Water Infrastructure Security Since 9/11: What's New, and Why?

CHARLES R. STACK, MPH, BCES, A.M.ASCE
Vice-President, NeoChloris Inc.
February 10, 2026

Charles Stack's background

- Master of Public Health, University of Illinois at Chicago (UIC), Epidemiology
- Experience in water and wastewater system design since 1980s
- Studied Soviet bioweapons, chemical weapons at UIC
- Member of FBI Private Industry Collaboration INFRAGARD , Subject Matter Expert on Water Infrastructure protection to FBI
- Board Certified Environmental Scientist, AAEES
- Contributing Author to National Standards for protection of water and wastewater infrastructure since 2005
- Associate Member, American Society of Civil Engineers (ASCE)

“What’s past is prologue…..”

William Shakespeare's
The Tempest (Act 2, Scene 1)

History of Threats to U.S. Water Infrastructure

This quote comes from a series of secret tapes recorded in Saddam Hussein's office in the mid-1990s (around August 1995) and released in February 2006 by ABC News.

During a discussion with his cabinet regarding United Nations inspectors and potential accusations of bio-terrorism, Deputy Prime Minister Tariq Aziz told Saddam:

"...the biological (attack) is very easy to make. It's so simple that any biologist can make a bottle of germs and drop it into a water tower and kill 100,000. This is not done by a state. No need to accuse a state. An individual can do it," he said.

(Chicago Tribune, Feb 16, 2006)

How did the US respond to the threats made by Saddam Hussein against US water infrastructure and subsequent attacks upon the Homeland?

- During the early-to-mid 2000s, after 9/11 and the anthrax incidents, there was national concern about **potential terrorist threats to critical infrastructure**, including water supplies.

- Illinois Governor Blagojevich's administration integrated **water system protection** into Illinois' homeland security framework.

- The governor promoted the development of **innovative detection technologies**—particularly by **Illinois small businesses and research institutions**—to identify chemical, biological, or radiological contaminants in municipal and regional water systems

BUILDING

BUSINESSES THAT BUILD COMMUNITIES

Chicago Community Ventures Newsletter Volume 2, Issue 4

2 Ci at INNOVATE Illinois 2005

2006 INNOVATE Illinois Kicks Off

As winners of the 2005 INNOVATE Illinois business challenge are still enjoying the visibility and new opportunities garnered since the 2005 event, the 2006 sponsors are gathering for the coming year.

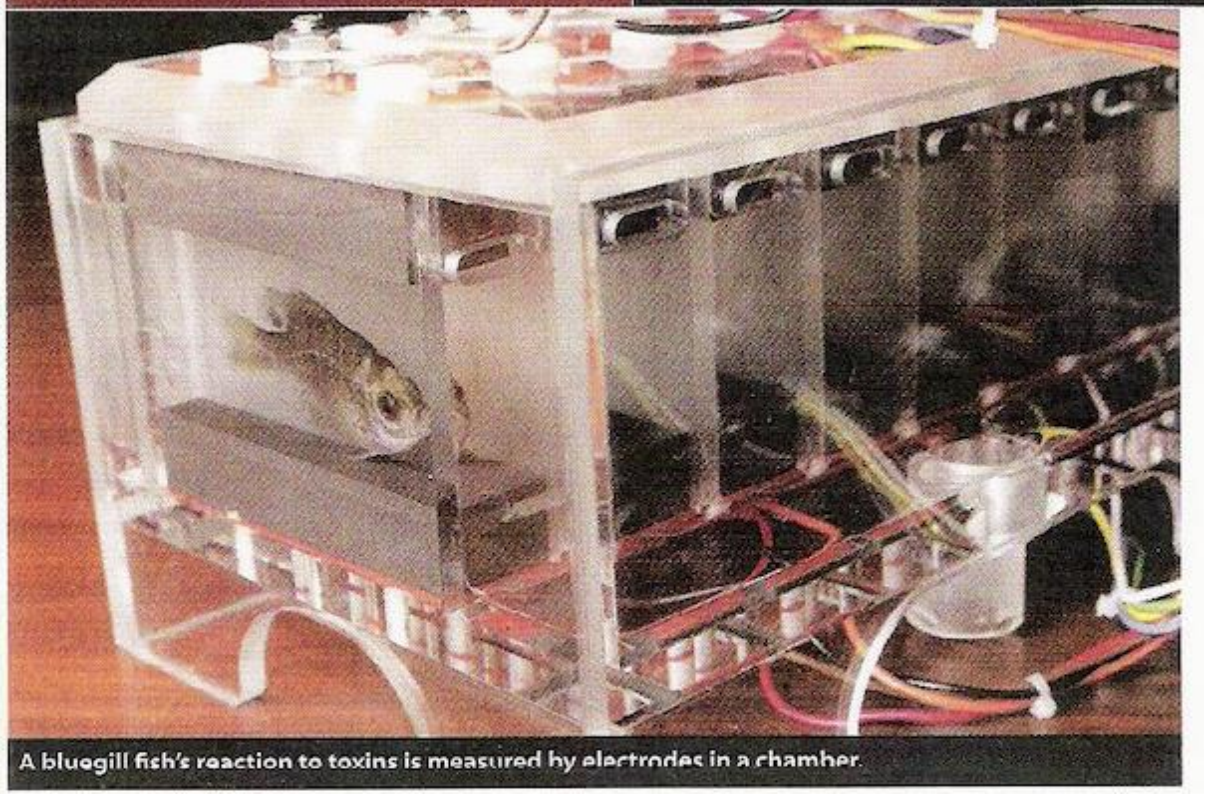
Constant Compliance, Inc. (2Ci), the winner of the 2005 Environmental sector award, builds technology for clean water, environmental and homeland security applications. Charles R. Stack, MPH, Vice President, credits INNOVATE Illinois with creating contacts with potential clients, business partners and funding prospects for the company. "There is a process to growing and sustaining an entrepreneurial company, and CCV has helped us through the steps of this process. I think every entrepreneur with a viable business plan can benefit from participating in INNOVATE Illinois."

