes it of vital strategic interest to global energy security and economic stability. So long as the world continues to largely depend on oil and gas for energy, this region will remain a major focal point of interest to global powers and developing countries. This has been the case since the end of World War II and will continue to be so for many more decades.

The nature of the threats has changed over the years. However, one factor remained constant throughout the past period and that is the West led the way in establishing and enforcing the security framework for the Arabian Gulf security. Although the means have changed with time, however the objective remained the same: To ensure dominance of the United States and its Western allies on the region.

Oil to the East

The rise of Asian powers with a notable increase in energy demands to cope with level and speed of growth has been having its impact on oil exports from the Arabian Gulf region. Moreover, the shale oil discoveries in northern America have largely reduced the United States oil imports. A simple review of Arabian Gulf oil exports to the United States shows that

it has been cut by nearly half of what it used to be less than two decades ago. According to the U.S. Energy Information Administration the United States imports of oil and petroleum products from the Arabian Gulf were 1,008,545,000 barrels in 2001 and dropped to 867,559,000 barrels in 2008 and to 575,807,000 barrels in 2018. In the second quarter of 2019, Bloomberg reported that U.S. imports of crude oil and condensate from Arabian Gulf reached 800,000 barrels per day, which accounts for only 6% of total shipments from the region.

Meanwhile China's import of oil from the Arabian Gulf has increased substantially over the past two decades. In the summer of 2019, Saudi Arabia ranked as number one supplier of oil to China with an average daily import of 1.83 million barrels per day. Currently four of the top eight suppliers of oil to China are in the Arabian Gulf – Saudi Arabia, Iraq, Oman and Iran. Japan, in turn, heavily relies on Arabian Gulf oil. According to 2018 figures, eight of the top ten of Japan's oil suppliers are in the region, in the following order: Saudi Arabia, United Arab Emirates (UAE), Qatar, Kuwait, Iran, Bahrain, Oman and Iraq. Iraq and Saudi Arabia are the top two exporters of oil to India followed by the UAE, Iran and Kuwait. After Iran was hit by the U.S. sanctions it lost its spot as the top supplier of oil to South Korea, and that spot went to Saudi Arabia, while Kuwait and the UAE remain on the list of top five suppliers. All in all, Asian powers import 80% of their oil from the Arabian Gulf region. While India and China import half of their oil requirements from the Arabian Gulf, Japan, South Korea, Singapore and Taiwan import three quarters of their oil from the region.

Asian powers also house the main depots and refineries that process the crude oil that is shipped back to Arabian Gulf countries. Millions of barrels of Iranian oil are stored in depots at Chinese ports serving as vital reserves to Tehran. These reserves enable both Iran and China to manipulate oil prices despite efforts by OPEC to stabilize the market. Although this practice has been linked to the imposition of U.S. sanctions on Iranian oil, however it has the potential to become a permanent situation even after sanctions are lifted due to the influence it could give China on oil rates. These depots bolster the current Chinese petroleum reserves that are estimated to be 325 million barrels of oil, which is equal to a little over a month of imports.

Bolstering Relations with Asia

The two major players in the Arab world that are regarded as regional power houses, Saudi Arabia and the United Arab Emirates (UAE), have embarked on a series of steps marking a strategic shift in their foreign relations policies. In the past few years, leaders of the two countries have improved and expanded their relations with China and India as well as other rising Asian powers such as Pakistan, Japan and South Korea. The scope of relations was no longer restricted to trade but has widened to include foreign direct investments – moving both ways – and the defence sector. Many Arab countries will likely follow – if they haven't already - the footsteps of Riyadh and Abu Dhabi in the coming years.

Comparing the commercial relations these two countries have with the U.S. with relations with Asian powers it will not be hard to conclude that the winds are blowing towards the East. For example, value of bilateral trade between UAE and China stands at around $55 billion per year, while with India is about $50 billion annually with an agreement between the two sides to double it by 2020. China has about 300,000 expats living in UAE, while India has the largest expat population that stands at 3.3-million strong. These figures are impressive compared to UAE-U.S. trade relations that stand at around $25 billion per year, while value of UAE-EU trade relations is about $47 billion annually. If UAE annual trade relations with other Asian powers like Japan ($24 billion), South Korea ($15 billion) and Pakistan ($9 billion) were added to China and India the total will come up to $153 billion compared to $72 billion with the U.S. and EU.

About 60 percent of the UAE's non-oil foreign trade is with Asian countries, and China's foreign direct investments (FDI) in the UAE totalled $9.1 billion in 2017, while India's FDI in UAE

totalled $1 billion in 2018. According to UAE minister of economy, China is currently the country's number one trade partner, accounting for nearly 10 percent of non-oil products in 2018. China is also Saudi Arabia's number one trade partner and has recently won $28-billion worth of economic agreements with the Kingdom. In 2019, Saudi Arabia signed trade agreements worth billions of dollars with Asian powers like India and Pakistan.

The United States' strength in trade relations with Arab Gulf States is largely due to its big exports of Defence and aviation products. Even U.S. FDI in UAE and Saudi Arabia are still larger than most Asian states, however China and some of its Asian partners are clearly making a strong push and starting to gain more ground. Arab Gulf countries are clearly taking notice of the political changes in Washington and what it could mean to their defence procurement programs as well as plans for industrial cooperation. While President Donald Trump has made it clear on more than one occasion that the U.S. military was deployed in the Arabian Gulf region to provide security in return for money from the Arab states there, the leading Democratic Party presidential candidate Joe Biden has vowed to halt defence programs with Saudi Arabia if he is elected. So, the prospects of maintaining the current Arabian Gulf security framework do not look promising when U.S. foreign policy seems to be ever more dictated by domestic politics.

Changing Policies

After the United Kingdom colonial power came to an end in the Arabian Gulf, the United States relied on two regional powers, Saudi Arabia and Iran, to prevent the Soviet Block from exerting any influence in the region. However, the Islamic Revolution in Iran brought an end to this arrangement. The so-called tankers war in the later part of the Iran-Iraq 8-year war underlined the importance of the region to global energy security and demonstrated the readiness of the United States to use military force to assert its dominance and ensure the flow of oil through the Strait of Hormuz. Shortly after the Iraqi invasion of Kuwait that sparked the Gulf War, led to the establishment of major military presence for the United States and its Western allies in the region. The regional security framework for the Arabian Gulf became very much U.S.-centric where Washington became the main guarantor of security.

The attacks on oil tankers and oil facilities in the Arabian (Persian) Gulf region in 2019 have undermined the regional security regime the United States and other Western powers has enforced since the development of the Carter doctrine in 1979.16 The asymmetrical threats that dominated the regional scene for the last two decades have escalated in the last years. However, actions by groups affiliated with the Iranian Revolutionary Guards have proven to be most serious threat to energy security with the employment of advanced weapons such as drones and cruise missiles. The U.S. failure to protect assets of its allies and retaliate against hostilities has all but contributed to the already dwindling confidence the Arab Gulf States have in Washington.

Most experts have agreed that Asian powers, especially China, would suffer the most in case hostilities broke out in the Arabian Gulf region between the United States and Iran. Iran has proved capable of disrupting flow of oil from the region even if the countries tried to surpass the Strait of Hormuz and use outlets on the Arabian Sea or the Red Sea. But while focus has been on Iran and non-state actors, the near-peer power struggle has re-emerged and occupied the global theatre where China and Russia are pushing ahead to assert influence worldwide.

Asian Technology and Blue Water Navies

While the Trump Administration sends out confusing messages about its commitment to the Arabian Gulf security and adopts more isolationist rhetoric, China and Russia move in ready to fill the vacuum. Asian powers import 80% of their oil from the Arabian Gulf region, which means they will be more willing to play a bigger political and military role in securing energy resources there. Although these powers do not yet possess the needed military power to provide the region with the adequate security, however China,

India and Japan are all building their blue water navies and are poised to have formidable power projection capabilities by 2035. China is expected to have in service six aircraft carriers, of which four will be nuclear-powered, while India will have about three carriers.19

China has already established a foothold in the vicinity of the Arabian Peninsula by opening its first overseas naval base in Djibouti on the Red Sea. China is working hard on carrying out its "one-belt one-road" plan linking its territories by land and sea with Europe and the rest of the world, especially vital routes to its energy resources in the Arabian Gulf. The Chinese naval presence will eventually contribute to improving military-to-military relations between China and its Arab Gulf neighbours. The Saudi military recently held naval exercise with the Chinese off the Port of Jeddah, in a step towards enhancing relations and joint operations.

China is making strong advances in its military technology and air power capabilities and is now able to protect what it regards as vital areas in the Indian Ocean, such as the case in the South China Sea where Chinese Navy is adopting area access area denial (A2/AD) approaches, making zones inaccessible by foreign powers. The Chinese will ultimately expand the A2/Ad zones as its military grows more capable and as the Arab Gulf neighbours become more receptive to its role. China already has strong strategic relations with Iran on all levels and will not face any problems from Tehran if it ever decides to establish a bigger military foothold in the region.

