critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

SPRING 2024
www.cip-association.org

FEATURE:
Protect our Electric Grid – Before it's Too Late

FEATURE:
Connecting Unrelated Industries Strengthens All Sectors

FEATURE:
Break down cyber and physical security silos to improve protection and operations

PROTECTING LIFE - SECURING AGRICULTURE

INVITATION TO PARTICIPATE

Securing the Inter-Connected Society

The premier event for the critical infrastructure protection and resilience community.

The first 'Critical Infrastructure Protection Week' will take place in Madrid Spain and will see IACIPP host the 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'EU-CIP Horizon Project' conference as the first events as part of this initiative.

Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe.

The conference will look at the developing themes and challenges facing the industry, including the importance of the updated NIS2 Directive and Directive on the Resilience of Critical Entities and the obligations of CI owner/operators and agencies, as well as create a better understanding of the issues and the threats, helping to facilitate the work to develop frameworks, good risk management, strategic planning and implementation.

Join us in Madrid, Spain for the the 9th Critical Infrastructure Protection and Resilience Europe discussion on securing Europe's critical infrastructure, part of CIP Week in Europe.

www.cipre-expo.com

Leading the debate for securing Europe's critical infrastructure

Co-Hosted by:

International Association of CIP Professionals

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

To discuss exhibiting and sponsorship opportunities contact:

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

Jina Lawrence
(Rest of World)
E: jinal@torchmarketing.co.uk
T: +44 (0) 7958 234 750

Ray Beauchamp
(Americas)
E: rayb@torchmarketing.co.uk
T: +1-408-921-2932

INFORMATION SHARING, COLLABORATION, COOPERATION ARE STILL CHAMPION

Since the last edition of CIPR News, we enjoyed the lively discussion at the 2024 Critical Infrastructure Protection & Resilience North America in Lake Charles, Louisiana, and the gathering of nearly 400 delegates enjoying the opportunity to share experiences, knowledge and skills, and more importantly to collaborate and cooperate with ideas.

What these discussions continue to highlight is the importance of those discussions and information sharing. Whether from government to operator/ industry, or industry to operator (or even industry to government) it is this information sharing that enables us to plan and prepare for what's around the corner. Resilience is all about planning and preparation, with the old adage from Benjamin Franklin 'By failing to prepare, you are preparing to fail' being as relevant now, as it was in 1790.

In Europe the International Association of CIP Professionals launches CIP Week in Europe in Madrid, Spain in November, with the aim to highlight and encourage greater information sharing and collaboration across countries and industries.

In this issue, we reflect on much of those words, with some great features from highly respected industry experts, that we hope you enjoy reading and find beneficial in your endeavours to provide your CI assets the best security and resilience.

And in fitting style, please feel free to share this issue with your colleagues who can also benefit from its news and features!

Thank you.

Ed.

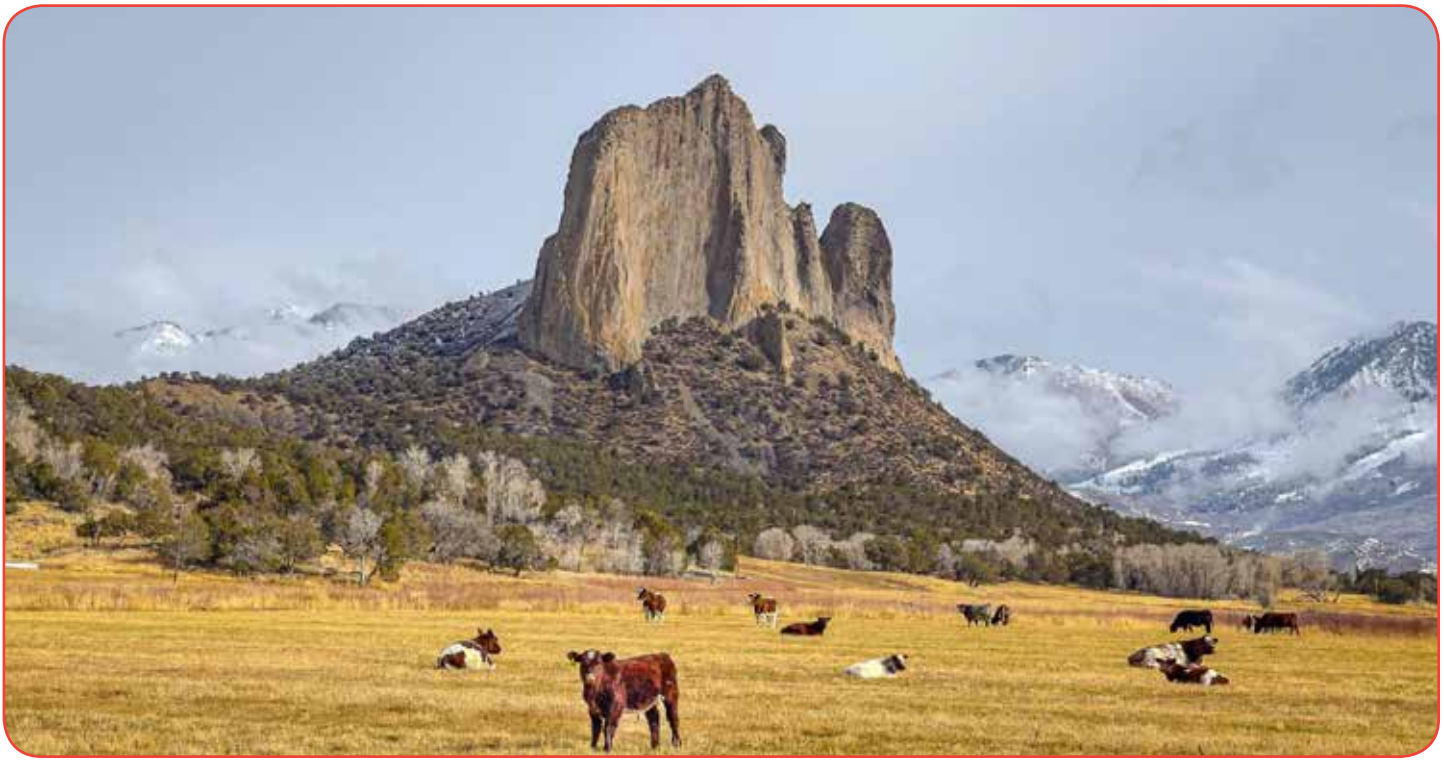
www.cip-association.org

Editorial:
Neil Walker
E: neilw@torchmarketing.co.uk

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

Critical Infrastructure Protection & Resilience News is the newsletter of the International Association of CIP Professionals and distributed to over 80,000 organisations globally.

Protecting Life - Securing Agriculture



By Dan Frazen, CO-CEM, Agriculture Emergency Co-ordinator (All Hazards), Colorado Dept of Agriculture

Images courtesy of Kris Stewart, Emergency Manager, Delta County (Colorado)

Whether a person had a bowl of cereal or a ribeye steak for dinner last night, it does not take much to convince our citizens that food & agriculture is one of the most important critical infrastructure sectors. Critical infrastructure protection (CIP) experts understand the interconnectivity and obvious dependence the Food & Agriculture Sector has on other sectors (e.g., Water, Transportation, Energy). We can also review the Federal Emergency Management Agency (FEMA)'s Community Lifelines and quickly visualize those same connections. Our agriculture supply chains are complex, the world is a dangerous place with threats looming, and we have an obligation to prepare and protect this sector at all levels.

The Importance of Agriculture

According to the United States Department of Agriculture (USDA) Economic Research Service (ERS), in 2023, agriculture, food, and related industries contributed 5.6% to the United States Gross Domestic Product (GDP) or $1.53 trillion. Agriculture workers comprise 10.4% of national employment. The ERS also estimated that there were 879 million acres of farmland in the US last year. In the State of Colorado alone, agriculture and agribusinesses contribute over $47 billion annually to the state's economy. There are approximately 39,000 farms and ranches in the

state, providing almost 200,000 jobs for Coloradoans. Colorado, although not a "dairy state," also has 200,000 milking cows, and is home to Leprino Foods, the world's largest pizza cheese (mozzarella) manufacturer. According to a Forbes report, this global dairy leader employed 5,000 people in 2023, and had a revenue of $3.6 billion thanks to pizza delivery chain restaurants and frozen pizzas.

Initiatives Past and Present to Protect Agriculture

If we look back over the past two decades at the relevant history, we see a theme that emerged during the Global War on Terror after the September 11th Attacks, and it persists today. Agriculture in the North America is vulnerable and criminals, terrorists, and our adversaries will attempt to exploit the vulnerabilities. An attack on agriculture would destroy communities in rural America and have a profoundly negative impact on state, provincial and national economies.

On November 19, 2003, the United States Senate Governmental Affairs Committee held a hearing entitled "Agroterrorism: The Threat to America's Breadbasket." The senators mentioned the caves of Afghanistan, a Central Intelligence Agency (CIA) report on the 9-11 hijackers being interested in crop dusting, and that agroterrorism was a true threat to the US economy. The committee chairperson for that hearing, Senator Susan Collins, stated that America's agriculture and food industry were just as important as America's urban centers and ports.

Former Senate Majority Leader Tom Daschle of South Dakota often spoke about the US military locating evidence that Al Qaeda

would target agriculture in the US homeland, which begins the timeline for this summary. Coincidentally, or perhaps not, the original Homeland Security Presidential Directive (HSPD) 8 was issued that same year, implemented via the National Planning Scenarios.

• 2003 - Al-Qaeda Cave in Afghanistan - Ag articles, USDA documents, List of six pathogens that target livestock and poultry located by special operations troops (also National Planning Scenario 14; Biological Attack - Foreign Animal Disease was published).

• 2007 – The Congressional Research Service (CRS) published a report titled Agroterrorism: Threats and Preparedness with the quote that agroterror attacks were "not about killing cows," but rather "causing economic damage, social unrest and loss of confidence in the government."

• 2015 – The Blue Ribbon Study Panel published A National Blueprint for Biodefense which stated, "The Food and Agriculture critical infrastructure sector is a distributed and highly complex system," and agriculture security is an important component of our national security.

• 2021- Presidential Executive Order 14017 on "America's Supply Chains" directed federal agencies to secure and strengthen the agriculture supply chain - USDA Agri-Food Supply Chain Assessment: Program and Policy Options for Strengthening Resilience identified six (6) vulnerabilities and made nine (9) recommendations. "Diversify" was the most important take-away.

• 2022 - National Security Memorandum (NSM) 16 - Strengthening the Security and Resilience of United States Food and Agriculture was published. David Steifel, Director of Biodefense on the National Security Council (NSC), engaged with agriculture emergency management associations and emphasized the importance of securing agriculture.

• 2024 - 118th Congress - Arkansas Senator Tom Cotton and New York Senator Kirsten Gillibrand are sponsors of the Farm and Food Cybersecurity Act, which is legislation that directs "the Secretary of Agriculture to periodically assess cybersecurity

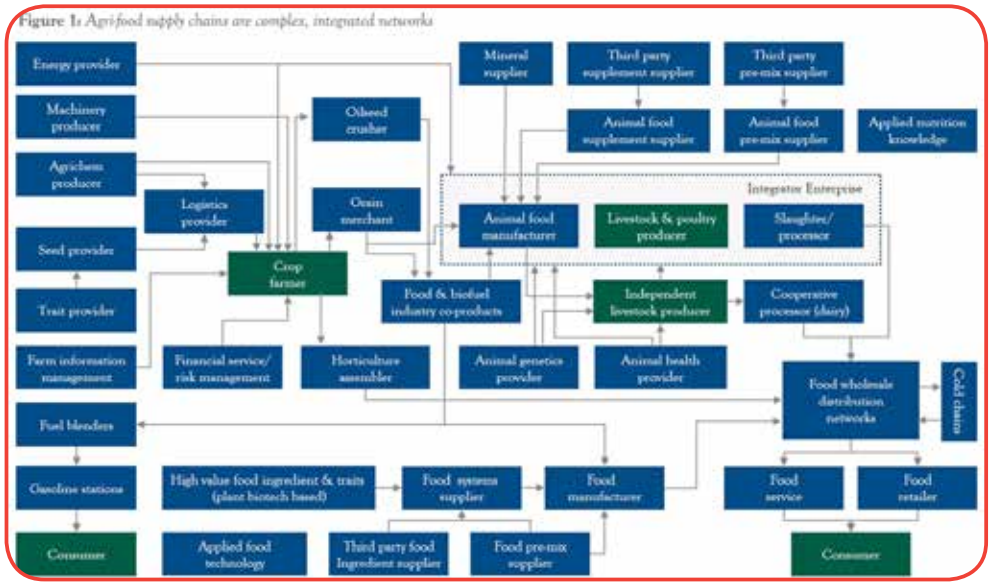


Figure 1: *Agrifood supply chains are complex, integrated networks*

threats to, and vulnerabilities in, the agriculture and food critical infrastructure sector and to provide recommendations to enhance their security and resilience, to require the Secretary of Agriculture to conduct an annual cross-sector simulation exercise relating to a food-related emergency or disruption, and for other purposes."

US Congressman Brad Finstad of Minnesota introduced and publicly supports the Farm and Food Cybersecurity Act, he stated, "Food and farm security is national security." Is it remarkable that the agriculture security message is the same from 2003 to today?

Understanding the Vulnerabilities and Threats

The US National Preparedness Goal says, quite simply: "Prevent, Protect, Mitigate, Respond, Recover." CIP, Homeland Security, and Law Enforcement professionals should always prioritize the defense of agriculture and food, but it is apparent that our attention is not always on raising livestock or growing crops to feed the world. There are so many different threats across all critical infrastructure sectors.

The agriculture sector is almost entirely under private ownership, which results in very different approaches to biosecurity and physical security across North America. The argument that rural, agricultural communities are underserved is a real one. Metropolitan areas have significantly more resources for all things security-related, raw materials, water supply, and transportation. And as previously mentioned, the supply chains upstream and downstream of a farm or ranch are complex.

Ag Vulnerability 101:

• The Food & Agriculture Sector is interconnected and dependent on other important critical infrastructure sectors.

• Agriculture business continuity can be challenging with single points of failure in supply chains, limited transportation routes and conveyances, and/or austere weather conditions with more drought, wind, fire, etc.

• The open range have large expanses of land that are not watched or even visited frequently. A rural sheriff's office may not have surveillance capabilities or even the staffing to patrol near farms and ranches, and producers may not see the need for fencing, cameras, drones, or anti-theft devices.

• The US Agriculture Transportation System is one of the most efficient transportation networks in the world, making for efficient contributions to commerce (and the economy), but also creating a target-rich environment for bad actors.

Humans are the greatest threat to agriculture. Natural hazards, to include drought, wildfires, severe weather, flooding, and plant & animal disease, are awful, but people are worse. The following groups can easily weaponize pests, tamper with chemicals, sabotage equipment, steal animals, or simply set a haystack on fire on a windy day.

Bad Actors:

• **Insiders** – The disgruntled worker motivated by revenge or hate is almost unstoppable.

• **Criminals** – The worst of society target the vulnerable for profit or because they are evil.

• **Competitors** – Those that injure and damage for a business advantage are in every industry, to include food and agriculture.

• **Activists / Domestic Extremists** – Anti-commercial agriculture views motivate a small, but often loud section of our populous. Ecological (Eco) Terrorists, Animal Rights Activists (not Welfare), and Radical Environmental Advocates are in this group.