The winners plan to use the award packages, valued at $20,000, to further develop their companies and reinvest in the community by hiring additional employees, creating local revenue and assisting in the revitalization of Chicago's redeveloping neighborhoods.

2Ci's BioSensor Platform was being used by the City of Hammond, Indiana to monitor sewage flows for toxic industrial wastewater discharges. Results were published and presented.

Performance of On-Line Respirometry at the Sanitary District of Hammond

INNOVATION NEWS

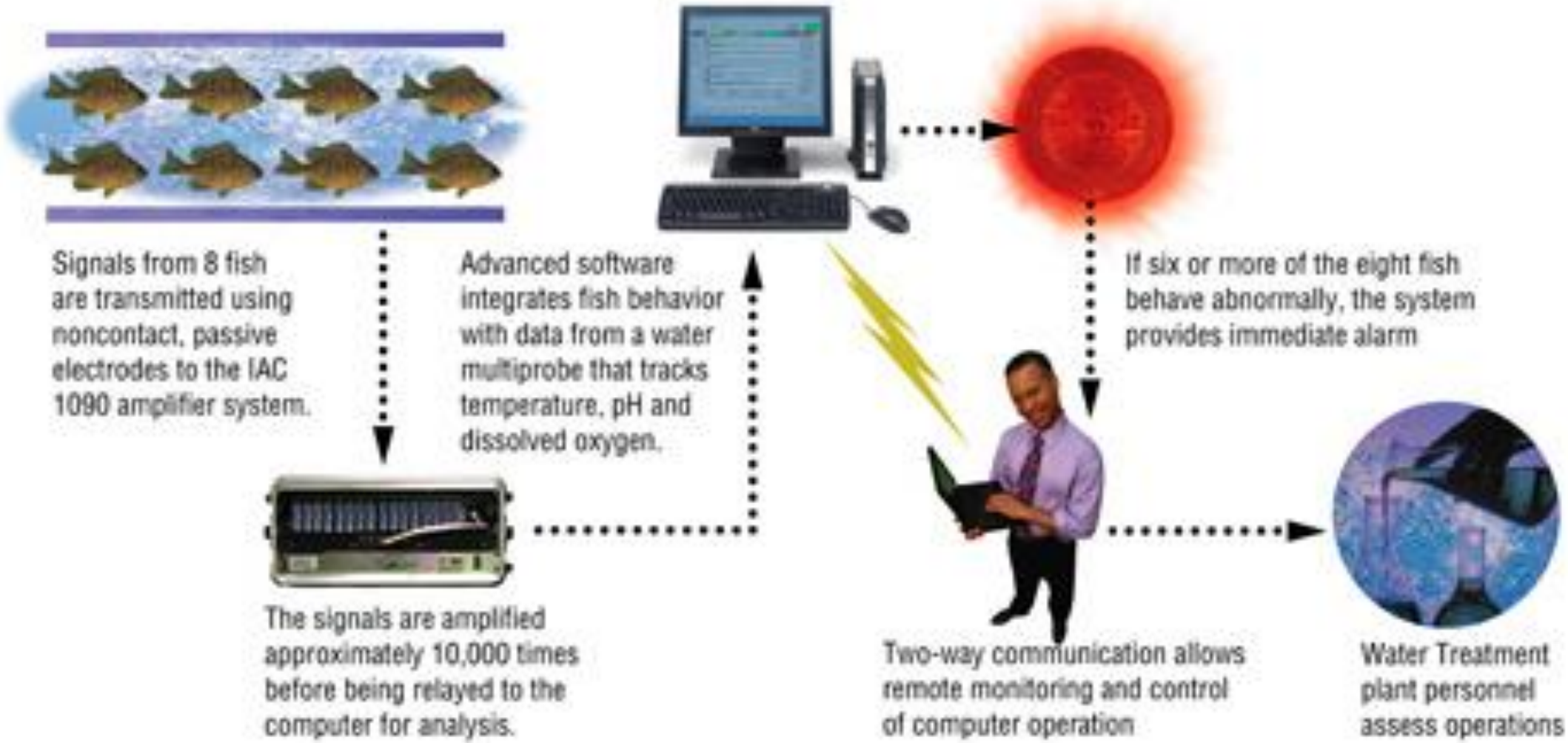


A bluegill fish's reaction to toxins is measured by electrodes in a chamber.