The size of military relations that already exist between the United States and the Arab Gulf States makes it unlikely that a full breakup between the two sides would take place – at least not any time soon. These countries have joint industrial projects and their military hardware is mostly from the U.S. and Europe. However, the Arab Gulf countries have been taking more steps recently setting themselves up to become closer to the Eastern powers in terms of technological development. The UAE has hinted last October that it was ready to receive the new generation 5G technology offered by the Chinese giant telecommunication company Huawei, despite U.S. opposition. When the U.S. is declining requests by its Arab allies to acquire certain military technologies, the latter are now seeking solutions in China. The best example of this was the Chinese selling of attack drones to both the UAE and Saudi Arabia, which is now opening a local factory to these Chinese Wing Loong 1 unmanned combat aerial vehicles (UCAV). Even long-term strategic programs such as alternative energy resources like nuclear power plants the Arab Gulf States seem to prefer non-Western providers. While Saudi Arabia is working with Argentina on developing its nuclear facilities, the UAE awarded the contract for its first nuclear power plant to South Korea.

Therefore, not only is China trying to improve relation with Arab Gulf countries in all fields and elevate them to a more strategic level, regional players appear ready and willing to work with China and other Asian powers moving further away from their Western allies. Arabian Gulf states are clearly embracing a strategy of a multi-polar world where the United States is no longer the sole dominant power. Hence, the threat to the current security regime in the Arabian Gulf, where the U.S. has been the dominant player, might evolve from asymmetrical to conventional and subsequently Asian powers, especially China, will likely challenge this dominance. This will have an impact on energy security from the Western perspectives in particular.

Alliances and strategic relations between nations are based on common interests and the level of the need one has to the other, and as such the majority of Arab Gulf States are bound to pivot to the East away from the long-time partnerships and alliances with the West, especially the U.S. The growing inter-regional trade relations and the increased dependence of rising Asian powers on crude oil of the Arabian Gulf and the rise of isolationism and populism in the West are driving most of the current Western allies in the Arab world to the East gradually ending an era of dominant influence for Europe and the United States on large parts of the Arab World. Therefore, shifting global energy demands are driving a big rapprochement between the oil-rich Arabian Gulf region and Asian powers, which could increase military competition between the U.S. and China in the region, and possibly undermine energy security regionally as well as globally.

By Riad Kahwaji, Director General, INEGMA

INEGMA is a strategy and security consultancy, research house, headquartered in Dubai and with an office in Beirut. We bring together the reach of a strong international network with specialist expertise and proven competence across a spectrum of advisory areas including political security, risk mitigation, strategic communication, energy security, economic partnerships and defence trade and cooperation. http://www.inegma.com

A word from the Chairman

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

International Association of CIP Professionals

As we enter not just a new year but a new decade, we all hope that times ahead will be safer, with less violence, less suffering and less poverty around the world. This however, may just be wishful thinking.

A new year normally bring new year's resolutions, and although helping to work towards world peace may be an aspirational aim for many it is one that most people can do very little to assist with. So, we tend to stick to those tried and tested promises of previous years such as being determined to get fit and exercise more. It is this which I think should be a priority for this year and beyond for those involved in infrastructure protection and resilience. Obviously, I don't mean the individuals personal goals but those of the organisation providing the service, striving to be 'fit for purpose' and to continually 'exercise' the plans that they have in place. If indeed those plans are there!

The community involved in managing risks to critical infrastructure is wide-ranging, composed of partnerships among owners and operators; National, local, and territorial governments; regional entities; non-profit organizations; and academia. Managing the risks from significant threat and hazards to physical and cyber critical infrastructure requires an integrated approach across this diverse community to:

• Identify, deter, detect, disrupt, and prepare for threats and hazards to infrastructure;

• Reduce vulnerabilities of critical assets, systems, and networks; and

• Mitigate the potential consequences to infrastructure of incidents or adverse events that do occur.

The success of this integrated approach depends on harnessing the full spectrum of capabilities, knowledge, and experience across the infrastructure community and the associated stakeholders. Bringing people together to collectively identify threats and hazards, to prepare plans to mitigate the consequences and to be ready to deal with whatever crisis may occur is not an easy task but it is an essential one.

The process has to be a collaborative effort with community partners, internal and external stakeholders, and others who may be impacted or part of the response to an incident should one occur.

It is only through collective activity that we can hope to prepare to be 'fit for purpose' and an essential part of that process has to be continually exercising the plans that are in place, learning the lessons identified from those exercises and ensuring those lessons are acted upon.

The world is moving ever faster and the need to plan for its protection and resilience requires a constant focus and huge effort from us all. As we see tensions rising as a result of the continuing 'spat' between the United States and Iran, a new year and indeed a new decade is a good time to reflect on how prepared we are within the critical infrastructure community to deal with the myriad of threats, both natural and man-made that will continue to challenge us.

Perhaps now is a good time for infrastructure organisations to reflect on their priorities and plans and to make some new year resolutions, one of which should be a commitment to developing and delivering exercises which will test the robustness of their thinking and planning.

The IACIPP Poll

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

Q. How prepared do you feel for a cyber attack?

- Very well prepared - 22%
- Well prepared - 11%
- We are preparing but not yet there - 56%
- We have just started preparations - 0%
- We are not prepared but have started - 0%
- We have not made any preparations and unprepared - 11%

The International Association of Critical Infrastructure Protection Professionals (IACIPP) is also considering what more we want to achieve in 2020 and further ahead into this new decade. This year we are supporting three conferences which focus on the protection and resilience of critical infrastructure and information:

- CIP Forum in Romania in March
- Critical Infrastructure Protection and Resilience North America in New Orleans at the end of April
- Critical Infrastructure Protection and Resilience Europe in Bucharest in October.

Through our input into these events and through our regional networks and our website we continue to deliver a platform for like minded people to get together, share experiences and ideas and to learn from each other.

The IACIPP has set its own new year's resolution and it is simply to bring even more people together this year and seek to enhance the collaborative effort across the range of stakeholders who play such a vital role within the infrastructure community.

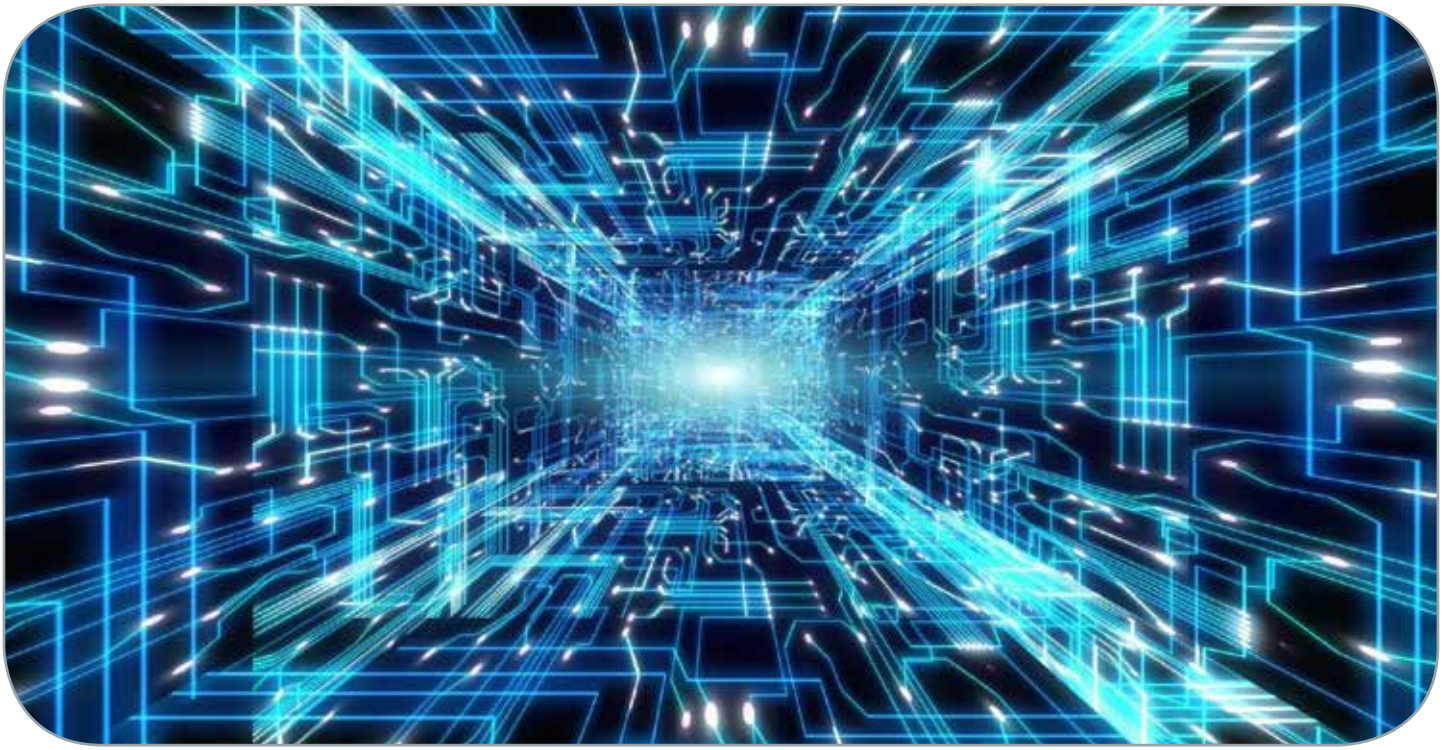
John Donlon QPM FSyI
Chairman IACIPP

Video of the Month

Some great resources are available on the IACIPP website, and this months featured video presentation comes from Alessandro Lazari, Regional Director for Mediterranean of the International Association of CIP Professionals and Manager at KPMG Advisory Italy.