• **Terrorists** – International or domestic terror cells attack agriculture with political and religious aims.

• **Adversaries** – The nation-states that wish ill upon the US

government are China, Russia, North Korea, and Iran for a myriad of reasons.

Knowing the usual suspects in a specific region is extremely important. For instance, in Colorado, the state's largest extremist group that threatens commercial animal agriculture is Direct Action Everywhere, also known as DXE. This group advocates for the total liberation of animals, and their direct action is burglary, theft, and criminal mischief under the guise of "rescuing" farm animals. Across the Western and Southern US, the Peoples' Republic of China is monitored by federal law enforcement and intelligence agencies when the communist party acquires agriculture data companies, purchases agriculture land near US Department of Defense (DOD) or US Department of Energy (DOE) facilities, or is involved in American agriculture technologies and seed research. Are China's initiatives in North America food security for a nation with over 1.4 billion people or attempts at espionage?

The Best Practices

Partnerships that collaborate and communicate on agriculture security are the key to successfully preparing and protecting the Food & Agriculture Sector. Several regions in the US have built AgSecure Working Groups to identify threats and share information. AgSecure brings together state and federal agencies with agriculture professionals, veterinarians, CIP or homeland security experts, law enforcement officers, inspectors (regulators), intelligence analysts, and emergency managers. These multi-disciplinary teams work closely with their field teams to have their

fingers on the pulse of agriculture, ag business, and the threats and hazards that could impact agriculture or the food supply. The positive relationships that are built in working groups often lead to other beneficial projects and initiatives. The AgSecure Working Group for the Rocky Mountain Region is led by the Colorado Department of Agriculture (CDA), and after re-starting their group two (2) years ago, the CDA now works closer with the Federal Bureau of Investigation (FBI), Colorado's state fusion center, and the US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Currently, the CDA's Agriculture Emergency Coordinator and the Region 8 CISA Cybersecurity Advisors (CSAs) are collaborating on a cybersecurity campaign specific to farms and ranches in rural Colorado.

Emergency managers and coordinators in state departments of agriculture and in the United States Department of Agriculture (USDA) are an outstanding place to start when building an AgSecure Working Group. Agriculture emergency managers understand the complexities of agriculture and the importance of drawing subject matter experts (SMEs) from all disciplines. These organizers have expertise in planning and logistics, and they promote a common operating language and picture. Most are members of agriculture emergency management associations, such as the National Alliance of State Animal and Agricultural Emergency Programs, the Multi-State Partnership (MSP) for Security in Agriculture, the Southern Agriculture & Animal Disaster Response Alliance (SAADRA), the Extension Disaster Education Network (EDEN), and the Western States Agriculture Resiliency Partnership (WSARP). These associations, much like CIP associations, have a stockpile of valuable resources to help protect agriculture.

We need to make a stronger commitment today to defend our homelands and protect our economies by prioritizing the security and business continuity of farms, ranches, and agricultural businesses across North America. The Food & Agriculture Sector, although vulnerable, can be better protected by regional, multi-disciplinary teams that coordinate, collaborate, and communicate.

Live Webinar: Enhancing Supply Chain Resilience through Government-Industry Collaboration

Tuesday 4th June 2024 - 11am EST / 4pm UK

In this webinar, we will explore the growing supply chain security challenges faced by organizations and critical infrastructure companies in ensuring their hardware and software remain free from cyber threats and attacks. This challenge has prompted substantial global government intercession with many recommendations, publications and outright legislation having been enacted.

This webinar will focus on initiatives of the U.S. Federal Government and its agencies. Our expert panel will discuss how Standards Development Organizations (SDOs) are aligning new standards with government goals of improving the nation's cyber and supply chain position for critical infrastructure.

Learning Outcomes:

- Elements critical to enhancing an organization's security posture
- Government initiatives focused on Cybersecurity and their impacts on the ICT and critical infrastructure industries
- Public and private partnerships to advance the goal of creating and maintaining trusted networks

SPEAKERS:

- Michael Bergman, Vice President of Technology and Standards, Consumer Technology Association (CTA)
- Mike Regan, Vice President, Business Performance, Telecoms Industry Association (TIA)
- Senior Representative, Cybersecurity & Infrastructure Security Agency (CISA)

REGISTER ONLINE TODAY AT
www.cip-association.org/supply-chain-webinar

New funding approved to strengthen Multi-Hazard Early Warning Systems in the Caribbean

The Caribbean is the second-most disaster-prone region in the world and is highly exposed to natural hazards such as hurricanes and tropical storms, floods, landslides, and storm surges. These hazards pose a risk to life and economic loss. To combat this, US 7 million dollars in funding for a new three-year project in the Caribbean region has been granted by the Climate Risk and Early Warning Systems (CREWS) Initiative.

The CREWS Caribbean 2.0 project will build on a recently completed project to continue strengthening early warning systems in the region. The project will be led by WMO and UNDRR, and implemented under the leadership of key regional organizations including the Caribbean Meteorological Organization (CMO), the Caribbean Disaster Emergency Management Agency (CDEMA), and the Caribbean Institute for Meteorology and Hydrology (CIMH). Other major partners include the International Federation of Red Cross and Red Crescent Societies (IFRC), the International Telecommunications Union (ITU) as well as the Caribbean Chamber of Commerce (CARICHAM).

Approval for the project followed a collaborative and inclusive project development process which was completed at the CREWS Caribbean Partners Meeting, held in Trinidad and Tobago in November 2023. The meeting secured final endorsement of the proposed activities from key regional partners. It was hosted by the CMO and CDEMA and convened over 47 members of the Regional Early Warning Consortium (REWSC), which will function as Project Steering Committee, as well as the President of the WMO Regional Association IV and CREWS Steering Committee Members and partners.

Effective Multi-Hazard Early Warning Systems (MHEWS) in the Caribbean region can only be made possible through the strong leadership of strengthened NMHSs, with the alignment of NDRMOs, who integrate co-design and delivery approaches in their services. This will enable improved disaster risk knowledge, better monitoring and forecasting, stronger warning and dissemination capabilities, and enhanced response capabilities of individuals, communities, business institutions, and organizations, with a particular focus on reaching and involving the last mile and the most vulnerable groups.

The main objective of CREWS Caribbean 2.0 is to enhance the operational capacities of NDRMOs and NMHSs, through regional cooperation and improved governance mechanisms conducive for users to participate and be engaged in the design and delivery of early warnings. The project will focus on strengthening MHEWS Governance on a regional level, improving disaster risk knowledge on the regional, national, and community levels, strengthening NMHs service provision, with a special focus on marine, severe weather, and hydrological capacities, strengthen warning dissemination and reinforce early action at the community level. In doing that, the project will contribute to the goals of the Early Warnings for All (EW4All) Initiative and other international frameworks, such as the SDGs, the Sendai Framework for Disaster Risk Reduction 2015-2030, or the Paris Agreement, while applying inclusive and gender responsive approaches, to ensure that those most at risk are engaged meaningfully in the development of MHEWS. The project will further build on the outcomes and achievements of CREWS Caribbean 1.0.

Protect our Electric Grid – Before it's Too Late

By Lt. Col. Tommy Waller (USMC Ret.) is the President & CEO of the non-profit public-interest Center for Security Policy. He is also co-director of the nationwide Secure the Grid Coalition.

Unless mitigation hardware is installed, the electrical grid – and all the critical infrastructures which depend on it – are at risk of catastrophic failure… from natural causes.

All Critical Infrastructures Depend on The Electric Grid

Modern civilization depends on electricity for every aspect of life and for the functioning of the wide range of critical infrastructures that sustain it. Almost without exception, the owners and operators of these critical infrastructures consume electricity from an outside "electric grid" rather than producing it on-site. This means that if the electric grid were to fail, resulting in widespread and long-term blackouts, these life-sustaining infrastructures would grind to a halt.

Lt. Col. Tommy Waller (USMC Ret.) , President & CEO, Center for Security Policy

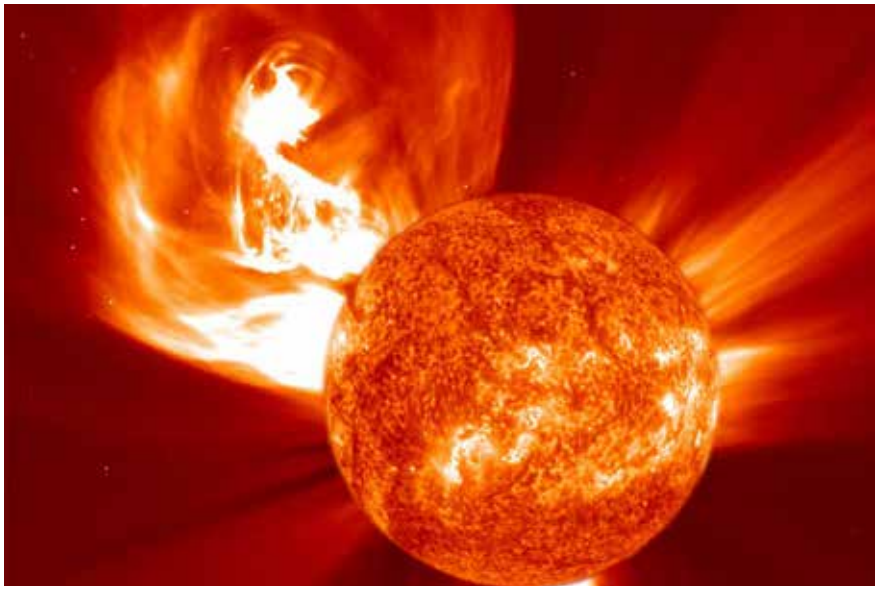
Modern societies are not prepared to live even a short time without electricity, especially in urban environments. In July 1977 a lightning strike took out three electrical substations in New York and caused a cascading power failure across the river in New Jersey. In less than one hour the entire city of New York was in total darkness. Civilization broke down after only 24 hours without electricity. In the ensuing chaos over 550 police officers were injured in the line of duty, 4,500 looters had been arrested and property damage was estimated at $300 million.

Suburban and rural populations may only be slightly more insulated to the immediate societal chaos from a blackout, but they are far from immune to its long-term devastating effects. Cold weather brought down the electric grid in Texas in February 2021 and in a blackout lasting only three days, more than 240 people died and the Texas economy sustained economic losses in the tens of billions of dollars.

While the state of Texas took aggressive action to fortify its grid against cold weather in response to this catastrophe, neither Texas, nor the rest of America, are prepared for the devastation that could come from another threat from Mother Nature – the sun.

The Sun: A Source of both Energy and Danger

Most people regard the sun as a positive source of energy for the planet – nurturing plant life and powering solar panels to help generate electricity. And while we know that we must be protected from the harmful UV rays the sun



Coronal Mass Ejection (CME) captured on camera by NASA – NASA's Goddard Space Flight Center/STEREO/Bill Thompson

produces, which cause injury such as sunburn and skin cancer, most don't realize that the sun can produce even more powerful effects, damaging infrastructure both in space and on earth.

Scientists in the late 19th century observed that the Sun produces "sunspots" and "solar flares." These events sometimes correspond to incredible arrays of lights in the night sky (such as the Aurora Borealis AKA "Northern Lights".) Sometimes, these visual events are followed by physical phenomena on earth – such as the massive solar storm in 1859 that caused Aurora Borealis to be seen as far south as New Orleans and Cuba.

The corresponding effects on earth during that 1859 solar storm (known as the "Carrington Event") included telegraph machines catching fire – which scientists later determined was the result of ground induced currents (GICs) traveling through the earth's crust. Eventually scientists discovered these GICs were created by the earth's magnetic field when it is struck by the invisible magnetized particles expelled from the sun during the storm – something they named a "Coronal Mass Ejection" (CME).

Solar Weather Damages Transformers & Other Infrastructures

When a CME strikes earth's magnetosphere, it causes a Geomagnetic Disturbance (GMD). This disturbance creates large ground induced currents (GICs) in the earth's crust "looking" for the "path of least resistance." Long conductors, such as telegraph lines, railroads, and – now – the long transmission lines of the electric power grid, quickly become that "path." These damaging currents in the ground travel up the ground connection of transformers, into the electric grid, across high voltage/low resistance transmission lines, causing thermal and harmonic damage to connected equipment. This includes large power transformers such as the one catastrophically damaged during a

March 1989 magnetic storm damage to a high-voltage transformer at a nuclear power center in Salem, New Jersey.

This transformer sustained major damage from GICs induced by the March 1989 Solar Storm. Photo credit: Dr. Jeffrey J. Love, USGS

much smaller solar storm in March 1989 at a nuclear power plant in Salem New Jersey.

It is important to note that we have not experienced a devastating solar super storm since the modern grid was developed. Each year as we expand the grid and connect the neutrals of additional transformers to the ground, we provide more entry points for GIC into the grid and it becomes more vulnerable. The March 1989 Solar Storm that damaged the above transformer and blacked out Quebec is regarded as a "40-year" solar storm (i.e. the moderate type that strikes earth roughly every 40 years). Just 9 hours without power as a result of this event caused USD13.2 billion in economic loss.

The 1859 Carrington Solar Storm is considered a much more powerful "100-year" storm and would thus cause much more catastrophic and widespread damage to transformers. Lloyd's of London estimates the economic cost of a Carrington-class solar storm on the North American electric grid at between USD600 billion to 2.6 trillion based on value of lost electrical load, not to mention the immense loss of human life.

It is a statistical certainty that the earth will experience another Carrington-class or larger event in the future. Unless modern societies take action to install mitigation hardware to block GICs produced by solar weather, such an event could result in the catastrophic loss of the electric grid.

But it's not just 40 and 100-year storms that cause damage to electric infrastructure connected to long transmission lines. A joint study by the global insurance leader Zurich and Lockheed Martin concluded that space weather has "an average impact on the order of USD10 billion per year each for both the overall US and European economies." This is due to the relatively small GICs generated during normal solar activity that travel through the crust of the earth, invade the electric grid through the grounded neutral connection of transformers, causing transformers to saturate and generate harmful "harmonics" which then travels down transmission lines into machinery powered by the grid. This means that critical infrastructure owners may experience malfunctions and increased maintenance requirements of grid-connected machinery specifically because harmful GICs were not blocked at the point of entry at the high voltage generation and transmission level of the electric grid.

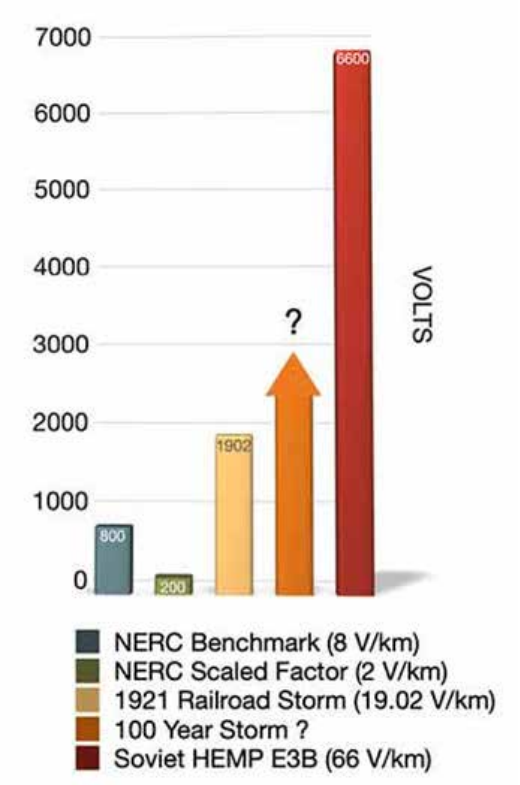
Critical infrastructure owners and operators worldwide cannot afford to prematurely lose equipment and grid operators definitely cannot afford to lose transformers during a time when supply chains are already strained. Russia's present war against the Ukraine and its targeting of electric infrastructure has placed major demand on electrical components such as transformers. Additionally, the worldwide exponential growth in the electrification of infrastructure (ranging from transportation to cookware) has increased demand–causing modern-day lead times to now extend into a range of 4-6 years for large transformers. What this means is that nations cannot afford to lose even a small number of transformers to harmful GICs without major, potentially catastrophic, consequences.