SENSORS

Swimming Sentinels

Fish enlisted in protecting water supplies from toxins


Signals from 8 fish are transmitted using noncontact, passive electrodes to the IAC 1090 amplifier system.
Advanced software integrates fish behavior with data from a water multiprobe that tracks temperature, pH and dissolved oxygen.
If six or more of the eight fish behave abnormally, the system provides immediate alarm
The signals are amplified approximately 10,000 times before being relayed to the computer for analysis.
Two-way communication allows remote monitoring and control of computer operation
Water Treatment plant personnel assess operations

ASCE/AWWA Draft American National Standard for Trial Use

Draft American National Standard for Trial Use

Guidelines for the Physical Security of Water Utilities

December 2006

ASCE
American Society of Civil Engineers

American Water Works Association
The Authoritative Resource on Safe Water™

Water Environment Federation®
Preserving & Enhancing the Global Water Environment

1.0 Application of Guidelines

1.1 Introduction

These water utility guidelines recommend physical and electronic security measures for physical protection systems to protect against identified adversaries, referred to as the design basis threats (DBTs), with specified motivation, tools, equipment, and weapons. Additional requirements and security equipment may be necessary to defend against threats with greater capabilities.

Threat Characteristics

Characteristic	Threat Categories			
	Vandal	Criminal	Saboteur	Terrorist
Motivation	Thrill, dare	Financial gain	Political cause	Political cause
Objective	Property damage	Theft	Disruption	Destruction and human casualties
Planning	Little or none	Possible	Definite	Extensive
Access	Stealth	Stealth	Stealth	Stealth or overt
Weapons	-	Knife, pistol, rifle	Explosives	Assault weapons, explosives, RPGs
Contaminants	-	-	Possible	Probable
Asset damage	Minimal	Minimal	Significant	Extensive
Injuries	-	Possible	Possible	Extensive
Fatalities	-	Possible	Possible	Definite

ASCE American Society of Civil Engineers

THE NATIONAL EMERGENCY RESPONSE & RESCUE TRAINING CENTER (NERRTC)

IN COOPERATION WITH THE

DEPARTMENT OF HOMELAND SECURITY (DHS)

STATE AND LOCAL GOVERNMENT COORDINATION PREPAREDNESS (SLGCP)

acknowledges

Charles R. Stack

for successful completion of the

Emergency Response to Threats of Intentional Contamination of Public Water Supplies