Alessandro Lazari's presentation 'The European Journey of CIPR' was presented at Critical Infrastructure Protection & Resilience Europe in Milan in October 2019 and can be viewed at www.cip-association.org.

Physical Security Investigation Management - The instruments for investigation



The Cited Work can be found in; ISIO www.intsi.org and [HIM]. Human Investigation Management. www.human-investigation-management.com

The technology is only as good as the user!

Regardless of the reason for investigation, the Investigation is only as good as the investigators and who does the investigation. In the world of security, criminology, and risk management, it is the person and not the weapon that creates havoc.

The concept of success for, criminology, security, and risk investigation management will depend on, the level of situational awareness of the decision-makers on the ground and their reaction speed. This applies to any form or field in management, research and application, besides vetting and compliance, because crime lives in all fields, e.g., business, human resources, construction, farming, education, security or, for that matter, where any human is involved.

When the investigation is related to crime then the outcomes could lead to life impacting or life & death situations, therefore, the importance of knowing all the truthful information is paramount. When any research is based on insufficient or unreliable information, then the narrative of a puzzle-built picture

will point the investigator into the wrong direction wasting time effort and money.

To heighten situational awareness and gathering information to conceptualize the narrative, one would rely on the people on the ground besides instruments for investigation, such as, incident and crime mapping software, CCTV, access control, perimeter security, drones, covert or overt surveillance equipment, social media tracking, mobile phone tracking, to mention but a few

There are words related to investigation such as, identify the modus operandi (pattern), which is one of the fundamental foundations for investigation. The pattern dictates the design and structure of any form, and it is obvious that once the pattern changes, so too does the formation of the structure. The word 'clue' could describe the X factor. Identifying or uncovering an element could point to identifying a pattern

Concept

To read the situation is to fully understand the nature of the beast (narrative). This is done by following a pattern of thought that could be described as building a puzzle. The placing of all pieces of the puzzle using their distinct patterns and shapes form the full picture. Subsequently, one must have conceptional thought and must be fully situational aware to ensure that all the pieces of the puzzle are considered and fit for construction. Consequently, one must distinguish and identify the pattern to comprehend the structural formation, which could change at a moment's notice.

The pieces of the puzzle must be truthful and all the information. As we know that people lie, hide or volunteer information for their own agenda, therefore, the tool must contain the knowledge and methods to critically out-think and outsmart the criminal. Furthermore, they also follow the tangible chain of evidence to comprehend the big picture.

Keep in mind that one can locate tangible items that a syndicate or person may use to commit an act of crime or terror. Therefore, connecting people with things must be an approach to follow.

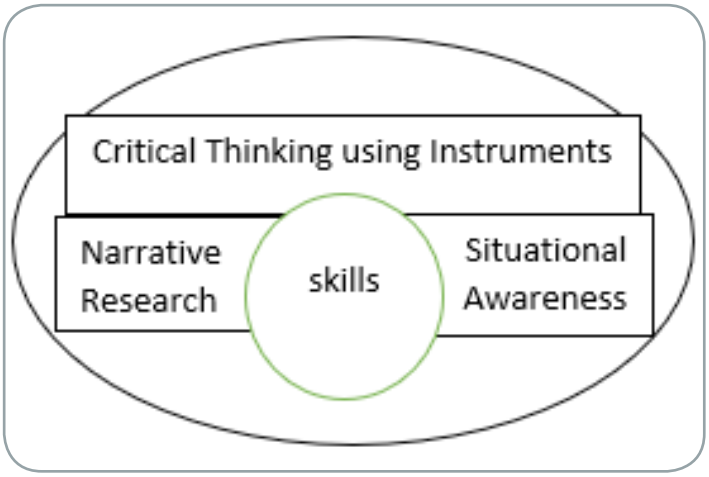
Taking all of the above into consideration for defining the hypothesis and selecting the tools to critically out-think or outsmart criminal certain issues had to be taken into consideration. Furthermore, it would be a human that must do the investigation for research, analytics and operations.

The technology is only as good as the users

To find the clues and the pattern, one must identify and comprehend the crime on/in a location or field of interest, the researcher/investigator must know the cultural of crime and methods of crime to select the instruments best suited. The practitioners need to read the situation and the people involved.

Stated earlier, the instrument is only as good as the user that is knowledgeable in distinct crime or domain experts (e.g., security consultants) that are, besides being soft-skilled and have the character traits, such as, mentally and emotionally intelligent. This dictates a question, 'who is best to select the instruments?"

The unbiased analyst/investigator is the hypothesis who must identify the pattern and formation of a structure by observing, interviewing and drawing up the questions for analysis. An example could be based on transnational or local organized crime, street gangs or the lone-wolf predator where the



practitioner must read the situation to find the first piece of the puzzle, by identifying a person of interest that may be working on their own or with others in concert.

A founding researcher Flavell (1976,1979) suggests for critical thinking (think out of the box), that the person must be self-aware and regulate themselves (you are the hypothesis) in social settings. By adding Situational Awareness to see the complete narrative and being of fully conscious by taking into consideration that unknown and known issues could impact the complete picture (Ensley 1995). Furthermore, the Critical Thinking soft skills must include lie, deception detection and critical situational interviewing regardless of culture, to identify a person-of- interest. (Kirsten 2018,19)

Regardless of the investigative method, the completed narrative (picture) must be reviewed to consider missing issues and be totally comprehended (got the picture). Thereafter, the narrative must again be dissected to identify how, what and where the hard evidence could be found relating to each piece of the puzzle, e.g. Cctv footage, mobile phone records, DNA, fingerprints, etc.,

The outcomes of using the instruments, and critical thinking methodology included in the soft skills will uncover new crime and discover copycat crime. The research base for all and guidance articles on where how and to use such can be found in the cited work.

Urban Guided Transport Management Cyber Security

The following is a technical article examining how the Multiple Independent Levels of Security (MILS) can meet the high system security requirements of the Urban guided transport management system (UGTMS).

The critical infrastructure protection has become an essential part of advanced human systems security strategies. Critical infrastructures are often formed by extensive networks of physical elements (either point or line types), their management system, human factor, technical standards, relevant legislation and management strategy as well, (EU 2005, Moteff 2003, Prochazkova 2014). It is necessary to take care of the security barriers for all mentioned types of elements (hard elements, soft elements, human factor and documents) in order to ensure the protection of the critical infrastructure. Physical protection is not enough.

The protection of infrastructure management systems is mostly linked to a single environment, through which managements are implemented for all infrastructures, the communication infrastructure. The protected system can be divided into three parts in terms of elements protection. We have a network of physical components distributed over an extensive territory that needs to be coordinated. The physical components may be stationary (lights, switches) or mobile (train sets). The second part is dispatch management. The dispatch management consist of a human factor and an information system.

The physical components and the dispatch management are connected through third part, i.e. the communication system. The communication takes place through the cyber space and with physical component form cyber physical systems (CPS). The communication system needs to reliable secure available

information flow at maintainable intensity, which will be also safe, RAMS (EN 50126-1 1999).

The article will exclusively address the security of interfaces between the communication system and the internal cyber environment of the critical infrastructure (Dunn 2004) furthermore. The solution with the least risk would be built up its own isolated data transmission system from the cyber security of the communication system point of view. Such a solution would be safe and reliable, yet unavailable and unmaintainable.

The physical extensiveness of infrastructures forms a large attack surface in physical space and it has high demands on the communication system. The public communication infrastructure is also used for communication, and therefore, the vastness, openness and dynamism of the public network leads to a large attack surface, this time in cyberspace, however with possible impacts in cyberspace and physical space as well (Peerenboom 2001). The Urban Guided Transport Management System (UGTMS) is an example of such infrastructure. UGTMS is described in the second chapter.

The security of the gates, which the information flow use for overcoming the interfaces between systems, can be ensured in the usual ways - access keys, passwords, firewalls, and so on. However, the regular gateway security techniques may not be sufficient in the case of critical infrastructures. Therefore, a system with multiple independent levels of security (MILS) is appropriate to use. System with the MILS principle guarantee that overcoming of one barrier does not make an attacker any easier to access other barriers. The MILS principles are described in Chapter 2. Chapter 3 deals with aspects of application of MILS principles at the Prague metro/subway as representatives of UGTMS.

1. The Urban Guided Transport Management

According to present knowledge and experience, three aspects of the UGTMS are important: system management levels; system architecture; and cyber-attacks at cyber-physical systems.

1.1 System Management levels

The structure of UGTMS can be divided according several various planes. One is the management plane where we distinguish three elemental levels, Figure 1. The "Operation planning" is ensured at the highest level, both long-term (strategic management) and short-term (tactical management). Only the level of politic management lies above the operation planning. The policy level for UGTMS is given by standard (IEC 62290 2018).

The lower two stages of the pyramid at Figure 1, are "Operation management and supervision" (Operational Management) and "Train operation" (Technical Management).

Operation management and train operation lie at lower level of management pyramid than operation planning at offices; however, they are more critical from the point of view of cyber security. Operation control centre and decentralized control of trains and waysides are an example of CPS. It is also necessary to ensure proper maintenance of the whole system in addition to management levels of operation. Maintenance pervades through the whole pyramid, from operation planning at top to train management at bottom.