North America's Decade of Inaction

Since May 2013, the agency of the United States government that regulates the bulk power grid (FERC) has required the electric utility industry in North America to establish and enforce a standard to protect the grid, especially those irreplaceable transformers, against a 100-year solar storm. National security experts, engineers, and solar weather scientists have warned for 11 years that the standard set by utilities is insufficient, even dangerously low, a reality recently confirmed in a peer-reviewed study by world-renowned scientists.

Nearly two years ago the U.S. Secretary of Energy Advisory Board (SEAB) was advised of the transparent deficiency in the current solar storm standard for the electric grid. Verbal and written testimony to the SEAB revealed the startling low level of protection required by the standard, which won't even be enforced until 2028.

The field strength of a solar event is measured in volts per kilometer ("V/km") and directly relates to how large the resulting GICs will be. The testimony pointed to a case study for the Virginia / Washington D.C. area and included a bar graph depicting the field strength (2 V/km) the current standard requires to protect against (in green) versus the field strength levels (and resulting GICs) produced in the 1921 Railroad Storm (19.02 V/km - in yellow), the larger Carrington event (in orange), and even those produced by Soviet high altitude nuclear tests (66 V/km), since nuclear EMP causes a similar and even stronger field strength and resulting GICs on the grid (in red).



This bar graph (utilizing the average 100 km length of a transmission line) was included in testimony to the U.S. Secretary of Energy Advisory Board (SEAB) and depicts the current level of protection of the grid in Virginia (green) versus known and suspected hazard levels (yellow, orange, and red).

The Good News: It's a Fixable Problem

The good news is that there are known, tested, and affordable technological solutions to protect our vital transformers and other critical infrastructures against GICs caused by solar weather. These are neutral blocking devices (NBDs) that can block these harmful ground induced currents at the point of entry, preventing them from invading the electric grid. NBDs not only protect irreplaceable transformers and high voltage breakers from damage, but also block out routine GICs that occur regularly, causing harmonics "downstream" in the grid and harming other critical infrastructures.

One such NBD, produced by Emprimus, is known as "SolidGround". It is a standard "one size fits all" product for all high voltage transformers (regardless of design) which is simply inserted in the transformer's neutral connection. Instead of running a high voltage transformer's copper wire directly into the ground, the utility runs the copper wire through the grounded NBD. The NBD then automatically detects and blocks the ground induced currents from entering the grid through that copper ground wire during a solar storm. A utility doesn't need to touch the high voltage phase lines that run the electricity to the rest of the grid, but rather install the NBD on the transformer's ground connection.

After years of use in the live power grid in at least three critical infrastructure substations in the North American electric grid, this "SolidGround" system has emerged as a tested and confirmed solution to mitigate the destructive impact of GICs. For example, American Transmission Company (ATC) has operated the "SolidGround" NBD since 2015. In 2019, Mr. Jim Vespalec, the Director of Asset Planning & Engineering for ATC, testified in front of the U.S. Senate Committee on Homeland Security and Governmental Affairs, reporting flawless performance with "several dozen" successful operations and "no adverse operating complications."

Similarly, the Western Area Power Administration (WAPA) has been utilizing the "SolidGround"

"SolidGround" on 345KV transformer in the ATC grid in Wisconsin (9+ years of testing)

"SolidGround" NBD protecting DOE's 345 kV transformer in the WAPA grid in South Dakota.

NBD solution since November 2022, where it has detected GIC and automatically engaged its protection 17 times in the past 12 months alone. Additionally, the Tennessee Valley Authority (TVA) implemented the "SolidGround" NBD system on a massive $20 million 500 kV transformer and it has also demonstrated its efficacy during critical events engaging its protection multiple times during solar events, with no problems.

What all this means is that "SolidGround" is activating and working during even very minor solar weather events, blocking GICs and preventing the resulting harmonics that can damage other critical infrastructures resulting in large economic loss on an annual basis. It also means that the technology will have no problem detecting and mitigating significant currents associated with the larger "40-year" or "100-year" storms that could devastate large power transformers and blackout the entire electric grid.

Solar Storm Protection is Affordable

Given the statistical near certainty that earth will be struck by a major solar storm in the future, the transparently defective protection standard, the $10B annual economic losses from routine solar weather and the availability of at least one extensively tested solution already operating in at least three locations in the North American grid, one might wonder why more action hasn't been taken. Some wrongly assume the effort would be too costly.

Not all portions of the grid and not all transformers are vulnerable to the GICs generated by solar weather. For those which are vulnerable, the "SolidGround" solution costs approximately $500,000 per transformer. Using this cost estimate and an analysis of vulnerable transformers, independent experts from the Foundation for Resilient Societies estimate that it would cost $4.1 billion to harden the entire U.S. electric grid against the devastating impact of GICs produced by solar weather. This estimate closely matches the estimates of Mr. Scott McBride of the U.S. Department of Energy's prestigious Idaho National Laboratory (INL) in his 2018 testimony before the U.S. Senate Homeland Security and Governmental Affairs Committee.

The Solution is "Bottom Up" Action

Despite the aforementioned warnings, and the fact that the U.S. Government passed a $1.2 trillion Infrastructure Bill in recent years, literally no action has been taken on the part of the current U.S. Department of Energy to protect the North American grid. This means that it is up to the states and the electric industry to take action.

The fastest way to solve this problem is through the creation of financial incentives and penalties by the entities who regulate utilities at the state and local level. Admittedly, electric utilities face daunting regulations from all quarters, ranging from environmental to security, and often find themselves in an impossible position where following one regulation will cause them to break another. When faced with such quandaries, they often end up choosing to "break" the regulations with the least financial penalties. Similarly, when choosing how and where to invest time, talent, energy, and resources – they ask themselves "where's the money?"

Understanding these basic tendencies in the wake of Winter Storm Uri in Texas, the state legislature passed laws that empowered the Texas Public Utility Commission to (1) create an effective weatherization protection standard at the state level, (2) impose financial penalties for grid operators who violate the standard, and (3) provide for "cost recovery" mechanisms to cover the costs of upgrades to meet the standard. This largely "solved" the cold-weather problem for the state's electric grid.

Admittedly, Texas is unique in that it has its "own grid" and does not fall under the jurisdiction of the U.S. Federal Energy Regulatory Commission (FERC), enabling it to solve the cold weather problem much faster and more effectively than the federal bureaucracy under FERC. Therefore, Texas can – and should – take the same actions to protect against the looming threat from solar weather. Other states can, and must, explore how to do the same.

Conclusion

"Bottom up" action to protect our electric infrastructure from solar weather will only happen if a few conditions are met:

• First, there must be sufficient awareness about the gravity of the threat. Fortunately, the award-winning documentary "Grid Down, Power Up" narrated by celebrity Dennis Quaid can provide that awareness to the public at large.

• Second, there must be an acknowledgement of the presently insufficient solar storm protection standard established by the U.S. FERC. Fortunately, the facts have been well-documented and made available to the public through official testimony to the U.S. Secretary of Energy. State and local regulators need only to verify these facts to begin taking action.

"SolidGround" NBD protecting a 500 kV transformer in the TVA grid. This transformer would cost upwards of $20 million, and years to replace if it were destroyed by ground induced currents from solar weather. The "SolidGround" unit protecting this transformer costs approximately $500k, or 2.5% of the value of the total asset.

• Third, because critical infrastructure owners and operators often pay much more for electricity than the common citizen, it will be imperative for them to understand and support the effort to require utilities to upgrade their systems with NBDs to mitigate solar weather. Utilities will undoubtedly pass on their costs to these customers through increases in the rate base.

Ultimately, critical infrastructure operators can provide greater resilience for the communities they serve by exploring methods of generating needed power on-site or locally through all-hazards resilient microgrids and reducing dependency on the outside electric grid. The U.S. Department of Homeland Security's "Resilient Power Working Group" has even published a best practices document that helps operators explore these options. This process, though, will take a long time.

Therefore, we need to protect the grid we have before it's too late.

IACIPP ANNOUNCES LAUNCH OF 'CIP WEEK' IN EUROPE

12th-14th November 2024, Madrid, Spain

The International Association of Critical Infrastructure Protection Professionals (IACIPP) has announced the launch of 'Critical Infrastructure Protection Week' in Europe as part of an initiative focused towards enhancing collaboration and cooperation amongst the industry.

With the imminent implementation of The Critical Entities Resilience Directive (CER Directive), which lays down obligations on EU Member States to take specific measures to ensure that essential services and infrastructures, for the maintenance of vital societal functions or economic activities, are provided in an unobstructed manner in the internal market. The deadline of 17th October 2024 is set for when Member States shall adopt and publish the measures necessary to comply with this Directive.

The NIS2 Directive, also known as the Network and Information Security Directive, is also a significant piece of legislation being implemented by 17th October 2024, aimed at improving cyber security and protecting critical infrastructure across the European Union (EU).

It builds upon the previous NIS Directive, addressing its shortcomings and expanding its scope to enhance security requirements, reporting obligations, and crisis management capabilities.

Compliance with the CER Directive and NIS2 Directive are crucial for businesses operating in the EU to safeguard their systems, mitigate threats, and ensure resilience. Penalties are enforceable on agencies and operators for non-compliance.

In light of the forthcoming challenges with the Directives, and the ever increasing threats against European critical infrastructures, IACIPP is launching 'CIP Week' in Europe to help raise awareness and promote greater collaboration amongst operators, agencies and the CI security community.

The first 'Critical Infrastructure Protection Week' will take place in Madrid Spain and will see IACIPP host the 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'EU-CIP Horizon Project' conference as the first events as part of the initiative.

John Donlon QPM, Chairman of The International Association of Critical Infrastructure Protection Professionals, said, "IACIPP is delighted to be announcing this new initiative in Europe, with the important aim of encouraging greater information sharing, collaboration and co-operation within the industry."

"The CER and NIS2 Directives are two of the most important pieces of legislation to arrive in Europe in recent years, and IACIPP along with other professional bodies have a degree of concern over the lack of preparation of some of the operators and agencies for the October deadline, and believe more needs to be done to ensure these minimum standards are met, and indeed exceeded in subsequent years."

"We are delighted the 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'EU-CIP Horizon Europe Project' conference are the first two events to contribute towards CIP Week, which we aim to be an annual event. Madrid is an excellent location for the launch of this program, with the CN-PIC driving Spain's efforts to meet the Directives' deadlines and be prepared." Added Mr Donlon.

Critical Infrastructure Protection & Resilience Europe (CIPRE) is the premier conference in Europe to discuss the operational threats and challenges, delivering though leadership and strategies for operators and agencies to plan security and resilience to their operations and assets.

The EU-CIP Horizon Europe Project* is set up to establish a novel pan European knowledge network for Resilient Infrastructures, which will enable policy makers to shape and produce data-driven evidence-based policies, while boosting the innovation capacity of Critical Infrastructures (CI) operators, authorities, and innovators (including SMEs).

Emilia Gugliandolo, Project Coordinator of EU-CIP, said, "The EU-CIP Project is delighted to be invited as part of the CIP Week initiative, enabling greater opportunities for the industry to explore the challenges and opportunities for bringing about synergetic, emerging disruptive solutions to security issues via cross-projects collaboration and innovation. We look forward to successful collaborations between the sectors and professionals in achieving the overall goals for the industry."

IACIPP is an international association of practitioners and professionals involved in the security, resilience and safety of critical infrastructure, both physical and information infrastructure, open to critical infrastructure operators and government agencies, including site managers, security officers, government agency officials, policy makers, research & academia. The Association also aims to share ideas, information, experiences, technology and best practise to enhance these objectives.

IACIPP is inviting the industry to join in CIP Week in Madrid on 12th-14th November 2024.

Further details available at www.cip-association.org, www.cipre-expo.com and www.eucip.eu.

Connecting Unrelated Industries Strengthens All Sectors

By Benjamin Dierker, executive director of the Alliance for Innovation and Infrastructure, the only nationwide public policy think tank dedicated to infrastructure in the United States

There are multiple sectors of critical infrastructure, which are often siloed and viewed as individual elements or discussed only one at a time. To move toward a more resilient framework, policymakers and industry professionals should be looking for cross-sector collaborations and partnerships that will strengthen aspects of their own work. This type of cooperation not only unleashes the potential to learn from others and see one's own sector differently, but it can open previously unseen opportunities.

Benjamin Dierker, Executive Director, Alliance for Innovation and Infrastructure

In a similar sense to which policymakers seek to avoid cascading effects, where a single point of failure in one sector leads to negative consequences in multiple other dependent sectors, we can identify and leverage a positive variant. Acting almost as an inverse of the cascading

effect, leveraging a sector and its processes to bolster others can push benefits not to dependent sectors but to even seemingly unrelated ones. However, this requires collaboration. Unlike a cascade, which will occur by its own inertia, the positive case offers resources which other parties must integrate to realize their benefits.

With the inverted model in mind, it calls for the use of something previously considered harmful. Carbon is a disfavored byproduct of industrial processes, particularly in the form of carbon dioxide, making it a negative production externality. This can be directly converted into a positive production externality when the carbon is easy, safe, and low-cost to capture, collect, handle, transport, and employ for other uses.

Carbon, then, serves as a common link where multiple relevant sectors align. Not only do many critical infrastructure components rely on carbon-intensive power and energy security, but many are dependent on strong and resilient construction materials like concrete and asphalt.

In particular, there is a natural link between the energy and transportation sectors that not only leverages existing critical infrastructure but produces inherent resilience outcomes for both sides and third parties. More than this, it has potential for environmental benefits and economic bolstering. It is the interplay between natural gas, pipelines, and roadways. It is not difficult to see why these are not naturally associated sectors: what do natural gas and roads have

to do with one another? But the pairing brings out something fascinating.

Through the decarbonizing of natural gas, energy users can produce their own hydrogen on site with a solid carbon byproduct rather than carbon dioxide emissions. This distributed hydrogen production method utilizes existing natural gas pipelines and is less capital intensive than more popular forms of centralized hydrogen production. This model also reduces strain and stress on other sectors, offering another indirect benefit.

The process begins with natural gas. This abundant and low-cost energy resource already provides the lion's share of electricity and industrial process heat in the United States and in many places around the world. The versatility and usefulness of natural gas makes it an ideal energy resource for providing robust power and energy security. Millions of miles of pipelines direct this resource into facilities around the country.