Milwaukee, Wisconsin

16 Hours

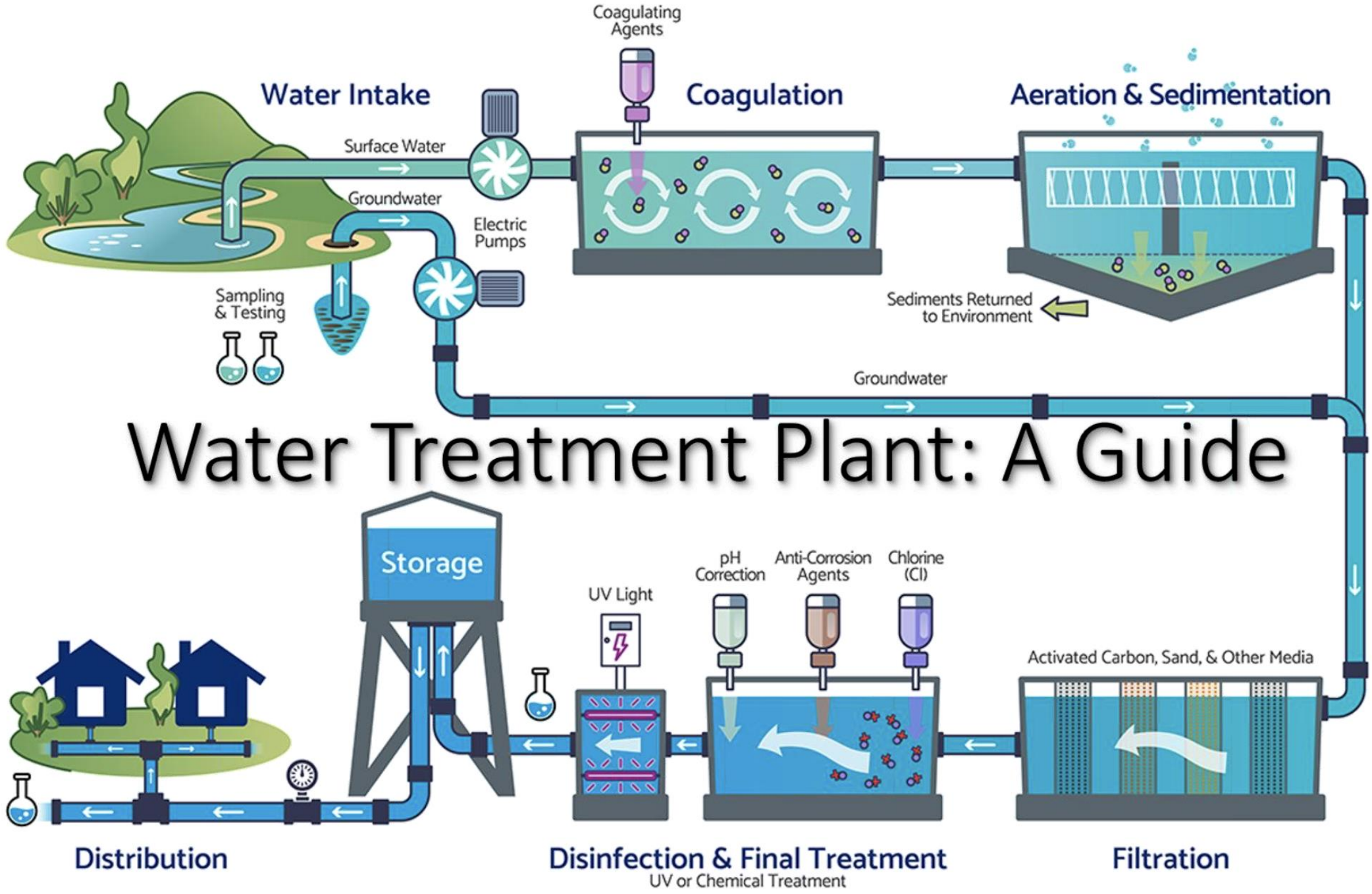
May 10-11, 2005

TEEX
TRAIN ▪ SERVE ▪ RESPOND

C. Suzanne Mencer
Director
State and Local Goverment Coordination Preparedness (SLGCP)

Dr. G. Kemble Bennett
Executive Director, NERRTC

EU NE4012 0009
State Board for Educator Certification #500132



Water Treatment Plant: A Guide

Terrorism Threats to the US Water Supply

Contamination of water sources

Terrorists could potentially introduce toxic chemicals or biological agents into reservoirs, lakes, or rivers.

Disruption of water treatment facilities including Cyber Attacks

Attacks on water treatment plants could disrupt the purification process, putting public health at risk.