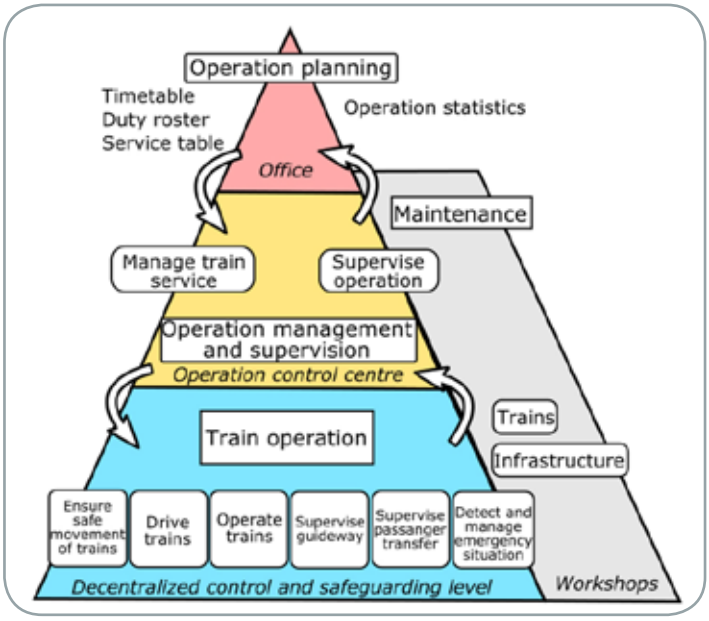


Fig. 1 Organization and operation structure of UGTMS (IEC 62290 2018).

1.2 System Architecture

Critical points need to be identified, before we begin to build the security measures of the system. We used UGTMS architecture according (IEC 62290 2018) shown in Figure 2 for this purpose. Figure 2 represent the lower two levels of the pyramid shown in Figure 1, i.e. the Operation management and supervision, and train operation. However, Figure 2 shows also links from these two levels out the system, for example to operation planning or maintenance.

The cybernetic core of the UGTMS composes of three subsystems:

1. Operation Control Subsystem.
2. Onboard Subsystem.
3. Wayside Subsystem.

Exchange of data and information is necessary to ensure among these three subsystems. Data Communication Subsystem secures the exchange of data and information.

As it is discussed at introduction, a dedicated network of

communication systems through the open radio space and public communications links are used for communication. Figure 2 illustrates a big number of interfaces between cybernetic systems with different security level requirements. Interfaces are located both on the outer edge of UGTMS cyberspace (passenger information, operation planning, CCTV surveillance, etc.), as well as at inner space of the system itself (Data Communication Subsystem). Security gates are necessary to build on these interfaces to ensure the security level requirements.

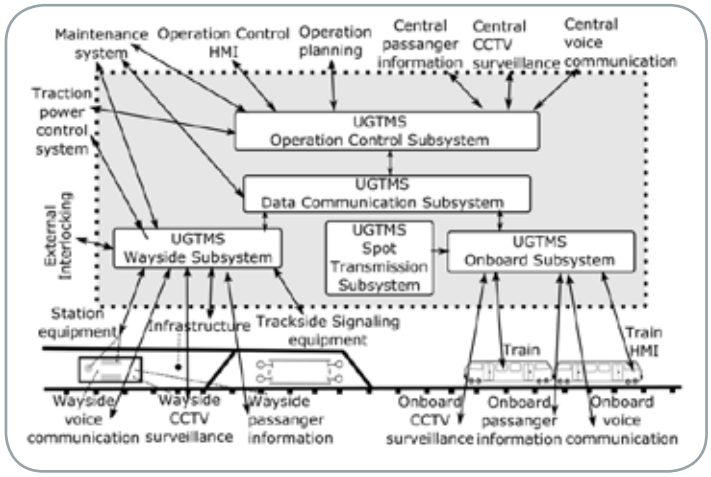


Fig. 2. The Urban guided transport management system architecture (IEC 62290 2018).

The number of security gates needs to be large, because we need to ensure safety of the Operation Control Subsystem as well as to guarantee the transmission path for each train and wayside elements. Security levels requirements need to be set up and ensured in view of the fact, that it is a CPS alongside. A cyber-attack on the CPS can lead to great material and human health damage and harm.

1.3 Cyber-attacks at cyber-physical systems

We live at a time when there are regular reports of cyber threats, whether associated with unknown invaders or technology manufacturers. Information security is often discussed in the context of these cases, but there is a little talk of possible impacts on the CPS.

The disruption of information security, for example at the office level on Figure 1, may lead to financial damages depending on the value of the infringed information. The disruption of the cyber security of the CPS as Operation Control Center, on the other hand, can lead to damage of both parts, the cybernetic as well as the physical part of the system. Losses on information, materials and human health and lives of CPS can be accompanied with losses on protected assets of neighborhood systems connected by links and flows to the CPS. Although, the CPS parts are at the bottom, from the point of view of the management levels, the requirements for their security levels are much greater. The critical infrastructure operators need to be convinced about this fact, as well as with industry 4.0, the heavy and chemical industry operators.

2. Multiple Independent Levels of Security

Regards to present knowledge and experience on the MILS, we further concentrate attention to: its operation principles; its operation planes; and its physical realization,

2.1 Operation principles of MILS

The previous chapter describes the situation where we have interfaces between subsystems with different security level requirements in cyberspace. We can also talk about trustworthy and untrustworthy space. The Information flow between these spaces needs to be secured, and it is necessary to build security gates to prevent the compromising of a trusted subsystem. Types of security barriers are described for example in standard (IEC / ISA 62443 2018).

The Standard (IEC / ISA 62443 2018) does not only describe the elemental safety barriers and procedures for control and autonomous systems in cyberspace but far more. It contains foremost the principles and requirements that the application of such barriers and procedures should meet, for example, in production networks of industry 4.0 or at the technical and operational level of critical infrastructure. One of the fundamental philosophies of standard (IEC / ISA 62443 2018) is the application of the "Defense in Depth" principles. We build the multiple security barriers, when we applicate defense in depth principles. Each one of security barriers then counts for the possibility of failure of the other barriers.

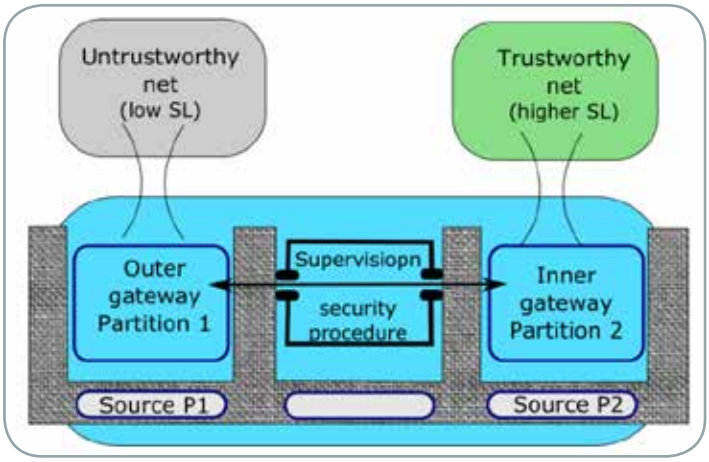


Fig. 3. Schematic representation of the interface between trusted and untrusted networks when applying MILS principles.

The principles inserted in the MILS approach (Harrison 2005) fully meet requirements of defense in depth strategy in the

security area of information flow between trusted and untrusted parts of cyberspace. Principles of MILS approaches stand for the creation of multiple gateways and security procedures through which the information flow needs to pass, Figure 3. Each gateway and each security procedure have their own resources (CPU, Hard drive, RAM, Ethernet, etc.). Disruption of one security barrier will not endanger the other barriers.

2.2 Operation planes of MILS

The MILS Approach application assumes that security setting starts already at the hardware level. Independent operation of individual gates and procedures requires also security settings of system to be respected on all operation planes of MILS, Figure 4. Following principles need to be comply with:

1. The operating system may not randomly allocate sources, as in the case of conventional operating systems. It needs firmly to follow the configuration plane (such as PikeOS).

2. The configuration plane or configuration file is the weakest point of the system and it needs to be protected accordingly (because affecting the all partitions).

3. The robustness of safety procedures on the monitoring plane greatly influences the benefits of the MILS system.

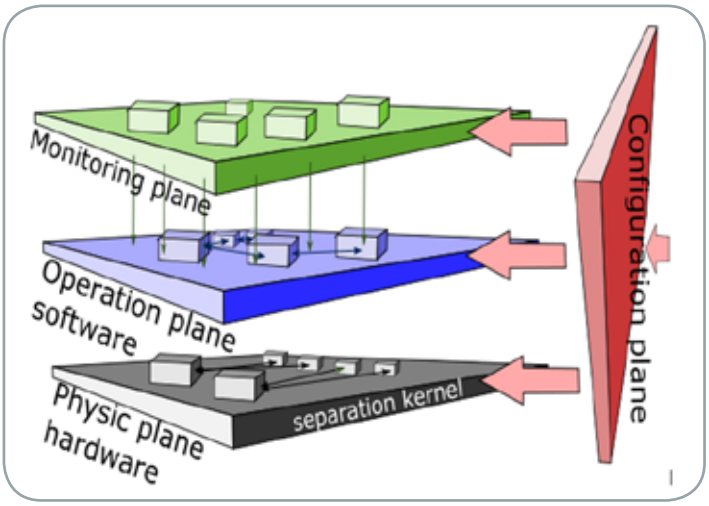


Fig. 4. Planes of MILS implementation, Physical plane (Hardware), Operation plane (Software), Monitoring plane (Security procedures) and Configuration plane (Configuration file) - (CITADEL 2016, CertMILS 2017).