Policymakers and environmentally-focused industry leaders recognize that burning natural gas leads to carbon dioxide emissions. The long-term resilience of the energy sector is at least partially dependent on environmental and climatic factors. Those seeking to decarbonize their power load have searched for alternatives ranging from carbon capture technology to carbon offsets to alternative power sources and electrification. These all range in efficiency and efficacy, but also require different levels of capital intensity and investment requirements.

Given the extensive network of critical infrastructure already in place – namely pipelines – the most efficient solution would be to leverage it. By extracting the most value from existing pipelines, industry leaders and policymakers can avoid unnecessary and costly build outs of new infrastructure. The innovative multi-sector process to achieve sustainable long-term critical infrastructure protection and resilience keeps natural gas as central to its equation, but pairs it with a move toward hydrogen.

Innovators have honed a process for decarbonizing natural gas to produce hydrogen that skips

the byproduct of carbon dioxide emissions. It is important that that process not fall into the trap of requiring new infrastructure, which would ultimately lead to delays, grid strain, and high expenses. Leveraging the pipeline network means utilizing a distributed production method rather than centralized. While extensive benefits can be derived from a centralized green hydrogen production process that employs electrolysis and similarly avoids carbon dioxide emissions, this requires new facilities, adds significant new demand for electricity from clean sources, which in turn requires new renewable generation deployments and accompanying transmission infrastructure. Once all this is in place, the hydrogen must be compressed and stored or transported through trucks or pipelines yet to be constructed or retrofitted.

Every step in that process depends on decades-long permitting and regulatory compliance, construction timelines, and interdependencies of their own. By contrast, the distributed model creates hydrogen at the end stage of the existing infrastructure and avoids these build outs, regulatory compliance, and associated costs and delays. These all serve as indirect benefits to the power sector – helping reduce strain to keep it resilient – and the pipeline sector – doubling down on the criticality of natural gas pipelines to ensure they are protected and operational to serve existing and new clients.

The process takes shape when the natural gas enters the facility through existing distribution lines. Once behind the meter, the gas moves through equipment that uses thermal methane pyrolysis. This is a superheating method that decomposes the methane molecule into its constituent parts of hydrogen and carbon. An initial heat reaction can be generated by burning the natural gas, then sustained by its own clean-burning hydrogen. The output is clean hydrogen gas and solid carbon powder with no other emissions.

Fully decarbonizing natural gas in a pre-combustion carbon capture technique means that only clean hydrogen (or the appropriate blend) is sent into the facility's combustion chambers, be they boilers, forges, or other generators. This means no need for investment in scrubbers or an expensive carbon capture apparatus. It also means capturing all of the carbon, making it highly efficient and effective, whereas other carbon capture processes use may more energy and capture less carbon, which is usually in the form of carbon dioxide and requires compression, storage, and transportation solutions of its own.

The hydrogen produced does not require storage tanks, because it is generated on site and on demand. The clean potential hydrogen can be stored in the form of natural gas and decarbonized at point of use. This once more leverages existing facilities.

The magic of the model comes from the carbon byproduct. As a solid powder, it is not lost to the atmosphere or diffuse and difficult to capture and store. The powder can be collected, safely handled, and sequestered or stored easily.

That ease of use also gives this form of carbon a natural advantage in use as a valuable input in other sectors. Policymakers often require or encourage carbon to be buried underground to remove it from the carbon balance sheet that ultimately influences the climate. But utilizing the carbon as a product can help improve the resilience of other sectors.

Sequestering carbon into our built environment completes the loop on a new potential circular economy related to carbon. Carbon black can be incorporated into asphalt and used to patch, repair, and resurface potholes and whole roadways and other surface applications.

Identifying partnerships where power generators and roadbuilders are in close communication may be few and far between. But this model demonstrates how the power sector can shed its emissions to reduce its carbon intensity and improve its own resilience, while providing a building material and strengthening agent to construction sectors and road builders.

Through this cross-sectoral model, economy-wide resilience can be strengthened by removing carbon. It reduces strain on the power grid while not threatening and even boosting energy security by continued use of natural gas. This decarbonized natural gas is fully carbon neutral.

Tying in still other sectors can turn this process fully carbon negative. For instance, by incorporating waste facilities and the agricultural sector, industry leaders can capture methane from landfills, wastewater sites, farms, and more and process these into renewable natural gas – a form of carbon neutral biogas with the same chemical signature as geologic natural gas for use in the same pipeline networks. With this type of carbon-neutral and renewable form of natural gas, the use of thermal methane pyrolysis removes carbon that was previously in the atmosphere and turns the entire balance sheet negative.

Further collaborations and partnerships can be imagined that pair into this type of model, because other sources of methane can be identified, other power sectors or gas users may enter the market, and innovators can

generate new applications for carbon black.

This is not to say it is the only model capable of such dynamic cross-sector collaboration. By contrast, it serves to underscore just such potential. If natural gas and potholes can find common cause, surely other sectors and their various solution challenges can find innovative partnerships and collaborations.

The process discussed here demonstrates an inverted cascading model, where one sector turns a problem into a resource that another sector can pick up and employ. By starting with one process and its byproduct, policymakers can follow it through to ensure laws and regulations not only allow but encourage these types of partnerships. Industry leaders can explore their own assets and liabilities, listen for the challenges and solutions in other sectors, and move toward piloting new processes.

Carbon is a national and global focal point. By decarbonizing natural gas, innovators can use technology to take the main negative out of a critical energy resource and turn it into a positive for other industries. But the process for doing so is where most of the benefits accrue. By leveraging existing critical infrastructure, a distributed hydrogen production model prevents the unnecessary building of new or specialized hydrogen pipelines to move the gas from centralized production sites. It also avoids adding strain to power demand or adding to the waitlist for new transmission infrastructure needed to connect wind and solar projects to the grid.

This enables a robust power sector, reduced emissions, leveraging critical pipeline sectors, and improving the resilience of roadways. Policymakers and industry actors must look for these types of innovative collaborations to move toward circular economies and resilience for the demand of the future.

Can nuclear physics and AI forecast earthquakes?

Novel, underwater detectors are being installed to monitor radon spikes in earthquake-prone locations across Europe. Checking the data against seismic activities could provide clues for predicting earthquakes.

An EU-funded project is taking a new approach to investigate the link between surface radon concentration and seismic activity.

Naturally present in all outdoor air at very low levels, radon gas is emitted from uranium, which is found in minute quantities in most rocks. Along fault zones, the tectonic movements result in increasing tension that in turn creates cracks in the underlying rock material.

An increasing number of cracks will increase radon emission from layers under stress. Participating scientists will observe changes in radon-concentration at the surface that reflect the changes in tension at deeper layers. These stem from small movements along fracture zones, as it can happen before an earthquake, and the changes in the geological and hydrological structure.

There are more than 600 studies from around the world on changes in various environmental parameters preceding earthquakes, often showing contradicting results. All the studies were, however, performed in different (non-standardised) ways using different type of detectors and measuring in different media.

In the Awareness and resilience through European multi-sensor system (ArtEmis) project, the measurements are performed in the same way in all selected monitoring sites.

ArtEmis is coordinated by Sweden's KTH Royal Institute of Technology and gathers 15 partners, mostly research organisations, but also representatives of the communities affected. The objective is to measure radon concentration in ground water in selected locations, corelate the data with seismic activity by using machine learning (ML), and build AI tools to improve forecast and earthquakes prediction.

JRC contributes with advice on the graphical display of data based on experience from the work on EUropean Radiological Data Exchange Platform (EURDEP). Furthermore, JRC measures the components to be used in the sensors for radioactive components. In particular, the Ra-226 (Radium 226 isotope) activity of electronic components is essential to know as it is the parent of Rn-222 (Radon 222 isotope).

The partners have designed and produced novel, in-water radon detectors equipped with additional sensors. Six detectors have been deployed in fault zones in earthquake prone areas in Italy's region of Abruzzo, the Ionian islands in Greece and Swiss Alps. Additional 30 are being developed to be installed by the end of 2024 in the same countries.

New funding approved to strengthen Multi-Hazard Early Warning Systems in the Caribbean

In a significant step for Chile and its commitment to disaster risk reduction (DRR), representatives from various sectors discussed the implementation of an action plan based on the recommendations of the application of the Global Methodology for Infrastructure Resilience, developed by the United Nations Office for Disaster Risk Reduction (UNDRR) and the Coalition for Disaster Resilient Infrastructure (CDRI).

Under the leadership of the National Service for Disaster Prevention and Response (SENAPRED) of Chile, and with the support of the UN Office in Chile, a high-level roundtable was organised during the VII Forum of the Countries of Latin America and the Caribbean on Sustainable Development, with the participation of various entities such as the Ministries of Public Construction, Housing and Urban Development, Energy, Transport and Telecommunications, Health, Education, Social Development and Environment. The methodology outlines a series of critical initiatives to improve DRR in Chile and strengthen the country's resilience to various hazards. Government leaders, international development banks, international agencies and private sector representatives came together to explore courses of action based on the results presented.

The High Level Roundtable explored mechanisms to strengthen infrastructure governance at national, regional and local levels, and shared their views on the plans, identifying key areas that require immediate attention and coordination among disaster management stakeholders.

In addition, key capacity building initiatives related to risk reduction and resilient infrastructure management were discussed. Recognising the importance of education and training in building a culture of preparedness and response, participants discussed ways to strengthen the capacities needed to meet current and future challenges.

In preparation for this roundtable, SENAPRED held a final validation workshop for the project "Improving Infrastructure Resilience by Strengthening Governance in Chile", which played a key role in the development of an implementation plan aimed at overcoming the gaps identified in the national scenario.

The project first mapped key actors, identifying cross-cutting and sectoral institutions, as well as relevant institutions and actors. This was followed by a review of existing policies and regulations, both cross-sectoral and sectoral. The next step was to identify vulnerabilities through data collection and stress testing analysis. Finally, an implementation plan with short-, medium- and long-term recommendations was developed, involving the participation of all key sectors for infrastructure management, and validated by both the workshop and the High-Level Roundtable.

"Infrastructure resilience is the backbone of sustainable prosperity in our region. It is necessary to work on setting clear priorities to strengthen the governance of this resilience at different levels and in different sectors, in order to prepare our communities to face the challenges of the future," said Nahuel Arenas Garcia, chief of UNDRR - Regional Office for the Americas and the Caribbean. "This high-level roundtable not only reflects our commitment to disaster resilience, but also to the implementation of the 2030 Agenda, ensuring that our actions are aligned with sustainable development priorities for the well-being of communities now and in the future," he added.

In Chile, estimated annual infrastructure losses are approximately US$5.4 billion due to disasters.

Why Airspace Awareness Matters for Critical Infrastructure Security

By Andrew Singer, SVP, Product & Customer Operations, SkySafe

With increased speed and manoeuvrability, unmanned aerial systems (UAS) can efficiently reach areas previously inaccessible to human operators. Unauthorized drone flights have already shut down international airports, infused contraband into prisons, damaged oil fields, and threatened military units and civilians across the globe.

Experts predict that over 10 million consumer drones will be shipped in the U.S. by 2030. Before the threat grows too large to handle, critical infrastructure security leaders should equip themselves with comprehensive airspace awareness to detect, track, and identify rogue UAS in their airspace.

The Imperative of Airspace Awareness

For this article, airspace awareness refers to a comprehensive understanding of all activities in a specific location's airspace. Drones, especially smaller ones, can easily bypass walls, fences, and traditional radar systems. Even small gaps in airspace awareness can lead to severe consequences.

Undetected and untracked, a malicious drone is free to attempt anything from espionage and theft to security breaches, disruptions,

and sabotage. Failure to detect and respond to this unauthorized activity can result in legal and financial repercussions, particularly when it risks property or human safety.

U.S. security leaders have already seen this happen across multiple states. The most infamous recent incident is the drone that crashed near a Pennsylvania power substation, trailing copper wires that could have short-circuited high-voltage equipment on contact. In 2019, a swarm of drones was sighted twice around Palo Verde Nuclear Generating Station in Arizona, the country's largest power plant by net generation. Consumer drones have also breached White House airspace at least twice, though fortunately none were harmed. The list goes on: drones have crashed or been flown over ports in Texas, oil storage facilities in Oklahoma, chemical facilities in Louisiana, New Jersey, and New Orleans, and nuclear labs in New Mexico and California.

Complete airspace awareness encompasses knowing what aircraft and UAS are present, their types, their current and projected flight paths, operator locations, and their intentions. This information enables security personnel to identify potential threats and take appropriate action before the damage is done.

A Darker Evolution

Modern drones have seen significant advancements in technology, capabilities, and features over recent years. They can fly faster and further, move in coordinated swarms, and send high-quality real-time transmissions. Advanced models can also avoid obstacles or even self-destruct.

This matter has not gone unnoticed by government agencies and security experts. In January 2024, the FBI warned that Chinese-made drones could pose a threat due to their ability to transmit sensitive data back to their manufacturers. When DJI recently released an "Update Module" for their discontinued Aeroscope system, analysis by SkySafe experts revealed that the upgrades had given DJI and the Chinese government the ability to cloak drones from detection.

As drone technology continues to evolve faster than the regulations that oversee it, security operators are left with the unenviable task of adapting to emerging threats without clear guidance.

Standards and Compliance Challenges

Airspace security is currently governed by a complex mix of regulations and standards that vary by country or state.

In the U.S., the Federal Aviation Administration (FAA) Reauthorization Act and Preventing Emerging Threats Act give the Department of Homeland Security (DHS) and Department of Justice (DOJ) the authority to counter and mitigate drone threats to covered facilities, including critical infrastructure.

Globally, the International Civil Aviation Organization (ICAO), ASTM International, and the ISO/TC 20/SC 16 subcommittee have introduced worldwide standards and recommended practices for UAS, covering operational rules and limitations and compliance requirements for safe integration into airspace systems.

While stronger regulations help to deter unauthorized airspace access, many security teams face difficulties with compliance and enforcement. Common obstacles include limited resources, personnel constraints, unclear divisions of responsibility between infrastructure management and local law enforcement, and rising costs for effective airspace awareness measures.

Organizations can stay abreast of the opportunities and security risks afforded by drones in the following ways:

- Frequent and thorough risk assessments of current drone use

- Developing and implementing drone use policies

- Investing in C-UAS technology and training to detect, identify, and mitigate potential threats

- Working closely with law enforcement and cybersecurity agencies to stay updated on best practices

Beyond Detection: Intelligent Airspace Awareness

While drone detection technology is a promising first step toward airspace awareness, it's only one step. A drone cannot be arrested or prosecuted, and traditional response methods like capturing or jamming a rogue UAS may not always be feasible. Even if one drone is removed from your airspace, a sufficiently motivated and prepared operator could have a replacement airborne that same week, day, or hour. These operators must be targeted to ground drone threats at the source.

Drone intelligence technology combines real-time detection, identification, and tracking capabilities to gauge the intent of rogue drones. These three mechanisms enable comprehensive airspace security by providing the necessary data to alert key figures early and effectively respond to potential threats. Depending on the situation, this can involve alerting the relevant authorities, activating the appropriate countermeasures, or even deploying interceptor drones.

When adopted wisely, drone intelligence technology helps predict future threats, protect critical facilities with drone tracking and analysis, and prosecute or investigate unauthorized drone operators.

Conclusion

With newer drones' advanced surveying capabilities and ability to capture high-resolution imagery, unauthorized drone incursions bear a serious potential for danger and sabotage.