Sabotage of water distribution systems

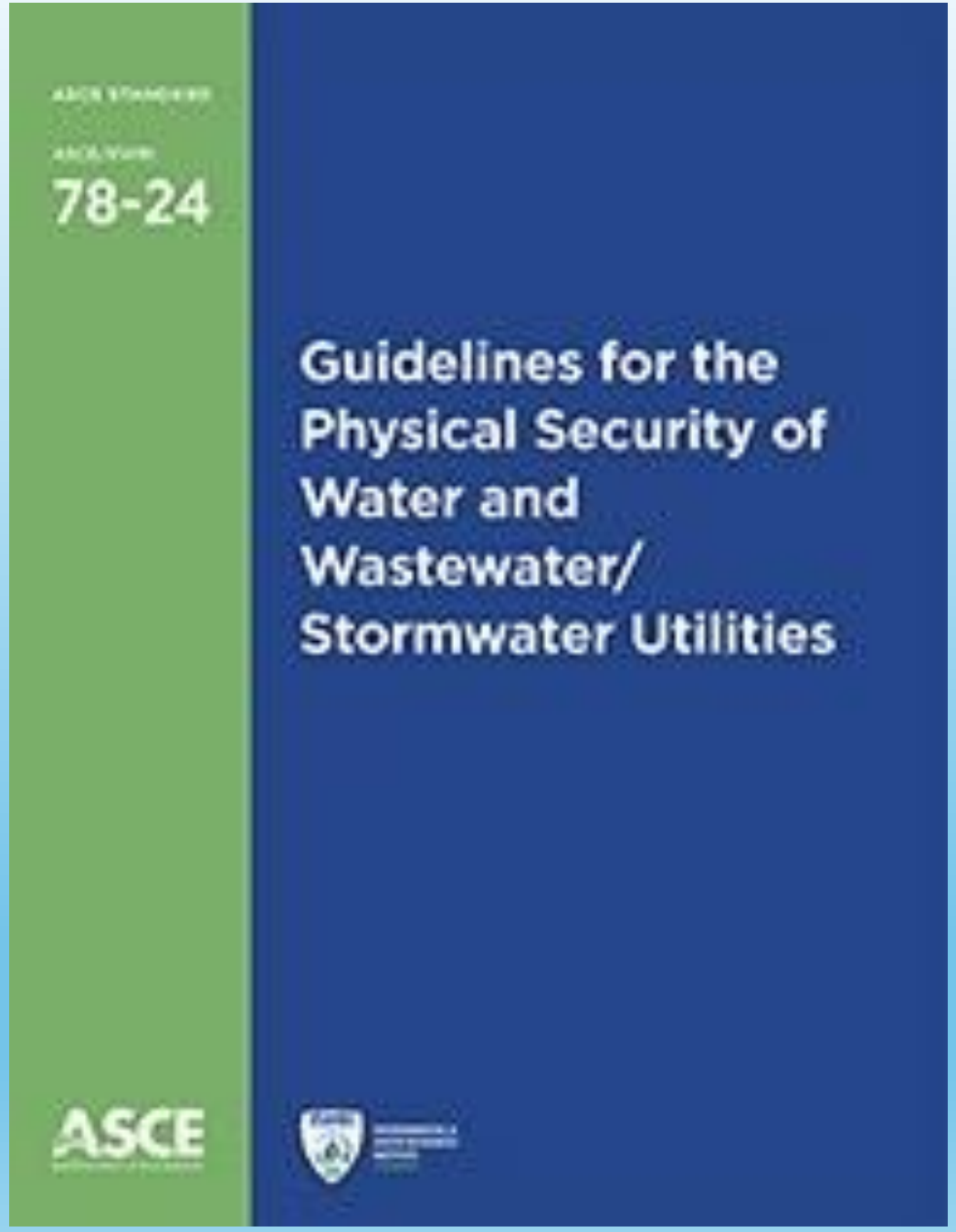
The water supply infrastructure, including pipelines and pumping stations, could be targeted by saboteurs.

- November 25, 2023

rol panel for a pump used by the Aliquippa Municipal Water Authority / photo via Aliquippa Water Authority

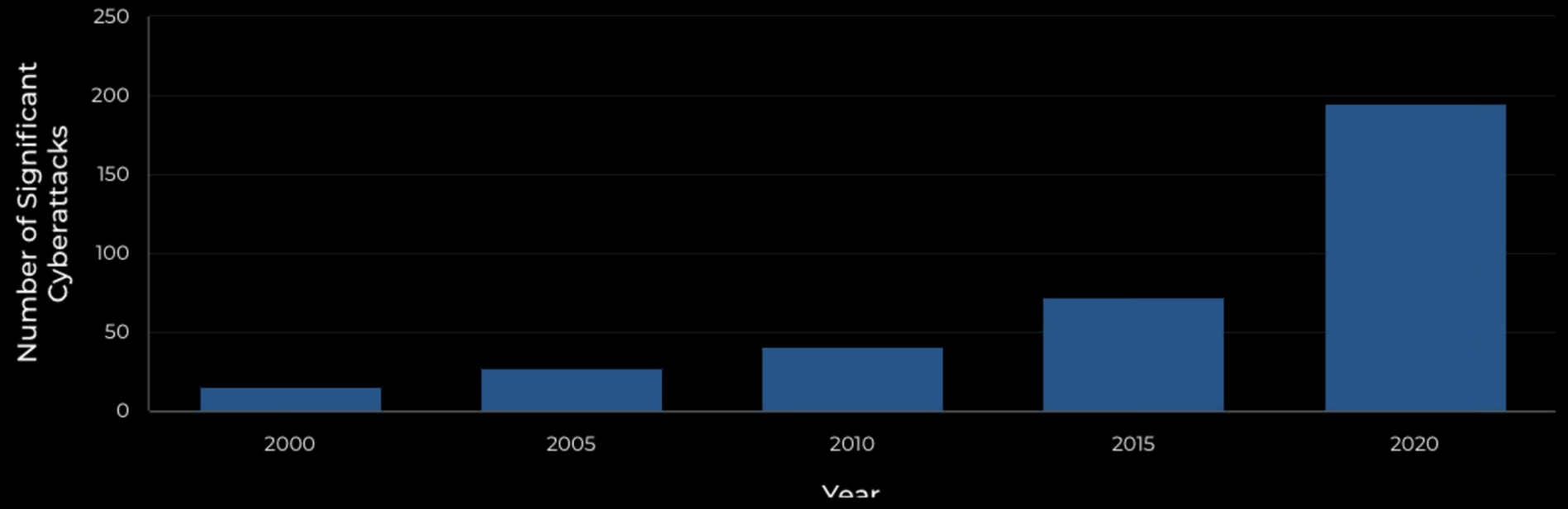
Recently Released Products

- Cybersecurity Alert - **Exploitation of Unitronics PLCs used in Water and Wastewater Systems**, 28 November 2023
- Cybersecurity Advisory – AA23-335A - CISA, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Environmental Protection Agency (EPA), and the Israel National Cyber Directorate (INCD) release joint Advisory on **IRGC-Affiliated Cyber Actors Exploiting PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities**, 1 December 2023
- Australian Signals Directorate Alert on **Exploitation of Unitronics Programmable Logic Controllers (PLCs),** 5 December 2023


78-24
Guidelines for the Physical Security of Water and Wastewater/ Stormwater Utilities
ASCE

What are some of the major water infrastructure security concerns that keep
the experts up at night in 2026?