An adaption plane is sometimes present in the planes of MILS implementation, Figure 4. The adaption hold position on the right side to the configuration plane, which it affects. The way how to implement the dynamic adaptability in the MILS without threaten the its security is the subject of an invention. For example, the projects CITADEL (2016) and CertMILS (2017) deal with it in the European space; see Chapter 4 for more details.

2.3 Physic realization of MILS

Several ways how to implement the MILS principles are known. Way of fixed allocation of resources, such as an Ethernet connection or Hard disk space, are obvious. A question of fixed allocation of CPU is more complicated. It is of course possible to have own processor for each barrier. This is, however, a very impractical option. In practice, the MILS is implemented on a single processor. A processor can be either multi core or single core. Distribution of resources for multicore CPU logically suggests to assign each core to different partition. If we have single core processor or there are less cores than security barriers, "kernel separations" (Rushby 1981) can be performed and individual core partitions are assigned to individual interface partition.

The security level of individual barriers is also important for the functioning the whole system. The benefit of MILS approach is weak or negligible in the case of weak or negligible barriers. However, we will get overall MILS security level with combination of barriers with high security level that we would otherwise find difficult or impossible to achieve.

Barriers should also be of different settings. The MILS principle also allows to combine technologies from multiple manufacturer for different partitions so that none of them have "keys" from the entire system. The system integrator is than only one, who has the access to whole system. We can then measure and compare barriers from individual manufacturer to get information about their behavior. However, integrator need to remember that the complexity of the system (the number and variety of barriers) increases demand for its operation and new threats can arise.

3. Pilot Project

We give example of introducing the MILS in the Praha subway.

3.1 Metro / Subway

The MILS Community addresses the development of the MILS approaches and its implementation into the protection of European infrastructures (MILS Community 2019). The MILS Community brings together the European technology companies and Academia, representatives of cyber security science from different areas.

The MILS Community makes to use of various European projects and addresses through them the challenges that arise in the application and development of new technologies, compatibility with standards such as (IEC / ISA 62443 2018) and pilot projects in areas like railways or smart grids. Projects CITADEL (2016) and CertMILS (2017) also deal with possibility of application at Praha Metro.

The Praha Metro is the classic representative of UGTMS (IEC 62290 2018). The Praha Metro does not reach the scale or intensity of transport of the largest European metropolis. However, the three lines transport 1.2 million people per day - 1.6 million journeys per day - 0.4 million transfer between lines (DPP 2015). These numbers document that Praha Metro is at least a critical regional infrastructure. The most occupied route C connects the largest Praha suburbs (middle class inhabitation) and the center of the city (offices and other workplaces) and its disturbance, such as falling the person into the railroad track, leads very fast to overflowing other transport infrastructure.

The MILS protection is tested in the UGTMS Onboard Subsystem at the Praha Metro, at present, Figure 2. In near future, every metro train will be equipped with the MILS protection. The transfer of information about position and other driving properties, as well as the remote control and communication with the operating center, should, therefore, be protected from cyber-attacks.

3.2 Integration and adaption

A concept of solution is not enough to solve technological problems, such as cyber-attacks in practice. A choice of suitable components (hardware and software), a way of their integration, certification, and in a dynamic environment such as cyberspace, a procedure of adaptability to new threats are also necessary.

A diversification of the suppliers and manufacturers of individual components of the system can increase the security as well as the complexity of the security barrier system, as was mentioned above. We have three levels of access and responsibilities in the question of gate control, Figure 5:

1. Manufacturers of individual elements.
2. The integrator.
3. An operator / user.

All three levels have their own rules (standards), which they are managed by, and the supervisory authorities that oversee them. Manufacturers, the integrator and an operator have also access to different parts of the system.

The technological setup of MILS called "T-Composition" was designed for the needs of the Praha Metro and other pilot cities (CITADEL 2016, CertMILS 2017). T-Composition are described in deliverable 8.1 of projects (CITADEL 2016, CertMILS 2017). The verification of MILS T-Composition usability in the Metro Onboard Subsystem is one of the activities within these projects CITADEL (2016) and CertMILS (2017). The use of the technology is assumed at the interfaces between the Data Communication Subsystem and the Metro Operation Control Subsystem, the Metro Onboard Subsystem and the Metro Wayside Subsystem, Figure 2.

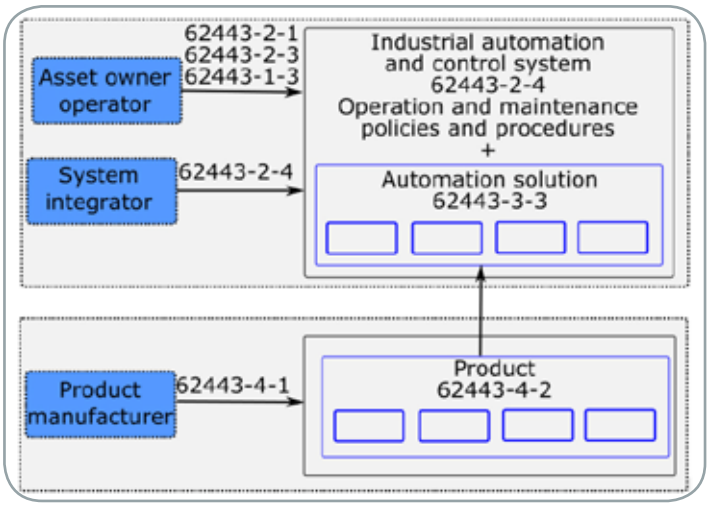


Fig. 5. Three Levels of Responsibility, Manufacturer, Integrator and Operator. Different parts of standard (IEC / ISA 62443 2018) for different phase of application.

The next step with that projects (CITADEL 2016 and certMILS 2017) deal, is the certification. Certification in relation to adaptability (or adaptability in relation to certification) is the issue for a separate article. The manufacturer, integrator and operator need to follow the various standards for operation, depending on the area of their activities, e.g. the UGTMS operator follow (IEC 62290 2018) standard. The standards do not create obligations only for them, but also create requirements for the previous segment of supply chain, Figure 5.

The area of cyber security is covered by own standards. We write here mainly about a standard (IEC / ISA 62443 2018). The standard (IEC / ISA 62443 2018) is not legally binding at Europe, but it gives guidance, how to proceed or what to expect from previous segments of supply chain point of view of individual technological parts as well as from the point of view of the whole system integration.

The cyber security of individual components can be also standardized with the Common Criteria (ISO / IEC 15408 1999). Both standards (IEC / ISA 62443 2018 and ISO / IEC 15408 1999) are considered in the European projects CITADEL (2016) and CertMILS (2017).

The possibility of reconfiguration based on operation requirements, adaptability, is one of the most important features of the system. Implementation of this quality in practice has considerable financial resources. Processes that can easily verify and implement these reconfigurations is necessary to prepare and apply. The solution of this issue is the technological setup of MILS called "I-composition", deliverable 8.1 of (CITADEL 2016 and CertMILS 2017). I-composition forms the certified foundation of the system. The I-composition are expanded with another attachments until the desired T-composition is achieved in Figure 6. The project (CertMILS 2017) deals with this issue.

Fig. 6. T-composition box with card .according to CITADEL (2016) and CertMILS (2017).

The system capability of adaptation has several levels. Projects CITADEL (2016) and CertMILS (2017) work now with three possible way of adaptability, fully self-adaptable system, semi self-adaptable system and manual-adaptable system:

1. The system, which can evaluate situation, define the most optimal configuration, secure switch and accomplish certification without the human intervention, stand at the highest level of the dynamic self-configuration (CITADEL 2016). The difficulty of fully self-adaptable system creation lies in maintaining the independence of individual security barriers and real-time certification.

2. The semi self-adaptable system is easier to setup. The semi-dynamic system has several the "allowable states" of resource distribution (CITADEL 2016). All allowable states are verified and certified beforehand. The system can switch only between allowable states. Secure procedure of switching needs to be prepared.

3. The manual-adaptable system is lest progressive from discussed ways of adaption, but it is also connected with lesser risk from unsupervised procedures. The manual-adaptable system uses the "I-composition" (CITADEL 2016, CertMILS 2017). Verified and certified I-composition has form of box with slot for cards, Figure 6. The card can be easily removed, modified, and installed back to box. The box and cards together create T-composition.

Conclusion

The criticality of infrastructures as well as the vulnerability are increasing with increasing the dependence of human systems on infrastructures. The cybernetic infrastructure is one such area where new harmful phenomena are dynamically emerging. The security disturbance caused by unknown attacker, hardware manufacturer or software developer has a great media attention today, although these phenomena have been present for a long time.

The protection of information and communications only at the information level with the help of the software is not sufficient. The hardware measure at the cybernetic security level is also necessary. The CPSs are particularly critical from the point of view of cyber-attack because they are associated with the physical world and physical impacts.