As consumer drones continue to grow exponentially in popularity, critical infrastructure security must stay ahead of their numbers and evolving technology. Security leaders should invest in future-proof, comprehensive airspace awareness technology and stay informed of industry standards and regulations.

Security leaders should further empower their teams to prevent or react to threats with drone intelligence technology by building standard operating procedures for drone incursions today. This will allow them to analyze potential threats and effectively protect critical infrastructure with constant airspace awareness.

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 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 open to qualifying individuals - see www.cip-association.org for more details.

Our 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

Critical Infrastructure Protection & Resilience North America (CIPRNA) took place on 12th-14th March in Prague, Lake Charles, Louisiana, co-hosted by the International Association of CIP Professionals (IACIPP).

We take a look at the success of the conference and exhibiton and some of its highlights reported by John Donlon, Chairman of CIPRNA.

Ladies & Gentlemen, before we all head off home or back to the casino to win back any money we may have lost, I just wanted to close the conference with a few comments.

Events such as these provide a fantastic opportunity to network with like minded friends and colleagues and I always go away having learned something new and worthwhile and I do hope you have all found the last few days to have been, educational, enjoyable and of real value.

We have had some insightful presentations by some very distinguished and experienced professionals and some great discussions across a whole range of issues which are affecting the international infrastructure and information communities.

We are very grateful to all the people and the organisations who have supported us and shared their knowledge, expertise and enthusiasm with us. We are also grateful to our exhibitors and sponsors without whom it would be almost impossible to deliver this conference.

We had a great start on day one with the keynote session with senior representatives from:

- The Office of Congressman Clay Higgins
- The Cybersecurity & Infrastructure Security Agency (CISA)
- The Governors Office of Homeland Security & Emergency Preparedness (GOSEP) – and –
- Nic Hunter – the Mayor of Lake Charles

Jonathan F 'Tyrone' Glover represented the Congressman, Dr Ryan Donaghy, CISA and Euclid Talley, GOSEP. Tyrone, Euclid and The Mayor, Nic Hunter, all spoke passionately about the efforts that are being made across the State of Louisiana to build resilience, in particular against adverse weather events.

They all made references to the need to lobby hard to leverage national funding streams and The Mayor proudly announced that by the end of 2024 Lake Charles is on target to be the most resilient city in Louisiana. That is quite a significant achievement when you consider the

issues the City and the State have had to deal with over the last few years.

The Mayor was keen to point out that there were 10 Federally declared natural disasters in the last 20 years which had a severe impact on Lake Charles and 5 of those were within his first year in Office.

Dr Ryan Donaghy from CISA clearly outlined the current challenges that both they and the country are facing and referenced this period of time as a, 'Dynamic Decade'. One which is typified by 'Democracies verses Autocracies'. She was keen to point out that terrorism, both international and domestic was very high on CISA's agenda and she provided facts and figures to evidence those concerns.

Dr. Donaghy also made the point that Government Departments within the United States were extremely keen to support conferences such as CIPRNA, as they believe them to be instrumental to securing our nations today, as we all face shared transnational challenges that affect our missions.

The conference obviously heard a great deal about the current and emerging threats that our critical infrastructure and information sectors are facing. Geopolitical and technological shifts are posing as big a threat as we have ever seen and we cannot hide away from the challenges before us. The challenges discussed included:

- Insider Threats
- Hostile use of Drones
- Industrial Control System Attacks
- Cyber Attacks
- Artificial Intelligence (AI) Deception and
- Lone Wolf Attacks

The threats that we all face are many and varied. We used to live in what has been commonly referenced as a VUCA world, one that is full of:

- Volatility
- Uncertainty
- Complexity and
- Ambiguity

However, this week we were informed that we have moved on, we are now in a TUNA world, one which is:

- Turbulent
- Uncertain
- Novel and
- Ambiguous

Not a great deal of difference between the two but whichever set of acronyms (and we will come back to acronyms) you prefer it is fairly clear that a lot of what may be ahead of us is unclear. We are facing multiple threats and hazards that are unpredictable, that are new to us and may have consequences that are broader and deeper than we might imagine.

When discussing both current and emerging issues, by far the most referenced subject raised during the conference, by a number of speakers, was around cyber security. We heard a great deal about State Actor activity, in particular the concerns around China, Russia, Iran and North Korea. Also, alongside cyber we had numerous discussions on the subject of climate change and adverse weather events.

Climate change continues to be a major concern and it continues to have a considerable impact on our infrastructure. February this year, was the hottest ever on record, as was the previous nine months before that. The temperatures during 2023 caused devastation through floods, droughts and heatwaves and we were told that there have been 350 weather related events during that time which have resulted in costs of over $1 billion dollars. Last year alone the United States saw twenty-five such events with over a billion-dollar costs attached to each of them.

Outside of cyber and climate activity we have covered a whole range of infrastructure and information related topics, including:

- Technology
- The potential benefits and disbenefits of Artificial Intelligence
- Communications
- Supply Chains
- Power
- Energy
- Pipelines
- Transport
- Insider Threats
- Resilience Planning, and many more.

The age-old subject of Public Private Partnerships (PPPs) came up on a number of occasions with trust, collaboration, cooperation and communication being the go-to words.

Once again, as with most years, I am always astounded at the imagination that goes into creating new acronyms around specific programmes or projects. I thought that the United Kingdom was top of the tree for the production and use of such acronyms but I think both individuals and

organisations in the United States give us a good run for our money. I have heard dozens of new ones here in Lake Charles, such as:

- NASSAEEP
- AGGEX
- DCIP
- DDIP and
- CCHAMP

However, the best one by far was, SBOM – which I am told relates to the 'Software Bomb of Materials'.

The best one liner of the week was given by a representative from CISA when talking about people with drones, stating they almost always fall into two categories, 'Careless and Clueless'.

The best fact of the conference was referenced in relation to the use of underwater detection systems when we learned that the speed of sound, in freshwater, is 1.4 meters a second, however I still don't know what it is in sea water!

Finally, the best quote of the week was delivered on day one by a keynote speaker who had taken a Benjamin Franklin quote - 'Lost time is never found' and changed the order of the first two words so that we saw 'Time lost is never found' and then claimed it to be his own original quote, very clever indeed.

CIPRNA 2024 in Lake Charles was a huge success and a lot of that success was due to the tremendous support we had from Lester Millet, the President of InfraGard, Louisiana and of course all our great speakers, the sponsors and exhibitors and the delegates for their active participation over the course of the conference.

Our next event is our European Conference, Critical Infrastructure Protection and Resilience Europe (CIPRE) which will take place in Madrid in November this year. Then in March next year we will be back in the United States, in Houston, for CIPRNA.

I hope we see you at one of these events, or even both of them.

John Donlon QPM FSyI
CIPRNA Chairman
Chairman - International Association of CIP Professionals

Urgent Warning from Multiple Cybersecurity Organizations on Current Threat to OT Systems

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE), United States Department of Agriculture (USDA), Food and Drug Administration (FDA), Multi-State Information Sharing and Analysis Center (MS-ISAC), Canadian Centre for Cyber Security (CCCS), and United Kingdom's National Cyber Security Centre (NCSC-UK)—hereafter referred to as "the authoring organizations"—are disseminating this fact sheet to highlight and safeguard against the continued malicious cyber activity conducted by pro-Russia hacktivists against operational technology (OT) devices in North America and Europe.

The authoring organizations are aware of pro-Russia hacktivists targeting and compromising small-scale OT systems in North American and European Water and Wastewater Systems (WWS), Dams, Energy, and Food and Agriculture Sectors. These hacktivists seek to compromise modular, internet-exposed industrial control systems (ICS) through their software components, such as human machine interfaces (HMIs), by exploiting virtual network computing (VNC) remote access software and default passwords.

The authoring organizations are releasing this fact sheet to share information and mitigations associated with this malicious activity, which has been observed since 2022 and as recently as April 2024. The authoring organizations encourage OT operators in critical infrastructure sectors—including WWS, Dams, Energy, and Food and Agriculture—to apply the recommendations listed in the Mitigations section of this fact sheet to defend against this activity.

Overview of Threat Actor Activity

Pro-Russia hacktivist activity against these sectors appears mostly limited to unsophisticated techniques that manipulate ICS equipment to create nuisance effects. However, investigations have identified that these actors are capable of techniques that pose physical threats against insecure and misconfigured OT environments. Pro-Russia hacktivists have been observed gaining remote access via a combination of exploiting publicly exposed internet-facing connections and outdated VNC software, as well as using the HMIs' factory default passwords and weak passwords without multifactor authentication.

Historically, these hacktivists have been known to exaggerate their capabilities and impacts to targets. Since 2022, they have claimed on social media to have conducted cyber operations—such as distributed denial of service, data leaks, and data wiping—against a variety of North American and international organizations. Based on victim incident reporting, this activity has caused limited disruption to operations.

2024 Year-to-Date Activity

In early 2024, the authoring organizations observed pro-Russia hacktivists targeting vulnerable industrial control systems in North America and Europe. CISA and the FBI have responded to several U.S.-based WWS victims who experienced limited physical disruptions from an unauthorized user remotely manipulating HMIs. Specifically, pro-Russia hacktivists manipulated HMIs, causing water pumps and blower equipment to exceed their normal operating parameters. In each case, the hacktivists maxed out set points, altered other settings, turned off alarm mechanisms, and changed administrative passwords to lock out the WWS operators. Some victims experienced minor

tank overflow events; however, most victims reverted to manual controls in the immediate aftermath and quickly restored operations.

The authoring organizations have observed pro-Russia hacktivists using a variety of techniques to gain remote access to HMIs and make changes to the underlying OT.

MITIGATIONS

The authoring organizations recommend critical infrastructure organizations implement the following mitigations to defend against this activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures.

Although critical infrastructure organizations can take steps to mitigate risks, it is ultimately the responsibility of the OT device manufacturer to build products that are secure by design and default. The authoring organizations urge device manufacturers to take ownership of the security outcomes of their customers in line with the joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software and CISA's Secure by Design and Default.

Foreign Investment in the U.S.: Efforts to Mitigate National Security Risks Can Be Strengthened

Foreign investment in U.S. companies benefits the economy but can also pose national security risks—such as by giving foreign investors access to sensitive data. The Committee on Foreign Investment in the U.S. reviews these investments and enters into agreements with companies to address risks. Over the last decade, the number of agreements has quadrupled and the work of monitoring and enforcing compliance has grown. But the agencies on the committee don't regularly coordinate their staffing needs. Also, it's unclear how they make enforcement decisions.

The U.S. is historically the world's largest recipient of foreign investment. This benefits the U.S. economy but can also present national security risks. The Committee on Foreign Investment in the United States (CFIUS) is an interagency committee authorized to review certain transactions involving foreign investment in the U.S. to identify risks to national security. To mitigate such risks, CFIUS has authority to enter into legal agreements with the companies involved and to monitor compliance with the agreements. Treasury serves as the committee's chair.

GAO was asked to review issues related to CFIUS mitigation agreements. This report (1) describes trends in mitigation agreements from 2000 through 2022, (2) evaluates selected CFIUS member agencies' approaches to monitoring and enforcing compliance with mitigation agreements and reviewing them for continued relevance, and (3) assesses the selected agencies' staffing for monitoring and enforcement. GAO selected five member agencies on the basis of the number of mitigation agreements each agency manages. GAO reviewed laws, regulations, and agency guidance. GAO also conducted a nongeneralizable review of mitigation agreements and interviewed agency officials.

CFIUS enters into agreements that require companies to mitigate national security risks stemming from foreign investment. Selected CFIUS member agencies monitor compliance with mitigation agreements by, among other things, conducting site visits to companies and working with independent auditors and monitors. If a company violates an agreement, CFIUS can take enforcement action, including imposing monetary penalties. The Department of the Treasury, as the committee's chair, issued public guidelines on CFIUS penalties in 2022. But CFIUS does not yet have a documented committee-wide process for deciding on enforcement actions, which has led to challenges in responding to certain violations, according to officials. CFIUS also does not have a documented committee-wide process for reviewing agreements for continued relevance. Documenting such processes would help ensure CFIUS member agencies respond in a timely manner to violations and can focus their resources on mitigation agreements that remain relevant.

Critical Infrastructure Resilience: Are we addressing the real challenges? In the right way?

By A. Jovanovic, Steinbeis European Risk & Resilience Institute, Germany & F. Guyomard, EDF, France

Resilience of critical infrastructures

In about the last two decades, the term resilience has taken the most prominent position among the words used in discussions on "how the infrastructure should prepare for its future challengers". Words like safety, protection, or risk, often used as synonyms, became less "fashionable", and the discussions among politicians, scientists, media and even ordinary people became very much focused on resilience, as the "ability of … to respond and adapt to change" (ISO). This is particularly true for the area of critical infrastructures (the "critical entities" in the EU Critical Entity Resilience CER Directive), where the above trend is amplified by the new types of threats, increased "black-box" character of many processes, increased uncertainty in social, political, technological, and climatic factors, increase in global interdependencies, and increased complexity of the infrastructures as systems. Above all, it has been the case when extreme threats, e.g., those resulting from extreme weather, emerging and disruptive new technologies (e.g., AI), the role of social networks, hyper-connectivity, or topics deep uncertainties.

Stability and transparency vs. agility

In the area of engineering, the above plethora of elements is further complicated by the fact that current resilience management of

infrastructure has been focused on components/assets, stability of processes, allocated/regulated responsibilities and compliance, resulting in inertia and rigidity of decision-making processes – just the opposite of the agility needed for "dealing with unforeseen". This engineering-focused approach is nowadays often challenged by societal and economic, often also political, pressures to focus on services and functions, collective response, adaptation, and "preparing for unknown futures". That is why the ways of designing, building, operating, and maintaining critical infrastructures have to be adapted to this new societal context, becoming more agile.

The "open talk" vs. "newspeak" of resilience

In the above situation, the stakeholders involved in critical infrastructure resilience often face difficulties when openly identifying and labeling in-practice real challenges, e.g., due to the fear that it could trigger suspicion that something related to safety, protection, risk prevention, etc. is not properly done. That in turn, can significantly hamper the capability of critical infrastructures to cope with new threats, especially the extreme ones. Many infrastructure owners will gladly discuss generic topics like "what are the risks of digitalization", but would probably be less willing to embark on the discussion on the possibly increased probability of accidents caused by the employees (e.g., the younger ones) "trusting the screen too much", without understanding the process behind the screen, or caused by the (e.g., the elderly) employees who "did not understand the IT black boxes standing between them and the process". Creating an environment for open talking about the challenges is possible and encouraged, not a buzzword-based "newspeak"- is, therefore, essential for achieving resilience of infrastructures and building the "public language of resilience" in society – which is important, as, e.g., almost 2/3 of all 89 major national risks listed in the 2023 UK National Risk Register are infrastructure-related.

Measuring the resilience of critical infrastructures

A further element of the above common language will be to introduce common measures for characterizing threats and infrastructure resilience against them, primarily by indicators. That would directly lead to the possibility to better identify, measure, compare and rank them. Current efforts of organizations like ISO (e.g., the ISO TS 31050 and the 22300-series), Geneva Association (documents on "new risk landscapes") or UNDRR ("5-point plant for resilience infrastructure") indicate the need to use indicators and measure resilience but do not provide hints on how one, possibly globally accepted measurement system could look like. A similar situation is also in the area of regulation (e.g., the EU CER Directive) or the insurance industry offering a unique possibility to include the resilience of a critical infrastructure as a factor in defining operational and business aspects. That would open a series of new opportunities, such as, e.g., the new resilience-oriented parametric insurance, where measuring resilience can be a game-changer.