Increasing Cyberattacks on US Water Infrastructure



The number of cyberattacks on US water infrastructure has risen sharply since 2000.

*Data from US Cybersecurity and Infrastructure Security Agency (CISA)

Some Recent Cyberattacks on Water Infrastructure

July 2022

South Staffordshire PLC, United Kingdom

Accessed SCADA Systems- Theft of Personally Identifiable Information. (PII)

- No affect on safe supply of water for 1.6M customers

November 2023

North Texas Municipal Water District, Texas, USA

Potentially >33,000 customer data files stolen. Operates 7 water treatment plants and 13 wastewater treatment plants servicing 2M residents across 10 counties

- Breach of Data and Loss of Business Systems

December 2023

Private Group Water Scheme, County Mayo, Ireland

Internet connected controller for water pressure. Device had default password. Entire water supply of 160 households.

-Complete Outage for 2 days

January 2024

Veolia North America, USA

Company operates 8,500 water and wastewater facilities around the world and in all 50 US states. Online bill payment system and theft of PII.

- customers experienced delays using the online bill payment systems.

April 2024

Tipton, Indiana, USA

The Cyber Army of Russia posted video showing hackers interacting with Tipton Wastewater Treatment Plant

- system transitioned to manual control

January 2023

Águas e Energia do Porto, Portugal

Company manages more than 1,200Miles of water infrastructure, possibly affecting millions of people.

- Data Stolen and disruption impacting customer service for several days

November 2023

Municipal Water Authority of Aliquippa, Pennsylvania, USA

Internet connected controller used to maintain water pressure was take offline. Services <30,000 customers, including 82 miles of water mains. Compromised operational technology, triggering manual override

January 2024

Southern Water, United Kingdom

2.5M customers and wastewater services)to more than 4.7M customers.

- Theft of PII and Ransomware of >750GB of data

January 2024

Hale Center, Muleshoe, Lockney and Abernathy, Texas, USA

SCADA systems hacked. Manual control overrides were needed. Remote Accessibility software