The concept of MILS has higher overall security level than individual barriers. The increments of infrastructure criticality and arise of new harmful cybernetic phenomena demand application of advanced security procedures. The European Critical Infrastructure operators, therefore, implement the MILS protection in rising number. The Praha Metro is one of operation, where the utilization of MILS principles is tested.

By Jan Prochazka, Petr Novobisky and Dana Prochazkova from UniControls a.s. and the Czech Technical University in Prague

Acknowledgement

The results published in the article were created with the support of the European projects "CITADEL" ID: 700665, "CertMILS" ID: 731456 and "RIRIZIBE" CZ.02.2.69 / 0.0 / 0.0 / 16-018 / 0002649.

Review, Vol. 15, No. 5).

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

The UN Counter-Terrorism Committee Executive Directorate (CTED) conducted a second follow-up assess progress made by Kyrgyzstan in implementing the Committee's recommendations

Since 2013, over 800 nationals of Kyrgyzstan have left for territories in Syria and Iraq that were controlled by ISIL (also known as 'Daesh') (including approximately 150 women and 100 children), of which at least 230-250 are believed dead. In those years, over 140 persons have been arrested and convicted for having taken part in terrorist activities in Syria and been relocated to the Kyrgyz Republic. Relevant authorities have dismantled several terrorist cells planning to commit terrorist attacks in Kyrgyzstan. As also reflected in its efforts, the Government is cognizant of the threat related to the continued return of its radicalized nationals intending to continue their terrorist activity in Kyrgyzstan and the region.

The delegation noted the focus of the Kyrgyz authorities on preventive measures, including counter-narratives and awareness raising measures, developing reintegration and rehabilitation measures for returning women and children, with the involvement of a wide array of international partners and civil society stakeholders. The delegation also reaffirmed the readiness of relevant United Nations bodies and international and regional organizations that joined the follow-up visit to support Kyrgyzstan in its counter-terrorism and counter violent extremism efforts through the provision of technical assistance as appropriate and in compliance with the Counter-Terrorism Committee's recommendations.

The visiting delegation included CTED experts, as well as representatives of the United Nations Office of Counter-Terrorism (UNOCT); the Monitoring Team of the Security Council Committee established pursuant to resolutions concerning ISIL (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities; the United Nations Office on Drugs and Crime (UNODC); the United Nations Entity for Gender Equality and Women's Empowerment (UN Women); the United Nations Regional Centre for Preventive Diplomacy in Central Asia (UNRCCA); the International Criminal Police Organization (INTERPOL); the Organization for Security and Cooperation in Europe (OSCE); the Eurasian Group for Combatting Money Laundering and Terrorism Financing (EAG); the Anti-Terrorist Centre of the Commonwealth of Independent States (CIS-ATC); and the Collective Security Treaty Organization (CSTO).

The delegation also held meetings with the UN Resident Coordinator a.i., the United Nations country team in Kyrgyzstan, the Programme Office of the UNODC, the OSCE Programme Office in Bishkek, and representatives of the donor community.

UNODC conducts exercise to counter maritime crime in Sri Lanka

The United Nations Office on Drugs and Crime (UNODC) conducted a Visit, Board, Search and Seizure (VBSS) exercise at the Sri Lanka Navy Base in Trincomalee in November 2019. The exercise is part of a VBSS Boarding Officer training course delivered by UNODC's Global Maritime Crime Programme (GMCP) to coastguards from Malaysia, Indonesia, the Philippines, Thailand and Vietnam with the support of the Sri Lanka Navy.

Akira Sugiyama, Ambassador of Japan in Sri Lanka, a major supporter of GMCP's work in the region, attended the event.

Mr. Sugiyama said that "This program provides maritime law enforcement officers in the Indo-Pacific region with precious opportunities to receive training for the VBSS procedures, using actual dhow boats captured by the Sri Lankan Navy. In addition, through this intensive program, comradeship among law enforcement officers in the region is developed. We believe that this program contributes a great deal to the maritime security in the Indo-Pacific region, which is vital to maintain a free and open Indo-Pacific."

Unprecedented number of crew kidnappings in the Gulf of Guinea despite drop in overall global numbers

Despite overall piracy incidents declining in 2019, there was an alarming increase in crew kidnappings across the Gulf of Guinea, according to the International Chamber of Commerce's International Maritime Bureau's (IMB) annual piracy report.

In 2019, IMB's Piracy Reporting Centre received 162 incidents of piracy and armed robbery against ships worldwide, in comparison to 201 reported incidents in 2018. The incidents included four hijacked vessels, 11 vessels fired upon, 17 attempted attacks, and 130 vessels boarded, according to the latest IMB figures. While the overall decline in piracy incidents is an encouraging development, vessels remain at risk in several regions, especially the Gulf of Guinea.

Gulf of Guinea

The number of crew kidnapped in the Gulf of Guinea increased more than 50% from 78 in 2018 to 121 in 2019. This equates to over 90% of global kidnappings reported at sea with 64 crew members kidnapped across six separate incidents in the last quarter of 2019 alone.

The region accounted for 64 incidents including all four vessel hijackings that occurred in 2019, as well as 10 out of 11 vessels that reported coming under fire.

"We remain concerned that this region has recorded an unprecedented rise in crew kidnaps. These latest statistics confirm the importance of increased information exchange and coordination between vessels, reporting and response agencies in the Gulf of Guinea Region. Without the necessary reporting structures in place, we will be unable to accurately highlight the high- risk areas for seafarers and address the rise of piracy incidents in these persistently vulnerable waters." – Michael Howlett, Director of the ICC International Maritime Bureau.

Singapore Straits

Similarly, the Singapore Straits experienced a rise in armed robbery attacks with 12 reported incidents in 2019, including 11 in the last quarter of 2019. The same region accounted for just three incidents for the entirety of 2018. IMB's latest figures also report that vessels were successfully boarded in 10 incidents across the region last year. Despite this rise, IMB considers the intensity of the attacks in the Singapore Straits to be 'low level' and usually limited to armed robbery from the vessel.

"This is a distraction and potentially dangerous for the crew in control of the vessel whilst navigating through these congested waters", continued Howlett. "The IMB PRC is grateful to Singapore law enforcement agencies for responding promptly to some of these incidents."

Indonesia

Armed robbery attacks in Indonesian ports are down from 36 incidents in 2018 to 25 in 2019. Dialogue and coordination between the Indonesian Marine Police (IMP) and the IMB PRC has led to a decrease in regional incidents, according to the report.

Elsewhere, in the Indian sub- continent, Bangladesh reported zero incidents for 2019. This is the first time since 2015 that no piracy or armed robbery incidents have been reported around Bangladesh

No incidents in Somalia, but risks remain

Across the Indian Ocean, Somalia reported zero piracy incidents, yet the IMB PRC advises that vessels and crews remain cautious when travelling through the region. In particular, the report warns that "Somali pirates continue to possess the capacity to carry out attacks in the Somali basin and wider Indian Ocean."

As with all piracy- related incidents, IMB urges all shipmasters and owners to report all actual, attempted and suspected piracy and armed robbery incidents to the IMB PRC. This first step in the response chain is vital to ensuring that adequate resources are allocated by authorities to tackle this crime.

Source: ICC International Maritime Bureau

Image courtesy: Euronav

New Destructive Wiper "ZeroCleare" has been identified by IBM® X-Force® Incident Response and Intelligent Services (IRIS) Targeting the Energy Sector in the Middle East

IBM® X-Force® researchers have identified a new malware new malware which they have dubbed "ZeroCleare" which has been used in destructive attacks against the critical energy sector.

According to X-Force analysis, ZeroCleare was used to execute a destructive attack that affected organizations in the energy and industrial sectors in the Middle East. Based on the analysis of the malware and the attackers' behaviour, they suspect Iran-based nation-state adversaries were involved to develop and deploy this new wiper.

Given the evolution of destructive malware targeting organizations in the region, they were not surprised to find that ZeroCleare bears some similarity to the Shamoon malware. Taking a page out of the Shamoon playbook, ZeroCleare aims to overwrite the Master Boot Record

(MBR) and disk partitions on Windows-based machines. As Shamoon did before it, the tool of choice in the attacks is EldoS RawDisk, a legitimate toolkit for interacting with files, disks, and partitions.

Nation-state groups and cyber criminals frequently use legitimate tools in ways that a vendor did not intend to accomplish malicious or destructive activity. Using RawDisk with malicious intent enabled ZeroCleare's operators to wipe the MBR and damage disk partitions on a large number of networked devices. To gain access to the device's core, ZeroCleare used an intentionally vulnerable driver and malicious PowerShell/Batch scripts to bypass Windows controls. Adding these 'living off the land' tactics to the scheme, ZeroCleare was spread to numerous devices on the affected network, sowing the seeds of a destructive attack that could affect thousands of devices and cause disruption that could take months to fully recover from. These tactics resemble the way Shamoon was launched in attacks on Arabian Gulf targets in 2018.

X-Force IRIS assesses that the ITG13 threat group, also known as APT34/OilRig, and at least one other group, likely based out of Iran, collaborated on the destructive portion of the attack. X-Force IRIS's assessment is based on ITG13's traditional mission, which has not included executing destructive cyber-attacks in the past, the gap in time between the initial access facilitated by ITG13 and the last stage of the intrusion, as well as the different TTPs our team observed.