Resilience ownership and resilience owners, the value of resilience

Although new demands for critical functions/services/infrastructures appear (e.g., in car-sharing or in the AI-control of demand for services and infrastructures) and the ways how they are demanded and provided, change by the day, the need to provide these services, e.g., energy or water supply, will remain. This makes the infrastructure operation and ensuring resilience even more complex and it has to be supported by the increased capacities of the regulators/governance. These, however, often tend to react slowly, or are poorly equipped to "deal with new and unforeseen challenges". Although other factors, such as market, technologies, demands and other stakeholders (infrastructure owners, competent authorities, general public), will certainly play an important role, the regulators, will certainly maintain a pivotal role in the process. They should) lead the process of establishing a (possibly global!) common language of resilience, common ways to measure it and, finally, proposing common ways to implement the whole concept practically, in a possibly aligned way, as an extension of existing good practices. They should help identify the "resilience owners" (similarly to the "risk owners"), and define the concept of "Value-of-Resilience" (VoR, similarly to the "Value-at-Risk", VaR). That would improve the identification and addressing of new threats, quantifying and ranking them, knowing better the level of resilience needed, and providing a framework for stress-testing resilience. Comparing investment in resilience with new VoR (including protection, absorption, recovery and adaptation capacities), would, thus, incentivize the bottom-up investment in enhancing resilience. This process has to involve all the relevant stakeholders, but must not be politicized, let alone allowed to focus on producing "white elephants" (e.g., in public research) or "emperor's/entities' new clothes" (e.g., by suppressing early warnings are misinterpreted or even banned). Only so, the important new regulations (such as CER, NIS2, AIA, etc.) will "live" and yield the expected improvements.

Break down cyber and physical security silos to improve protection and operations

By Thomasina Martin, Genetec

With digital transformation in full swing, threat actors are finding new ways to exploit weaknesses in critical infrastructure. While information technology (IT) and physical security departments have been on a converging path for years, it's more important than ever for security and IT to work together to safeguard the physical and digital perimeter.

Unifying security solutions is a foundational step in bringing these functions together. They help teams address evolving security needs, simplify compliance, and improve operations.

Unify and automate to reduce cyber-breaches due to human error

Some cybersecurity events, like the ransomware attack on the Colonial Pipeline, are driven by sophisticated strategies. Others, such as recent assaults on drinking water systems, are the result of criminals exploiting human error. They look for cybersecurity missteps like forgetting to change default passwords or not closely managing an access control system.

If access control systems aren't regularly audited, they introduce

vulnerabilities. For example, employees may change roles and retain access to sensitive areas. Or they misplace, lose, or loan out keys and fobs. Without active monitoring, it can take a year or more for organizations to discover a breach and weeks to mitigate risks.

Reduce the likelihood of unauthorized access by updating older access control systems to a unified solution that automates the process of auditing credentials. This also decreases the time it takes to discover and address a security breach.

A unified security platform that links credentials to employee and contractor identification files can automatically adjust access rights to certain areas based on attributes like job function or employment status. It can switch access on or off based on time of day or for a specified length of time, so temporary access rights end when they should.

Unified systems can also more effectively address vulnerabilities due to hardware or software. They can automate the detection and resolution of these issues and generate a dashboard with a cybersecurity scorecard. This helps IT and security teams spot and respond to weaknesses or threats. For example, cameras with out-of-date software or passwords are a weak point. A unified security platform will point out these issues and guide operators to resolve the issue.

A layered approach to perimeter security

In addition to cyber breaches, physical attacks on power grids and substations are also rising. While

critical infrastructure facilities are protected by fences and other barriers, attackers have discovered ways to damage infrastructure without crossing the perimeter.

A layered approach to physical security is key. Fences, cameras, sensors, environmental design, and other tactics play a role. A thoughtfully designed unified security solution brings these systems together so they can be managed from one interface. Thus, teams are empowered to spot trouble quickly and respond effectively.

This may include defining what steps to take if important systems fail or perimeters are breached. Digitized standard operating procedures (SOPs) within the system can guide operators on step-by-step instructions to respond to the incident without delay.

Simplify compliance through a unified system

The information collected by a unified security system can help organizations improve operations and ensure compliance, as well. One of the main physical security requirements of the North American Electric Reliability Corporation (NERC) is that Energy & Utilities organizations must record all access control activities, maintain logs for authorized access, and monitor critical facilities for unauthorized access 24/7.

In the event of an access breach, NERC requires organizations to investigate and categorize the alarm incident and implement the appropriate response plan within 15 minutes. Verification of the alarm details and the response must be documented and are subject to an audit and review.

A unified security system that optimizes evidence reporting and digitizes SOPs can help organizations comply. Being able to securely collect, manage, and share digital evidence from multiple sites makes it easier to meet different audit requirements. Likewise, digitized SOPs guide personnel in their response to events to

maintain compliance across a distributed organization.

Facilitate collaboration between IT and physical security teams

Critical infrastructure organizations are taking different approaches to help teams collaborate to protect against physical and cyberattacks. For some, IT teams are bringing physical security into their group. In others, physical security leaders are expanding their departments with IT skills. And some are broadening the security operations (SecOps) function to address security risks and capitalize on data coming from both groups.

An open, unified physical security platform supports all convergence strategies. Data flows into an intuitive platform, providing a shared view for consistent decision-making across all teams dedicated to keeping infrastructure secure.

Thomasina Martin is Vertical Key Account Manager – Utilities at Genetec. Working in the private utilities sector, she helped spearhead the design and execution of security hardening projects for electrical substations and critical infrastructure in compliance with NERC/CIP regulations.

Urgent Warning from Multiple Cybersecurity Organizations on Current Threat to OT Systems

Pro-Russia hacktivists are conducting malicious cyber activity against operational technology (OT) devices and critical infrastructure organizations are encouraged to implement mitigations, according to a Fact Sheet released today by the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Environmental Protection Agency (EPA), Department of Energy (DOE), United States Department of Agriculture (USDA), Multi-State Information Sharing and Analysis Center (MS-ISAC), the U.K. National Cyber Security Centre, and the Canadian Centre for Cyber Security.

According to the report, "Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity," the hacktivists are compromising small-scale OT systems in North American and European Water and Wastewater Systems (WWS), dams, energy, and food and agriculture sectors.

Since 2022, the authoring organizations observed malicious activity and are releasing this joint guidance to share information and mitigations associated with the pro-Russia hacktivists' recent cyber operations against OT.

"This year we have observed pro-Russia hacktivists expand their targeting to include vulnerable North American and European industrial control systems," said Dave Luber, NSA's Director of Cybersecurity. "NSA highly recommends critical infrastructure organizations' OT administrators implement the mitigations outlined in this report, especially changing any default passwords, to improve their cybersecurity posture and reduce their system's vulnerability to this type of targeting."

The recommendations in this report include hardening human machine interfaces, limiting exposure of OT systems to the internet, using strong and unique passwords, and implementing multifactor authentication for all access to the OT network. These recommendations are helpful to counter any actors using these techniques.

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.

Invitation to Participate

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

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

The 7th Critical Infrastructure Protection and Resilience North America will bring together the CI community, leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing America's critical infrastructure.

As we come out or one of the most challenging times in recent history, off the back of a pandemic, it has stressed how important collaboration in protection of critical infrastructure is for a country's national security.

Join us in Houston, Texas, USA for the premier event for operators and government establishments tasked with managing the region's Critical Infrastructure Protection and Resilience.

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

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

To discuss exhibiting and sponsorship opportunities contact:

Ray Beauchamp
(Americas)
E: rayb@torchmarketing.co.uk
T: +1 408-921-2932

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

The premier discussion for securing America's critical infrastructure

Supporting Organisations:

International Association of CIP Professionals

Help2Protect

STME

ISIO

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

An Interview with CITGO

Ben Lane, CIPRNA event manager, met Sterling Neblett, Vice President & General Manager, CITGO Lake Charles refinery.

Ben Lane (BL): Lake Charles is situated in quite a vulnerable location on the Gulf Coast and the area has experienced numerous hurricanes, including Hurricane Laura in 2020, which caused much local damage – how does CITGO plan for such natural disaster events?

Sterling Neblett (SN): The Lake Charles Refinery has a robust hurricane emergency response plan that covers preparations prior to the storm, what happens during the storm, and procedures to inspect and restart the refinery after the storm passes, all with the overarching goal of safety first for our people. Back-to-back hurricanes hit the CITGO Lake Charles Refinery in 2020, so we keep our response plan and procedures updated and ready.

Sterling Neblett, Vice President & General Manager, CITGO Lake Charles refinery

Hurricanes cause damage in three ways, and our facility needs to be ready for all:

- Wind – our systems are designed and built with potential winds in mind. Personnel cannot work in high wind conditions, so our shut down plans in advance of a storm take this

into account.

• Rain – We design our drainage and water treatment systems for historical probable rain events, whether related to a hurricane or not. This takes into consideration the topography and size of our facility. We have constructed tanks on our facility with the sole purpose of collecting rainfall runoff to prevent any of the materials we handle from escaping the area.

• Surge – our facility is situated on a natural bluff, with most of our site located above typical surge levels.

BL: Many local and national industries rely on the services of CITGO. How does it work with its stakeholders/partners to ensure continuity of supply in such extreme circumstances/events?

SN: Through our Business Continuity Plan, we work with various teams, including supply and trading and our Corpus Christi refinery, to minimize disruptions. As you know, these types of supply disruptions can increase prices for customers - no one wants that. As we have experienced, it can take many days to restore electrical service in the aftermath of a hurricane, and these types of utilities are required for us to ship products to our national and international customers. To assist our local first responders in these situations, we provide fuel that is stored in our tanks until proper services are restored.

BL: How often are plans against the threats of disasters (whether natural or man-made) or terrorism type threats, including cyber threats, reviewed and how do you aim to improve on those plans – what goals are deemed to be an improvement on a plan?

SN: We review our hurricane plan annually, incorporating changes that are learned from each hurricane season – even if no storm affects us. We also conduct spill response drills and training – occasionally with industry and government partners – so that we can be prepared if ever needed. Regarding cyber threats, we recently conducted a tabletop exercise with senior management with the goal of testing and strengthening our cyber incident response plan.

BL: Did CITGO learn from the Colonial Pipeline ransomware attack in 2021, and how did it change its program against cyber threats?

SN: The Colonial incident reinforced our existing efforts to strengthen our cyber defense and detection capabilities. While we already had a cyber plan, we have devoted more time and resources in our ability to respond and recover quickly should a cyber incident occur.

About Sterling Neblett

Sterling Neblett was named Vice President & General Manager of the Lake Charles Manufacturing Complex in March 2022. Sterling started his CITGO career in 1990 at the Lake Charles Manufacturing Complex where he held several engineering and logistics positions. Numerous economics, information technology and logistics positions followed at the corporate offices and Lake Charles culminating in his position as General Manager of Refinery Optimization and Excellence in Houston. In 2021 he was appointed General Manager of Engineering and Business Services at the Lemont Refinery. Sterling holds a bachelor's degree in Chemical Engineering from University of Arkansas.

Geopolitics Accelerates Need For Stronger Cyber Crisis Management

ENISA publishes a study on 'Best Practices for Cyber Crisis Management' that assists in preparation for crisis management. The study was conducted for the EU Cyber Crisis Liaison Organisation Network (CyCLONe) and is now available publicly.

The geopolitical situation continues to impact the cyber threat landscape also within the European Union. Planning for expected or unexpected threats and incidents is vital for good crisis management.

EU Agency for Cybersecurity Executive Director, Juhan Lepassaar underlined that "Sharing best practices for Member States is a step in successfully strengthening cyber crisis management. This report serves as a tool to assist with implementing the provisions of the NIS2 Directive. Crisis management processes for business continuity are paramount."

The study outlines the framework and circumstances with cyber crisis scenarios and proposes a series of best practices that will enable the transition into the new requirements of NIS2 Directive, the EU-wide legislation on cybersecurity. The study aims to bring a heterogeneous ecosystem towards stronger harmonisation.

The proposed best practices are clustered into the four phases of the cyber crisis management cycle (prevention, preparedness, response and recovery) and refer to issues arising during each stage with an all-hazards approach.

Concluding with a list of recommendations, ENISA proposes steps to improve Member States' capacity-building and operational cooperation in the context of cyber crisis management.

Cyber Crisis Management Framework through NIS2

The long history of the EU regarding cybersecurity, and particularly cyber crisis, proves its commitment in building a solid legislative framework to safeguard Member States from emerging threats. Built upon the first directive on Network and Information Security (NIS) that was set in 2016, the NIS2 entry into force marks a transformative period in the field of cybersecurity in the EU due to the new, upgraded provisions and obligations for Member States to incorporate into their national legislation. A key change brought by the adoption of NIS2 includes the reinforced role of ENISA in coordinating cybersecurity actors, such as EU-Cyber Crises Liaison Organisation Network (EU-CyCLONe) and the EU CSIRTs Network.

The European cyber crisis liaison organisation network (EU-CyCLONe)

Under NIS2 Directive, ENISA's mandate has a role as the secretariat for Cyber Crises Liaison Organisation Network (EU CyCLONe), a network dedicated to enhance Member States' national authorities' cooperation in cyber crisis activities and management.

The network collaborates and develops information sharing and situational awareness based on the support and tools provided by ENISA. The network is chaired in turns by a representative from the Presidency of the Council of the EU.

Formed by the representatives of Member States' cyber crisis management authorities, the EU CyCLONe intervenes together with the European Commission in case of large-scale cybersecurity incidents likely to have a significant impact on services and activities falling into the scope of the NIS2. ENISA also supports the organisation of exercises for EU CyCLONe members, such as CySOPex (played by officers) and as, in this case, BlueOLEx (played by executives).

ENISA pioneers the development of proper mechanisms and consistency for cyber incidents, crisis management and conducting cyber exercises. ENISA is tasked to roll-out the implementation of the Cybersecurity Support Action in 2022 that includes the provision of support to Member States to further mitigate the risks of large-scale cybersecurity incidents in the short term.

World Border Security Congress

25th-27th March 2025

Madrid, Spain

www.world-border-congress.com

Patrolling the Periphery - Developing Border Strategies Through Co-operation and Technology

Co-hosted and Supported by:

GOBIERNO DE ESPAÑA | MINISTERIO DEL INTERIOR

SAVE THE DATES

Spain's vast coastline and strategic location between Africa and Europe present unique challenges for the National Police and Guardia Civil.

Spain faces a constant influx of migrants seeking a better life in Europe. The Canary Islands and the enclaves of Ceuta and Melilla, bordering Morocco, are popular entry points. Patrolling these vast stretches, especially maritime borders, requires significant resources.

Spain is also a key entry point for hashish from Morocco and cocaine from South America destined for other European countries. The decentralized nature of trafficking groups makes it difficult to infiltrate and dismantle them.

The country, and region's, border security landscape is constantly evolving. By addressing these challenges through international collaboration, innovative technologies, and strategic resource allocation, the international border security community can strive towards a more secure future.