- Muleshoe water tank overflow for about 30-45 min before manual override


dji
HERO3+

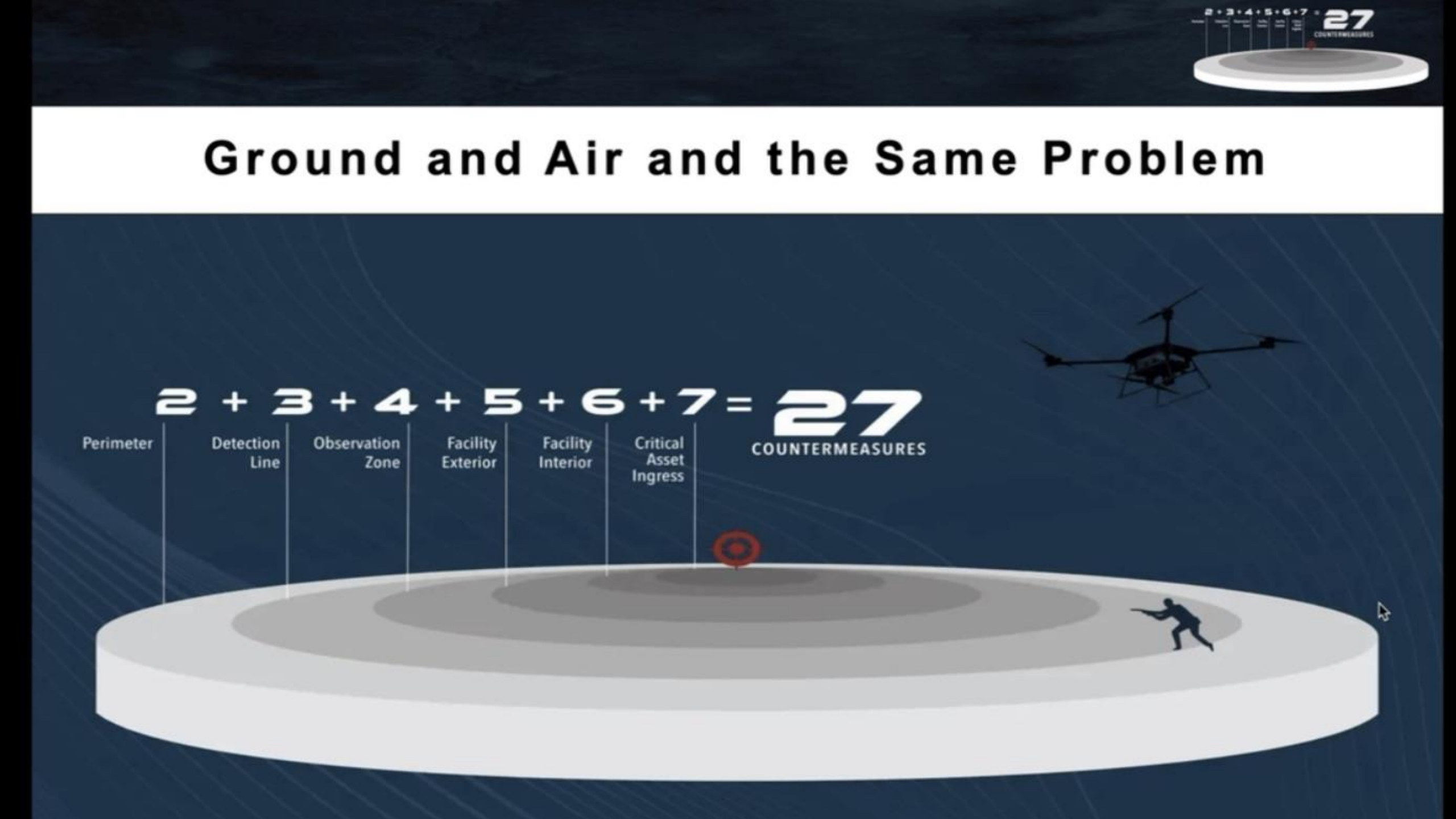
Ground and Air and the Same Problem

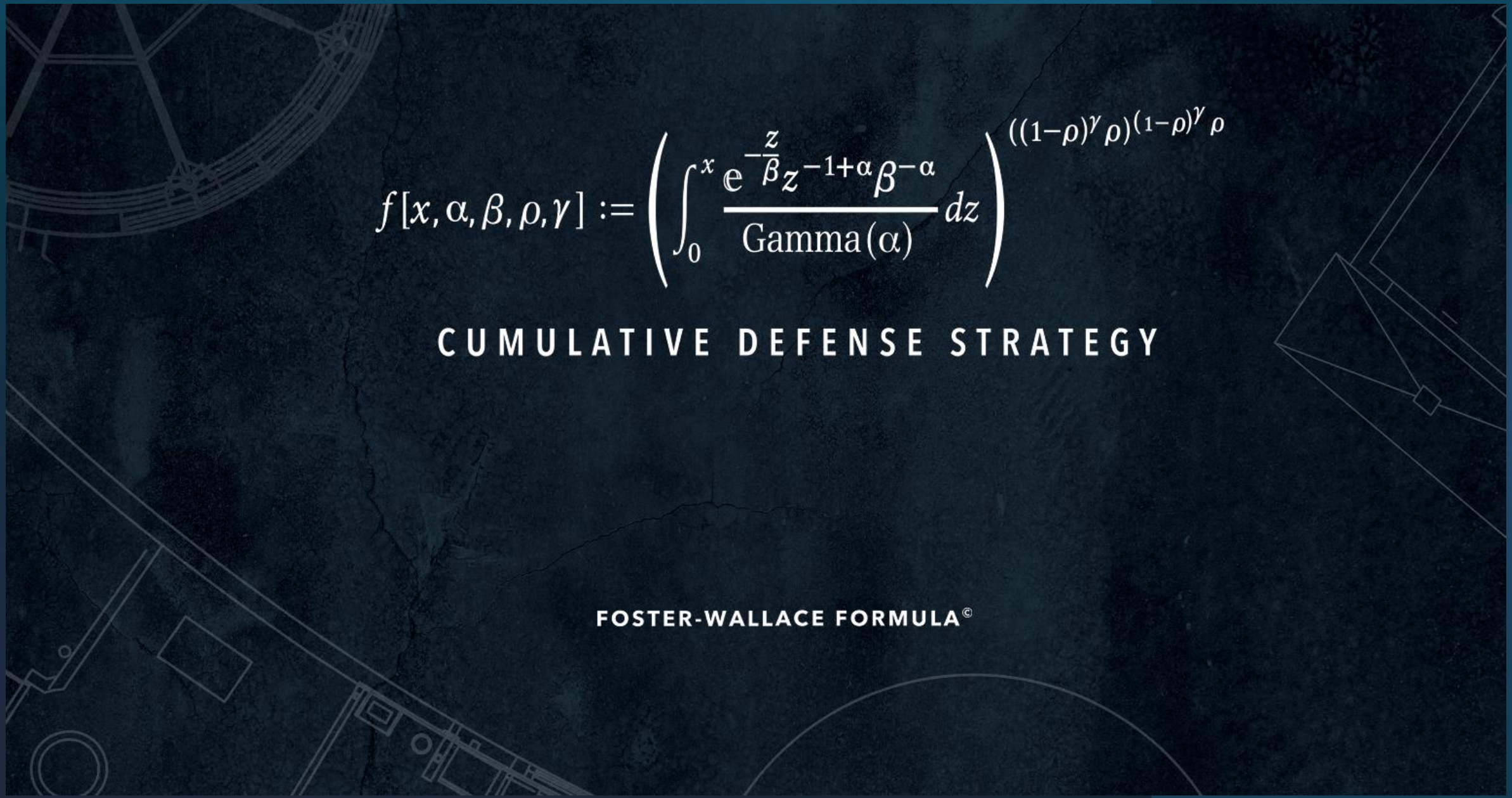
Airspace is simply another approach path to the same asset.