To date, X-Force IRIS has not found any previous reporting on the "ZeroCleare" wiper, its indicators, or elements observed in this campaign. It is possible that it is a recently developed malware and that the campaign we analyzed is one of the first to use this version.

TSP Projects has been acquired by international mass transit, mobility and infrastructure company SYSTRA

As a wholly owned subsidiary of SYSTRA Ltd the company will now be known as TSP Projects, a SYSTRA company. The investment marks a major milestone for SYSTRA, creating an 800 strong combined workforce in the UK and provides TSP Projects with a permanent owner. In the security industry, TSP Projects are experts in the

supply of Hostile Vehicle Mitigation measures for both short and long term requirements with a lineage that dates back to 2004. The modular PAS 68 range are some of the highest performing measures in their class with our re-deployable range forming a major element of the UK's strategic National Barrier Asset. Originally designed and tested as part of the Corus and then Tata Steel groups, these products and services were developed further under British Steel as TSP Projects and look forward to continued success under SYSTRA.

ReCAAP Conducts Anti-Piracy Capacity Building Programme for Senior Officers of Maritime Authorities and Law Enforcement Agencies in Cooperation with Vietnam Coast Guard

ReCAAP Information Sharing Centre (ISC) in cooperation with ReCAAP Vietnam Focal Point (Vietnam Coast Guard) convened the Capacity Building Senior Officer's Meeting in Hanoi, Vietnam.

The three-day programme will gather senior officers from 16 ReCAAP member countries as well as Malaysia and Indonesia to review the situation of piracy and armed robbery against ships in Asia including the incidents of abduction of crew in the Sulu-Celebes Seas, share specific case studies, and discuss ways to improve the maritime safety situation in Asia.

Complementing the programme is a lecture on international maritime laws and their applications, as well as a scenario-based exercise facilitated by Professor Max Mejia of the World Maritime University.

Participants of the programme will also have an opportunity to have a dialogue with the shipping industry based in Vietnam to better understand their concerns.

"The ReCAAP model is unique because it gives emphasis on information sharing among a network of 20 ReCAAP Focal Points across Asia, Australia, Europe and the United States as an approach to fighting maritime crimes," said Mr Masafumi Kuroki, Executive Director of ReCAAP ISC. "Thanks to the regional and international cooperation, incidents of piracy and sea robbery in Asia are decreasing. We will continue to strengthen the capability and cooperation of ReCAAP Focal Points and regional authorities to keep Asian waters—one of the most economically vital in the world—safe for seafarers, ships and cargoes."

The ReCAAP Member Countries represented at the Capacity Building Senior Officers' Meeting 2019 in Hanoi are Australia, Bangladesh, Brunei, Cambodia, China, India, Japan, Korea, Laos, Myanmar, the Philippines, Singapore, Sri Lanka, Thailand, the United Kingdom, and Vietnam.

FLIR Announces Multiple Cameras for Critical Infrastructure and Safe City Security

FLIR Systems have announced three dome-shaped, Pan-Tilt-Zoom (PTZ) security cameras, including two dual-sensor camera series for critical infrastructure locations the FLIR Elara™ DX-Series and the FLIR Saros™ DM-Series, and a high-resolution visible camera for safe city deployments, the FLIR Quasar™ 4K IR PTZ. The latest FLIR security products offer multiple lens options for long- and short-range needs to enable accurate perimeter protection of critical infrastructure, remote facilities, and in urban city environments, day or night.

Given the enhanced security requirements of critical infrastructure sites such as utility substations and transportation centers, the latest FLIR cameras featuring both thermal imaging and

4K high-resolution sensors, the Elara DX-Series and Saros DM-Series, deliver superior perimeter security protection in nearly all weather and light conditions. The FLIR Elara DX-Series features longer viewing range capabilities, infrared illumination, and a wiper blade that can be remotely operated for use in harsh conditions to ensure a clear view. The more compact Saros DM-Series provides shorter viewing range capabilities in a weatherized housing. Both series offer eight lens options to enable tailoring for the customer application and environment.

For the growing metropolitan city safety and security market, the Quasar 4K IR PTZ delivers high-resolution visible video quality with excellent low light capabilities to give operators high-fidelity monitoring in large and crowded coverage areas.

All three new FLIR security cameras provide a comprehensive end-to-end experience with seamless integration to FLIR Systems' video management system (VMS) platform, United VMS, or can serve as a complementary solution integrated with other major VMS platforms.

"With our latest products, FLIR is delivering advanced cameras purpose-built for perimeter protection and the evolving security needs of critical infrastructure sites and cities," said Travis Merrill, President of the Commercial Business Unit at FLIR. "For situational awareness in diverse environments including utility substations, data centers, oil and gas fields, airports, or cities, these perimeter protection cameras are designed to withstand harsh environments to help keep sites secure and people safe."

QinetiQ with strategic partner Inzpire successfully completed the first-ever series of UK sector-wide, cyber resilience exercises for the UK's Critical National Infrastructure (CNI) Electrical Distribution organisations

Cyber-attacks on individuals, commercial organisations, CNI and Government departments are increasingly common and constantly evolving, impacting on reputation, safety and share price. Whether it is due to hacktivists, cyber criminals or nation states, the cyber threat is one which the UK is trying to stay one step ahead of, in an environment without traditional boundaries and where the threat cannot always been seen and the impact is not immediately obvious.

Future generations of board level executives, operational managers and technical engineers must be equipped with the knowledge, skills and confidence in cyber capabilities to maximise the opportunities that cyberspace creates and ensure resilience against the potential threats. Cyber Security needs to form part of 'business as usual' activities, requiring education, training, operational planning & preparation and consideration throughout a capability or service lifecycle. Only then will an organisation be able to increase the awareness, skills and knowledge of operations within cyberspace and better understand how to plan and respond to threats, and to synchronise operations in

both the physical space and cyber domains.

QinetiQ's expertise, with over 20 years of experience in providing training, exercising and operational assurance, has been applied to the UK's electricity sector in a first of its kind series of sector wide cyber resilience exercises. Exercising increases the confidence of individuals, teams, organisations and sectors in their ability to identify, protect, detect, respond and recover in order to sustain operations in the event of cyber-attack.

QinetiQ as the Lead Exercise Integrator, working in partnership with BEIS, NCSC and strategic partner Inzpire, facilitated a series of exercises collectively known as "PowerPlay". PowerPlay was specially designed and executed to prepare and equip the electricity sector's engineering, operational and executive teams with the knowledge, skills and confidence in their processes and technologies to maximise the opportunities that cyberspace creates whilst ensuring resilience against the cyber threat.

The three exercises, started with an operational / command & control focused exercise to understand the role of individual organisations and how communications and decisions are made within the context of a much larger, coordinated sector wide incident. Following this was a live-exercise focused on the 3rd party supply chain (without knowledge that they were being exercised) to examine how they would analyse and fuse multiple cyber-incidents to create common situational awareness and coordinate incident response. The exercise series culminated in a large, distributed exercise involving over 170 participants at 13 different locations across the UK and abroad. A complex set of inter-connected events played out based on attacks varying from spearphishing to more specialist attacks on both IT and Operational Technology networks.

Dr Richard Randel, Principal System Engineer Cyber, Information and Training at QinetiQ said: "The exercise demonstrates how QinetiQ can work with Government partners and the CNI sector, bringing together our capabilities and experience, to increase the resilience of the UK and recognise the importance of exercising as a means to assure operations."

John, Scottish and Southern Electricity Networks said: "We would like to thank the NCSC for the invitation and our subsequent involvement in the sector-wide cyber security test. The challenge and results from the scenario exercising has been invaluable in applying improvements to our emergency planning and resilience processes, along with recognising the importance of cross industry support and alignment during such events."

A participant said: "It provided us with a greater awareness of the cyber threats within the sector and how all business functions need to work together to respond to a cyber-incident."

Cyber and information security consultancy Ascentor has launched a new service for SMEs called CyberWyse

It's a fast track approach to implementing the basic cyber security measures to protect against 80% of cyber attacks. CyberWyse combines certification for Cyber Essentials (CE) PLUS and the Information Assurance for Small Medium Enterprise (IASME) Governance Standard with cyber security insurance.

All delivered with expert full support from Ascentor. When implemented effectively, the two standards provide a holistic set of pragmatic, appropriate and cost effect controls that will thwart the majority of cyber attacks.

Commenting on the new service, Ascentor's MD, Dave James said "We designed CyberWyse for Small and Medium Enterprises (SMEs) who know they need to take action to improve their cyber security – but are just not sure what to do. It takes away the headache of not having enough time, skill or resource and helps you through a quick and effective approach to reducing your organisation's exposure to the cyber risk."

Schiebel Camcopter® S-100 Deployed for River Pollution Crisis in Malaysia Following Illegal Chemical Waste Dump

Schiebel's CAMCOPTER® S-100, supported by Three Tis Group, was deployed as a first emergency response providing critical situational information during the Kim Kim river toxic pollution crisis in Malaysia.

In March 2019 more than two tons of illegal chemical waste were dumped in the Kim Kim river, which is located near the largest industrial area in the South of Malaysia, Johor Malaysia. As a result, toxic fumes were released throughout the adjoining area affecting more than 6,000 people with many being hospitalised and numerous schools being closed.