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

Join us in Madrid, Spain on 25th-27th March 2025 for the next gathering of international border security, protection and migration management professionals.

www.world-border-congress.com

To discuss exhibiting and sponsorship opportunities and your involvement contact:

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

Ray Beauchamp
Americas
E: rayb@torchmarketing.co.uk
T: +1 408-921-2932

Jerome Merite
France
E: j.callumerite@gmail.com
T: +33 (0) 6 11 27 10 53

for the international border management and security industry

Supported by:

Media Partners:

Is Cybersecurity As Enchanted as Sleeping Beauty?

Tomas Petru, Head of Sales CE, Goldilock

In my work, I sift through a vast amount of news regarding cybersecurity, examining numerous reports that are available, researching the attack and breach stories. The situation is, without doubt, severe. You might have come across the staggering figure of 8 trillion U.S. dollars, representing the annual global cost of cybercrime. It's a number that's hard to overlook. To counteract this, the amount expected to be spent on cybersecurity for 2023 is projected to reach 150 billion dollars. A simple calculation reveals that what we invest in our protection equates to merely a week's worth of the damages caused by cybercrime.

When you juxtapose these figures with the costs associated with physical defense and warfare, the perspective shifts dramatically as well. The Second World War has been estimated to cost around one trillion U.S. dollars, which, adjusted for today's inflation, amounts to 17 trillion dollars. This means that the annual cost of cybercrime is equivalent to the expenses of two years of Second World War! Another shocking comparison is with global defense spending, which is currently around 2 trillion U.S. dollars. Therefore, the damages from cybercrime are four times greater every year than our

fully loaded global defense costs.

Despite these sobering numbers, when we observe business practices within the blended realms of the physical and cyber worlds and scrutinize the strategies of management and, quite importantly, the practices and approaches of IT and cybersecurity specialists, it's evident that the prevailing attitude is 'business as usual.' This approach has been static for the past 25 years, punctuated only by bold declarations that the tide will turn in favor of the defenders. Yet the approach remains unchanged. A well-known adage suggests that expecting different outcomes while repeating the same actions is a folly. It appears the entire market is under a spell, bewitched by connectivity—insisting on connecting everything, everywhere, all the time. The numbers clearly indicate that this mantra of connectivity is flawed. And yet, even as the ship sinks, the party rages on, with Sleeping Beauty and the entire kingdom lost in a deep slumber.

How Did We Get Here?

It seems that in the physical world, we are more capable of recognizing change, although even this is debatable. If you examine photographs of Las Vegas or Dubai from 1990, you'll see a sparse landscape with only a few buildings, basic infrastructure, and plenty of open space. Fast forward to the years 2000, 2010, and 2024, the transformation is undeniable—10-lane highways, high-rises sprouting like mushrooms, and hotels housing thousands of rooms. Decades of change might not be immediately visible, but after refreshing

our memory, we can recall and acknowledge the dramatic developments.

In the cyber world of the early '90s, we operated individual computers; the fortunate few had modems connecting to quirky BBS systems, and interconnected business applications were a rarity. As we transitioned to the internet, and by the year 2000, we witnessed the emergence of the first significant websites, albeit with limited content. We were all friends then, excited about the possibilities. Even viruses, which did exist, were more of an annoyance than a threat, often whimsically asking for a 'cookie'. They were there not to kill, yet.

The subsequent decade propelled us into the age of services, and through the dot-com bubble, we arrived at the brink of carrying full-blown computers in our pockets. Today, an astounding 17 billion devices are connected to the internet, twice as many as there are people on the planet. By 2027, we anticipate connecting at least another 10 billion devices. The real world and the cyber world are no longer separate realms; they have merged into our singular reality. With AI widely accessible, the year 2023 brought a transformation as significant as the invention of the steam engine.

The Current State of Cybersecurity

How have businesses, their management, and IT, cyber, and technology specialists responded? They persist in the old ways—connecting more, faster, and continuously. They seem to ignore that we no longer inhabit the sparse digital landscape of the '90s. We live in a world dense with digital highways and skyscrapers. Not everyone is a friend, not on a personal level, and certainly not on a governmental level anymore. The initial excitement of globalization has waned, and we are witnessing a considerable rollback and polarization. The United States, through legislation like the Inflation Reduction Act and CHIPS Act, has financed globalization, but what about the security professionals?

The prevalent, albeit flawed, response has been to layer on more software tools for protection. However, each of these tools often

requires one or two additional software systems, and as we've come to realize, they are riddled with vulnerabilities as expansive as the holes in Emmental cheese. The database of vulnerabilities has ballooned from 10,000 known vulnerabilities in 2010 to over 220,000 known vulnerabilities today—a 22-fold increase. It's reasonable to infer that we're only seeing the tip of the iceberg. Even if we disregard the millions of unknown vulnerabilities, it's a fair assumption that cybercriminals are aware of hundreds, if not thousands, of yet-to-be-publicly-disclosed issues.

Businesses, along with cybersecurity and IT providers, still leave the door ajar, despite all the security claims and statements about the tide turning in favor of the defenders. The situation has grown so dire that Gartner predicts successful attacks with the intent to cause physical harm and kill by 2027. I believe this is already occurring. Data leaks not only lead to financial and business ruin but also to shattered lives and, ultimately, death. It's time to do things differently.

Waking Up from the Enchantment

76%. What number is it? 76% represents the potential cybercrime exposure decrease by simply disconnecting white-collar workplaces from the internet outside of their business hours. By doing so, we can decrease the attack surface by 76%. If there were a 76% chance of winning the lottery, wouldn't you take that bet every time?

98.2% is another number defined with the masters of backup from Veeam in our discussion. Their experience suggests that three hours are typically needed to update the weekly backups. Disconnecting them for the rest of the week provides such a significant security benefit that they've proposed an ingenious idea: when the backups are disconnected, connect a system configured in the same way, only with fake data, creating a very effective honeypot. As attackers in ransomware cases are going not only after the databases but also after the backups and archives to prevent restoration, this strategy could turn the tables by comforting attackers with fake data while giving defenders their own 'kill box' to identify any change or activity.

OT systems are notoriously difficult to protect, regardless of the supplier, even among the big names. The security in these systems is laughably inadequate. There have been moments when this worked to our advantage, such as when we sabotaged Iranian centrifuges to hinder their nuclear program. But when we are the target, there's no reason to laugh. Let's not delude ourselves; the only working solution for protecting OT systems is isolation and disconnection. A straightforward approach is to air-gap these systems with a device such as Goldilock Drawbridge, which allows scheduling of time frames for system synchronization with central control. For constant telemetry, another less-known technology, the data diode, which allows one-way data transfer, can be used in conjunction with Drawbridge to create an impenetrable solution.

Ignoring the risks of compromised technology from unfriendly manufacturers in unfriendly countries is not an option. The risk is serious and well-documented. In some countries, swap-and-replace programs are in place, but until you can take advantage of these, installing a Drawbridge at the borders of these technology centers makes perfect sense.

For something straightforward, consider the real story of a power plant where the security manager identified the connection between the IT and OT systems. They pulled out the wire from the rack, tied a red ribbon around it, placed wire cutters next to it, and instructed the service crew to cut the cable if things went awry. This rudimentary method works but is not scalable and is challenging to manage across multiple remote locations.

A number of critical infrastructure entities, not just banks, manage vast databases of personal data. It's time to view such data as a lethal weapon, as its leak can destroy lives. In most cases, truly critical data can be stored separately for auditing and security reasons and replaced by artificial identifiers for daily operations. Databases containing critical data should be air-gapped to protect against both external and internal attackers.

Physical infrastructure, especially for utilities and businesses operating in vast and high-risk areas, is often at risk. Frequently, infrastructure wires are connected during construction for testing purposes and are never disconnected afterward, thereby creating efficient access points for attackers. The solution? Disconnection of such infrastructure after initial tests and reactivation only during

authorized service. Managing such physical infrastructure might be cumbersome, but it can be streamlined by air-gapping with devices like Goldilock Drawbridge that provide out-of-band control.

Critical infrastructure entities can do a lot with a little effort. By fine-tuning their physical infrastructure, following TSA's requirement to be able to operate in "island mode," and deploying isolation and segmentation strategies, they can improve resilience by decreasing their operational dependence on connectivity. We must awaken from our enchanted slumber and start doing things differently. Otherwise, the proverbial boat will sink.

To my astonishment, it's incredibly difficult to enact this change. The mantra of always being connected has indoctrinated us deeply. There is nowhere to hide. A major telecommunications operator was recently brought down following international political events, despite their confidence in their security teams and tools. It makes me profoundly sad, but I understand that shifting to a disconnection strategy is a radical departure from the previous mantra.

All of this relates to the defense-in-depth strategy, which must replace perimeter protection. Zero trust is a significant milestone on this journey, but it's just the beginning. Physical security of cyber infrastructure at layer one is imperative. Just as we have circuit breakers in our electrical networks, secured valves in water and gas distribution, and floodgates in tunnels, it's time for drawbridges in our cyber critical infrastructure.

To reprogram our approach to cybersecurity, consider the following comfortable strategies:

Learn from Fairy Tales during the time with your kids:

Even Disney movies offer blueprints for defense in depth—proven by centuries. They showcase all components of island operation, segmentation, and isolation.

Study Historical Fortifications:

Beyond just castles, explore literature about fortifications. It's both entertaining and enlightening, providing great ideas for critical infrastructure protection. You can get inspired even by the notoriously known "The Art of War".

Visit Castles with your family:

Travel to castles across Europe, such as those in UK, Germany, the Czech Republic, or France. These visits can inspire protection strategies for your critical infrastructure while providing quality family time.

Let's disconnect to reduce cybercrime exposure, save money, and, most importantly, save lives. It's time for the cybersecurity industry to embrace the drawbridge concept—disconnecting and isolating to protect.

ICYMI – FEMA Signs MOU to Strengthen Cooperation with The Swedish Civil Contingencies Agency

FEMA signed a Memorandum of Understanding (MOU) with The Swedish Civil Contingencies Agency. This MOU formalizes our countries' mutual commitment to advancing global resilience and sharing emergency management strategies. FEMA Administrator Deanne Criswell joined the Director General of the Swedish Civil Contingencies Agency Charlotte Petri Gornitzka and Sweden's Minister of Civil Defence Carl-Oskar Bohlin at the Swedish embassy.

"2024 is FEMA's Year of Resilience, an opportunity to highlight the important work we do to help communities mitigate risk, so they can respond faster and recover more effectively," said Administrator Criswell. "The emergency management field is becoming more complex and our disaster tempo continues to increase and we know that we cannot solve these problems alone. With this partnership, Sweden and the U.S. can share best practices on how we incentivize individuals and communities to mitigate their risks."

The MOU recognizes that the United States and Sweden face growing national security threats and natural disaster risks. The memorandum builds upon our existing cooperation and Sweden's recent ascension to NATO, to foster greater collaboration on plans and priorities. It also helps us encourage readiness, civil protection and disaster risk reduction within our respective territories.

TSA announces appointment of members to the Surface Transportation Security Advisory Committee

The Transportation Security Administration (TSA) appointed nine people as voting members of the Surface Transportation Security Advisory Committee (STSAC). With these appointments, two new and seven reappointed, the STSAC now includes 30 voting members.

The STSAC was established by Congress in 2019 to advise the TSA Administrator on surface transportation security matters, including recommendations for the development, refinement and implementation of policies, programs, initiatives, rulemakings, and security directives pertaining to the surface transportation sector.

The new members are:

- Christopher Hand, Director of Research, Brotherhood of Railroad Signalmen

- Kaitlyn Holmecki, Senior Manager, International Trade & Security Policy, American Trucking Association

The reappointed members are:

- Jared Cassity, Chief of Safety and Alternate National Legislative Director, SMART Transportation

- James Cook, Assistant Chief of Police, AMTRAK

- Brian Harrell, Vice President & Chief Security Officer, AVANGRID

- Norma Krayem, Vice President, Chair, Cybersecurity, Privacy & Digital Innovation Practice Group, Van Scoyoc Associates

- Robert Mims, Director, Technology Security, Southern Company Gas

- Christopher Trucillo, Chief of Police, New Jersey Transit Police Department

- Lowell Williams, Chief Executive Officer, Cold Iron Security

The STSAC members represent each mode of surface transportation, such as freight rail, highways, mass transit, over-the-road bus, passenger rail, pipelines, school bus industry and trucking among others. For a complete list, please see the STSAC Charter. The Committee also has 14 non-voting members who serve in an advisory capacity for two-year terms from the Departments of Defense, Energy, Homeland Security, and Transportation, as well as the Federal Bureau of Investigation.

Custom-made Awareness Raising to enhance Cybersecurity Culture

The European Union Agency for Cybersecurity (ENISA) empowers organisations by publishing the updated version of the 'Awareness Raising in a Box'.

Advanced protection of systems and a robust cybersecurity strategy have become a priority for all kinds of organisations, as cybersecurity issues and threats have evolved to be increasingly sophisticated and pervasive. Thus, awareness raising activities and having a relevant methodology in place are a fundamental to integrating cybersecurity in the organisational culture. With a view to achieve this goal, applying game design elements in cybersecurity awareness activities can simplify familiarisation with terms and concepts through

a hands-on experience and motivate employees' participation.

To test the new edition of the all-in-one toolkit, ENISA piloted the Awareness Raising in a Box (AR-in-a-BOX) with the Cypriot Digital Security Authority and the Cypriot National Coordination Centre.

AR-in-a-Box allows professionals from small and medium (SMEs) to big enterprises and public or private entities, to improve their knowledge on cybersecurity awareness techniques. This comprehensive toolkit offers a blend of theoretical frameworks and practical resources, enabling organisations to craft tailored cybersecurity awareness programmes, including gamification of content.

Notably, the updated version features an online Cyber Awareness Game accessible through the EU ACADEMY.

The updated version of AR-in-a-Box includes the existing catalogue of instructions, games and activities but has also been enriched with the addition of a new guide for the development of internal and external cyber crisis communication plans.

The cyber crisis communication guide aims to help organisations and experts improve their communicational preparedness and response, in times of a cybersecurity crisis. As such incidents may impact several aspects of their operations, the guide provides a holistic approach on their protection and mitigation of risks and damages.

Shaping Cybersecurity Policy towards a trusted and secure Europe

European Union Agency for Cybersecurity (ENISA),the European Commission (DG CNECT) and the Belgian presidency of the Council of the European Union organised the 2nd EU Cybersecurity Policy Conference.

This year significant attention was dedicated to the ongoing implementation process of the latest EU cybersecurity policies, both from the national and EU perspective. Against the backdrop of evolving geopolitical developments and the ever-shifting cyber threat landscape, discussions also touched upon the complexities and hurdles within the cybersecurity world and how they will eventually shape the policy priorities.

Among the themes of the conference was the implementation process of the NIS2 Directive provisions and its impact on critical infrastructure sectors, the necessity for more synergies between defence and civilian cybersecurity communities, as well as the emergence of global cybersecurity threats, combined with the rise of new technologies, such as AI, and how policy foresight in this domain might contribute towards better cybersecurity preparedness.

In 2023, ENISA developed the NIS 360 methodology to do an assessment of NIS sectors on an annual basis, to understand better their overall maturity, criticality and to identify areas for improvement. The first edition covered 10 NIS sub-sectors. The policy framework in the finance sector is the most mature, while the telecoms, digital infrastructure, trust and finance sectors are scoring the highest in risk management.

CISA Announces Secure by Design Commitments from Leading Technology Providers

CISA has announced voluntary commitments by 68 of the world's leading software manufacturers to CISA's Secure by Design pledge to design products with greater security built in.

"More secure software is our best hope to protect against the seemingly never-ending scourge of cyberattacks facing our nation. I am glad to see leading software manufacturers recognize this by joining us at CISA to build a future that is more secure by design," CISA Director Jen Easterly said. "I applaud the companies who have already signed our pledge for their leadership and call on all software manufacturers to take the pledge and join us in creating a world where technology is safe and secure right out of the box."

By catalyzing action by some of the largest technology manufacturers, the Secure by Design pledge marks a major milestone in CISA's Secure by Design initiative. Participating software manufacturers are pledging to work over the next year to demonstrate measurable progress towards seven concrete goals. Collectively, these commitments will help protect Americans by securing the technology that our critical infrastructure relies on.

"A more secure by design future is indeed possible. The items in the pledge directly address some of the most pervasive cybersecurity threats we at CISA see today, and by taking the pledge software manufacturers are helping raise our national cybersecurity baseline," CISA Senior Technical Advisor Jack Cable said. "Every software manufacturer should recognize that they have a responsibility to protect their customers, contributing to our national and economic security. I appreciate the leadership of those who signed on and hope that every technology manufacturer will follow suit."

The seven goals of the pledge are:

- Multi-factor authentication (MFA). Within one year of signing the pledge, demonstrate actions taken to measurably increase the use of multi-factor authentication across the manufacturer's products.

- Default passwords. Within one year of signing the pledge, demonstrate measurable progress towards reducing default passwords across the manufacturers' products.

- Reducing entire classes of vulnerability. Within one year of signing the pledge, demonstrate actions taken towards enabling a significant measurable reduction in the prevalence of one or more vulnerability classes across the manufacturer's products.

- Security patches. Within one year of signing the pledge, demonstrate actions taken to measurably increase the installation of security patches by customers.

- Vulnerability disclosure policy. Within one year of signing the pledge, publish a vulnerability disclosure policy (VDP) that authorizes testing by members of the public on products offered by the manufacturer, commits to not recommending or pursuing legal action against anyone engaging in good faith efforts to follow the VDP, provides a clear channel to report vulnerabilities, and allows for public disclosure of vulnerabilities in line with coordinated vulnerability disclosure best practices and international standards.

- CVEs. Within one year of signing the pledge, demonstrate transparency in vulnerability reporting by including accurate Common Weakness Enumeration (CWE) and Common Platform Enumeration (CPE) fields in every Common Vulnerabilities and Exposures (CVE) record for the manufacturer's products. Additionally, issue CVEs in a timely manner for, at minimum, all critical or high impact vulnerabilities (whether discovered internally or by a third party) that either require actions by a customer to patch or have evidence of active exploitation.

- Evidence of intrusions. Within one year of signing the pledge, demonstrate a measurable increase in the ability for customers to gather evidence of cybersecurity intrusions affecting the manufacturer's products.

Each goal has core criteria which manufacturers are committing to work towards, in addition to context and example approaches to achieve the goal and demonstrate measurable progress. To enable a variety of approaches, software manufacturers participating in the pledge have the discretion to decide how best they can meet and demonstrate the core criteria of each goal, but progress should be demonstrated in public.

CISA's global Secure by Design initiative, launched last year, implements the White House's National Cybersecurity Strategy by shifting the cybersecurity burden away from end users and individuals to technology manufacturers who are most able to bear it. CISA urges software manufacturers to review CISA's Secure by Design guidance and Secure by Design alerts to build security into their products.

Help2Protect against the Insider Threat

Insider Threat Awareness and Program Development Training platform

Help2Protect.info

Protect your company from Insider Threats

In Collaboration with:

International Association of CIP Professionals

See below for 20% Off Special Offer

THREE TYPES OF INSIDERS - ONE TOOL TO DETECT THEM

Insiders may be involuntarily helping by not being sufficiently aware and trained about the potential impact of their actions, or they may be negligent. Only a small proportion of Insiders are malicious and have the intentional aim to damage the organisation. The Help2Protect program covers all 3 categories of Insiders: accidental, negligent and malicious. It also includes all types of crimes, including theft, espionage, sabotage, violent activism and organised crime, including terrorism.

BE PROACTIVE
AWARENESS TRAINING

How to help to protect you, your organisation and your colleagues.

BE READY
PROGRAM DEVELOPMENT TRAINING

How do you develop an effective Insider Threat Program for your organisation

An eLearning Platform dedicated to Security and the Insider Threat

www.help2protect.info

SPECIAL OFFER FOR IACIPP – 20% DISCOUNT OFF THE COURSE

IACIPP are offering you a 20% discount off this Insider Threat Detection and Prevention online course.

Register at: www.cip-association.org/help2protect - Promo Code: 7UATQW7M

ClanTect completes the installation of first of several critical infrastructure sites

ClanTect MDT works through the application of sound and vibration technology to execute an accurate, fast and safe search of any type of vehicle in 60 seconds.

Sensors are attached to the vehicle, to the ground and (in the case of wind) to a retractable 'WindFrame', so that all sources of vibration are measured and analysed. Even the faintest of movements (including a breath or the slight nod or twitch of a body) will be identified.

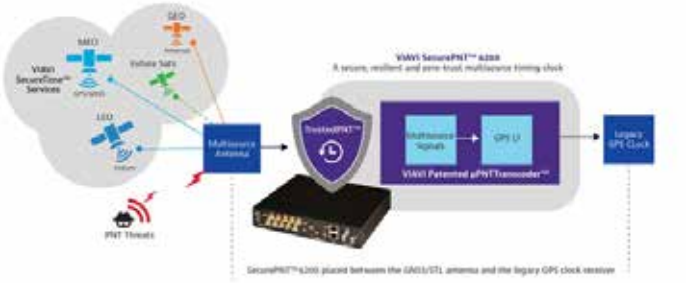
Critical infrastructure protection is now a key sector for ClanTect. ClanTect are engaged in multiple projects across a wide range of different sectors: petro-chemical and industrial sites, government buildings, distribution centres and nuclear and other energy facilities. These organisations have common issues: many sites were originally constructed 50 or more years ago, the infrastructure is aging, many are located in remote areas, with only very basic of search capabilities for vehicles at the entry and exit points. These factors create an enormous exposure to the illicit entry of 'bad actors', using ever more sophisticated techniques to gain entry.

Without exception, all of these sites have entrance and exit gates in very open environments, where the vehicles are exposed to multiple sources of external sound and ground vibration, including wind and rain, passing traffic, construction or maintenance work

ClanTect's in-house signal processing gives us a unique way of 'cancelling out' all other sources of external vibration, thereby being able to identify the all-important 'internal' vibration, i.e., emanating from people hiding inside the vehicle. ClanTect have replaced many older technology systems over the last few years, due to this ability to continue to operate and produce accurate search results in exposed open environments.

VIAVI Introduces Industry's Most Comprehensive Solution for Resilient Positioning, Navigation and Timing for Critical Infrastructure

Viavi Solutions announced the availability of SecurePNT™ 6200 with SecureTimeSM services, a resilient timing clock solution that delivers the most comprehensive assurance of positioning, navigation and timing (PNT) services used in critical infrastructure operations..



SecurePNT and SecureTime build on VIAVI's proven assured PNT solutions with the addition of the Fugro AtomiChron® timing service, enabling intelligent zero-trust multisource assurance combining signals from Geosynchronous Orbit (GEO), Low Earth Orbit (LEO) and Medium Earth Orbit (MEO) GPS and GNSS constellations.

Essential networks throughout the world – including 5G communications, transportation, energy, public safety, finance, defense and data centers – rely on publicly available GPS and GNSS signals for synchronization based on timing and location. These signals are occasionally unavailable or at risk of being jammed or spoofed, or satellites themselves can be attacked, with potentially catastrophic consequences. Governments have begun mandating that critical infrastructure providers improve resilience of their networks through more responsible use of PNT services.

VIAVI's portfolio of assured PNT products have been proven to provide redundant timing and location security in civilian and military applications, based on connectivity to the broadest range of timing sources in the market. The Fugro AtomiChron® timing source enables the VIAVI SecureTime eGNSSSM GEO service to deliver true authenticated and encrypted resilience and higher accuracy, not previously supported by traditional GNSS.

Indra equips the European Commission cyber risk management center with secure communications prepared to withstand future quantum computer attacks

The first pan-European virtual center for dynamic cyber risk management is being set up by an industry team led by Leonardo and including Indra. It will monitor, in real time, the degree of threat to which digital infrastructures are exposed throughout the continent, tracking the activity of criminal groups on the Internet, dark web and social networks, relying on different databases to extract intelligence.

The company will equip the center with advanced hybrid protection mechanisms to face the post-quantum scenario, in which the irruption of quantum computing will change the rules of cryptography, forcing the incorporation of new, even more secure algorithms to protect communications.

The centre will be equipped with Indra's COMSec proprietary technology solution that provides end-to-end encrypted voice, instant messaging and video services over mobile phones and PCs, using any cellular, wireless or satellite network worldwide, that will enable the personnel and managers to hold multiple video conferences and telephone conversations and exchange sensitive information.

Indra's technology will also protect the conversations and information exchanges within the center itself and cipher the data that are stored in it, preparing it to withstand "harvest now, decrypt later" threats whenever the technology so permits. Moreover, the post-quantum protocol which is used complies with the European NIS (Network and Information Systems Security) regulation and it has been supervised by the Spanish National Cryptologic Center.

Corero Network Security and SEMPRE Launch Partnership To Secure the Availability of Critical Infrastructure

Corero Network Security, the distributed denial of service (DDoS) protection specialists, announced a partnership with SEMPRE, a technology company dedicated to securing America's critical infrastructure.

Together, Corero and SEMPRE are developing military-grade, resilient communications nodes to support the future of high-availability communications services.

Corero's on-premises DDoS protection technology, ideally suited for this challenge, delivers analytics and protection across modular or distributed environments. The Corero SmartWall ONE architecture features node-by-node scaling and partitioned command-and-control, adapting dynamically to the tactical footprint of resilient critical infrastructure deployments.

SEMPRE provides a secure, resilient 5G cellular network and private local cloud for anytime, anywhere access to communications and high-performance edge computing. The security-focused software architecture within a tamper-resistant EMP-hardened enclosure ensures the network and local cloud are available in real-time, where and when its needed. Both SEMPRE fixed and mobile networks overlay and extend existing telecommunication infrastructure or operate as a stand-alone solution.

Rob Spalding, CEO of SEMPRE and former senior director of strategy at the National Security Council and retired USAF Brigadier General, stated, "By combining SEMPRE's secure anywhere, anytime network with Corero's industry-leading DDoS protection, we're creating a powerful solution for the military and beyond. This means critical information will flow freely even under attack, empowering decision-makers to react swiftly and accurately in any situation."

Johnson Controls Launches Security Operations Centers Service Offering

Johnson Controls has announced the commercial availability of its Security Operations Centers (SOC) service offering in the North American market. Building on 50 years of central monitoring and response services internationally, the SOC offering is available to North American customers seeking to improve business continuity and help reduce risk at a predictable as-a-service fee.

Johnson Controls designed this service offering with flexible bundled service packages to meet every facility's specific needs, delivered with complete onsite support or hybrid models. Common features provided by the SOC include:

- Standardized Protocols: Johnson Controls works directly with customers to develop standardized operating procedures to drive consistency and business efficiency.

- Thorough Assessments: A complete assessment of an organizations people, processes and technologies to recommend best practices and implement uniform protocols to help reduce risks.

- Staffing Support: Guaranteed 24/7/365 support.

- Auditing and Reporting: A comprehensive Quality Assurance program ensures consistency and provides visibility into accuracy of work being performed.

In addition to the SOC, Johnson Controls launched its Security Lifecycle Management with OpenBlue Services in 2024 which combines Johnson Controls OpenBlue suite of connected solutions, and the ability to monitor and manage security devices across vendors, with remote support services and meaningful insights from skilled engineers.

Cyolo Partners with Dragos to Unveil Holistic Secure Remote Access Solution for Critical Infrastructure

Cyolo, the secure remote access company for operational technology (OT) and industrial control systems (ICS), announced a strategic partnership with Dragos, a global supplier of cybersecurity for ICS/OT. Under the umbrella of Cyolo's CyoloVerse partner program, Cyolo's PRO Secure Remote Access Platform will work with Dragos's OT cybersecurity platform. This collaboration will provide organizations with an interoperable solution to protect their critical infrastructure against cyber threats.

New technology implementations in ICS/OT environments pose unique risks for critical infrastructure. Today's risks include lack of support for modern authentication or connectivity methods in traditional environments, connecting existing infrastructure with highly vulnerable end-of-life operating systems, or risk of breaches from third-party remote access.

This interoperability is designed to provide OT customers visibility and management of their asset inventory and enhance asset vulnerability detection and remediation capabilities through a seamless secure controlled access platform.

Bringing the Cyolo PRO platform alongside the Dragos OT-native network visibility and monitoring offerings gives an unparalleled advantage. The Dragos Platform enables organizations to scale protection, the threat intelligence to keep on top of current threats, and the tools to respond quickly to incidents. With Cyolo's role-based access, application, and policy control, in the future the Dragos Platform will be able to manage Cyolo's Identity-based parameters (users, applications, resources, policy) in accordance with SOC/IR policies and guidelines.

The solution plans to integrate Cyolo PRO and the Dragos Platform through an API architecture or operator console. It will deliver visibility and control of critical digital assets through secure identity-based access. Together, both companies will deliver simpler, stronger, and more efficient security controls that lay the foundation for Zero Trust (NIST 800-207).

ADVERTISING SALES

Ray Beauchamp -
Americas
E: rayb@torchmarketing.co.uk
T: +1-408-921-2932

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

Jina Lawrence
Rest of World
E: jinal@torchmarketing.co.uk
T: +44 (0) 7958 234750

INVITATION TO PARTICIPATE

Securing the Inter-Connected Society

The premier event for the critical infrastructure protection and resilience community.

The first 'Critical Infrastructure Protection Week' will take place in Madrid Spain and will see IACIPP host the 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'EU-CIP Horizon Project' conference as the first events as part of this initiative.

Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe.

The conference will look at the developing themes and challenges facing the industry, including the importance of the updated NIS2 Directive and Directive on the Resilience of Critical Entities and the obligations of CI owner/operators and agencies, as well as create a better understanding of the issues and the threats, helping to facilitate the work to develop frameworks, good risk management, strategic planning and implementation.

Join us in Madrid, Spain for the the 9th Critical Infrastructure Protection and Resilience Europe discussion on securing Europe's critical infrastructure, part of CIP Week in Europe.

www.cipre-expo.com

Leading the debate for securing Europe's critical infrastructure

Co-Hosted by:

International Association of CIP Professionals

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

To discuss exhibiting and sponsorship opportunities contact:

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

Jina Lawrence
(Rest of World)
E: jinal@torchmarketing.co.uk
T: +44 (0) 7958 234 750

Ray Beauchamp
(Americas)
E: rayb@torchmarketing.co.uk
T: +1-408-921-2932