Facility diagram with ground paths + aerial paths converging on the same asset

- •Traditional security protects:
  - Doors
  - Gates
  - Fences
  - Roads
- •Drones introduce direct aerial access:
  - Over fences
  - Over walls
  - Over secure zones
- •Effective C-UAS extends the perimeter upward
- •Ground sensors and air sensors must be:
  - Coordinated

Ground and Air and the Same Problem




$f[x,\alpha,\beta,\rho,\gamma] := \left(\int_0^x \frac{e^{-\frac{z}{\beta}} z^{-1+\alpha} \beta^{-\alpha}}{\text{Gamma}(\alpha)} dz \right)^{((1-\rho)^\gamma \rho)^{(1-\rho)^\gamma \rho}}$
CUMULATIVE DEFENSE STRATEGY
FOSTER-WALLACE FORMULA©

2.5.5.2 Unmanned (Uncrewed) Aircraft System Data Sniffing Adversaries can attach a radio frequency transmitter to uncrewed aircraft systems to disrupt existing wireless communications.

When the disruption is removed, devices on the network retransmit their credentials to reconnect. The credentials are captured by a receiver on the uncrewed aircraft system and processed by the adversary to exploit vulnerabilities in the network.

ASCE 78-24, 2.5 SCENARIO IDENTIFICATION, ATTACK VECTORS – 2.5.5.2 *Unmanned (Uncrewed) Aircraft System Data Sniffing* (page 9)

“Empirical Risk Analysis Methodology for Adversarial Threats against Critical Infrastructure”

Authors: David W. Wallace, Lloyd Foster, Kris Schartau, David Lewin, and Conrad G. Keyes Jr., P.E., D.WRE, L.S.,

Publication: Journal of Infrastructure Systems
Volume 30, Issue 1

https://doi.org/10.1061/JITSE4.ISENG-2291

Cumulative Defense Strategy Overview

Cumulative Defense Strategy is a process that is used to help secure critical assets against malevolent attacks. The process takes a wholistic approach into helping protect the facility under evaluation.

Similar to methodologies used by other organizations, the approach considers the consequence of a particular critical asset being compromised and the approach used to carry out the attack.

Using path analysis and the existing physical security counter-measure installed at the facility, the degree of difficulty to compromise the critical asset is mathematically
calculated using the Foster–Wallace Formula (Wallace and Foster 2021).

With this information, the facilities' vulnerability to different attack scenarios can be evaluated, response plans can be formulated, and subsequent risk management decisions can be made to further mitigate the current exposure in the event of an attack.

(ASCE 78-24, Guidelines for the Physical Security of Water and Wastewater/Stormwater Utilities - Preface, Page ix)

Further sources of information and assistance:

- ❑ CISA – Cybersecurity & Infrastructure Security Agency, www.cisa.gov

CISA has curated a database of no-cost cybersecurity services and tools as part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments.

- ❑ US Environmental Protection Agency - https://www.epa.gov/cyberwater/epa-cybersecurity-water-sector

The EPA offers cybersecurity guidance and training for water and wastewater facilities, conducts cyber risk assessment, conducts cybersecurity exercises and provides technical assistance for drinking water and wastewater systems.

- ❑ Federal Bureau of Investigation

The FBI investigates terrorism and threats to critical infrastructure, including water systems. FBI recommends calling 911 first and then submitting information online via https://tips.fbi.gov/home or calling their local field office.

- ❑ INFRAGARD - https://www.infragard.fbi.gov/

INFRAGARD has many local chapters and contributes to water security by improving threat awareness, preparedness, and collaboration among infrastructure owners/operators and law enforcement.

Neo-Chloris

Thank you for attending!

Charles R. Stack, MPH, BCES, A.M. ASCE
Vice-President, NeoChloris Inc.
cstack@neochloris.com
www.neochloris.com