The Malaysia Ministry of Energy, Science, Technology, Environment and Climate Change (MESTECC), in collaboration with Malaysian Armed Forces (MAF), called for a first emergency disaster response to analyse and scan the polluted river and adjoining area. The CAMCOPTER® S-100 was the Unmanned Air System (UAS) of choice and was deployed from March to September 2019 by MAF, supported by Schiebel's partner Three Tis Group, to gain situational information of the affected area. The UAS was operated by day and night for a total of approximately 30 flight hours.

The CAMCOPTER® S-100 was equipped with FLIR Systems Star SAFIRE 380-HDc, which delivers stabilised multi-spectral imaging and intelligence functions.

"The CAMCOPTER® S-100 is perfectly suited for emergency response in crisis situations. Given its small size and innovative technology it is capable of flying in difficult terrain whilst collecting valuable data," said Tunku Ahmad Zahir Bin Tunku Ibrahim, Managing Director at Three Tis Group.

360 Vision CCTV cameras - now with High Secure cyber protection

UK CCTV camera manufacturer, 360 Vision Technology, has announced that its Predator 'all-in-one' PTZ range is now an accredited Vision HS camera solution, certified to have completed the CAPSS approval process by the Centre for the Protection of National Infrastructure (CPNI).

Ensuring cyber security measures are capable of protecting against the very real threats faced by surveillance system operators, 360 Vision Technology's team of software developers is constantly working to ensure that these threats can be averted.

"There has been a lot of negative press relating to the potential vulnerabilities integrators may accidentally introduce into their customers' surveillance systems," says Adrian Kirk, Strategic Account Director at 360 Vision Technology. "With concerns over the ease at which some edge devices can be used as an

access gateway by cyber criminals, we're taking cyber security seriously and helping integrators to mitigate that risk by specifying Predator UK manufactured cameras and Vision HS video management software.

"Action to remove these threats is unlikely to happen fast as the UK market is still flooded by potentially unsafe Far East CCTV cameras, that are being sold at bargain basement prices, which make them commercially attractive to some purchasers.

The problem is further compounded by installation companies who may have limited expertise when it comes to providing tight network security. For example, steps should be taken to prevent the edge device's set-up browser being accessed - enabling a hacker to disable or change critical camera settings, or worse, access the wider corporate network. However, supporting peace of mind for any integrator or end-user, when a 360 Vision Technology Predator camera is deployed at the edge, it cannot be used to enable unauthorised access to a security or corporate network."

Despite the increased emphasis on cyber security, and more and more sophisticated cyber-attacks taking place, many leading camera manufacturers still supply easy to get to, direct access points (typically via an RJ45 port), located within a camera's power supply – but removing this risk is essential to ensure security and corporate confidentiality is not compromised.

"360 Vision cyber security protection ensures surveillance capability is not compromised, by removing the risks associated with insecure camera access," Adrian concludes. "To provide additional protection for our customers, we are proud to announce that the 'Predator HS' product range is now an accredited camera solution to work with Vision HS - certified to achieve CAPSS approval by the CPNI."

Aveillant's bespoke anti-drone system deployed at Heathrow to protect the UK's busiest airfield

Aveillant Limited, a Thales Company, has announced that its anti-drone systems have been deployed at Heathrow as part of the airport's bespoke set of end-to-end counter drone measures provided by Operational Solutions Ltd to help to keep the country's busiest airfield free from drones.

This one-of-a-kind Counter Drone system works by detecting and tracking drones in surrounding airspace and alerting airports of unauthorised drone use quickly and efficiently. This new and innovative system also works to locate the drone pilots themselves and can be used to identify their location.

This technology has been specifically designed for Heathrow Airport by Operational Solutions Ltd and comprises of a variety of leading counter drone technologies, including systems from Aveillant.

The fast and accurate detection of rogue drones helps to keep Heathrow's passengers and colleagues safe and will support the airport, law enforcement and air traffic controllers as they work to protect Heathrow's airspace. This new kit will enhance detection capabilities and minimise delays, helping passengers to get away on time. The technology will also help the airport to meet its sustainability objectives, by reducing the fuel wastage and additional flight stacking caused by unauthorised drones use.

Vehicle mounted net capture system was launched at DSEI London 2019

Test result white paper highlights SEEKERe as a solution to help prevent acts of terrorism at events, stadiums, arenas and other large-scale venue.

DetectaChem a manufacturer of handheld explosive and drug detection technology, today announced the publication of a white paper detailing analysis and findings following an in-depth Department of Defense evaluation of their SEEKERe handheld explosive detector specific to threat screening at security entry points.

2019 the SEEKERe was selected for evaluation by the National Center for Spectator Sports Safety and Security (NCS4) in collaboration with the National Sports Security Laboratory (NSSL) for evaluation of technologies needed to fill identified security gaps at sport and entertainment venues. The evaluation was part of a Department of Defense Domestic Preparedness Support Initiative (DPSI)

contract and the resulting 145-page assessment and evaluation white paper was published by the NSSL at the University of Southern Mississippi.

A selection of evaluation criteria included:

Detection of trace and bulk homemade, military and precursor explosive materials within 30 seconds.

Can identify, discover or locate threats or hazards through active search procedures.

Can prevent, avoid or stop an imminent, threatened or actual act of terrorism.

Provides Command the needed information to decide on evacuation or shelter in place.

SEEKERe obtained an overall evaluation score of 2.98/3.00 for Application, Capability, Ease of Use, Mobility, Purchasing Options, Maintenance and Environmental functionality.

These scores were determined by Subject Matter Expert evaluators and comprised over 37 different evaluation criteria.

Cited debriefing evaluator comments about SEEKERe included:

'Provides an additional tool for sports and entertainment security to address an explosive attack.'

'SEEKERe is faster to deploy than a K-9 or bomb squad to clear unattended bags.'

'Should deter a potential bomber trying to bring in explosive compounds into a facility.'

'Detects trace explosives on bag carrying handles, inside bags, or on hands or clothing.'

'Gives venue security personnel needed information for setting a minimum area of safety based on the FBI Bomb Safety Card for protection of spectators.'

ARES Security And Bevilacqua Research Sign Agreement To Launch AI Decision Support Software

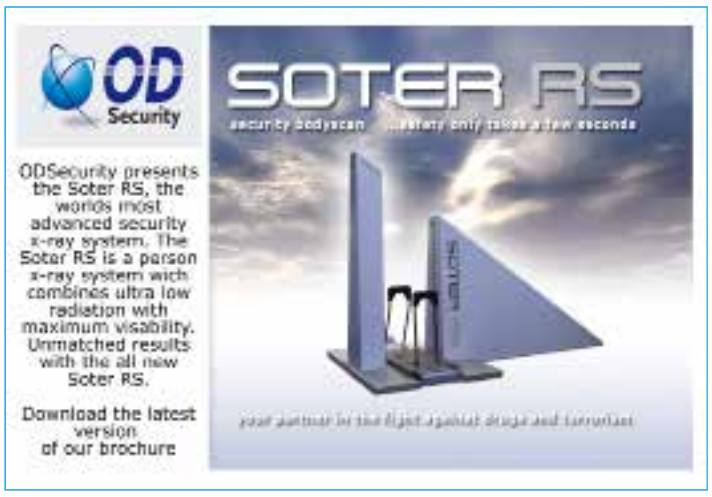
ARES Security and Bevilacqua Research Corporation (BRC) have signed a Strategic License and Alliance Agreement to further develop artificial intelligence software solutions that meet the market demands of DoD, Government, Commercial and Critical Infrastructure customers who require rapid decision support to respond to major incidents and complex threats. Under the agreement, ARES Security will develop commercial software for rapid decision support, called AVERT AI. Threats are evolving at an accelerated pace making the ability to quickly identify and appropriately respond increasingly challenging. Experience and in-depth training are essential to quickly make the right decision for an effective response. But it is nearly impossible to train and prepare for each potential threat scenario and even more unlikely to have the experience required to respond to emerging sophisticated threats. Together, ARES Security and BRC will market AVERT AI and build solutions that improve the rapid decision-making process that is increasingly critical to incident response when seconds count.

World Security Report

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

Border Security Report

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



January 2020

17-17
Risk Managemrnt Conference
Miami, USA

20-21
Cyber Security for Critical Assets MENA
Dunai, UAE

20-22
Africa Maritime Security Forum
Dakar, Senegal

February 2020

4-5
European Police Congress (EPC)
Berlin, Germany

5-7
Privacy and Security Conference
Victoria, Canada

11-12
Cyber Risk Insights Conference
San Francisco, USA

13-15
International Fire, Safety and Security Expo
Dhaka, Bangladesh

24-29
Secure India
Bengaluru, India

March 2020

3-5
Security & Policing
Farnborough, UK
Securityandpolicing.co.uk

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

17-18
Cyber Security & Cloud Expo Global 2020
London, UK
www.world-border-congress.com

March 31-2 April
World Border Security Congress
Athens, Greece
www.world-border-congress.com

April 2020

28-30
Critical Infrastructure Protection & Resilience North America
New Orleans, LA, USA
www.ciprna-expo.com

ADVERTISING SALES

Paul Gloc
UK
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

For Rest of World contact:
E: marketing@knmmedia.com
T: +44 (0) 1273 931 593

critical infrastructure PROTECTION AND RESILIENCE EUROPE

6th-8th October 2020

Bucharest, Romania

www.cipre-expo.com

CALL FOR PAPERS

Abstract submittal deadline - 28th February 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: