Protect Your Utility
What You Can Do to Prevent and Mitigate Hostile Events

CWWA NWWC – Niagara Falls, ON

November 14, 2023

Welcome

Charles Egli
Director of Preparedness and Response
WaterISAC

Alec Davison
All-Hazards Analyst
WaterISAC

Objective

Share best practices and lessons learned from real world experiences, including past incidents so that attendees can build or improve upon security and incident management policies at their utilities.

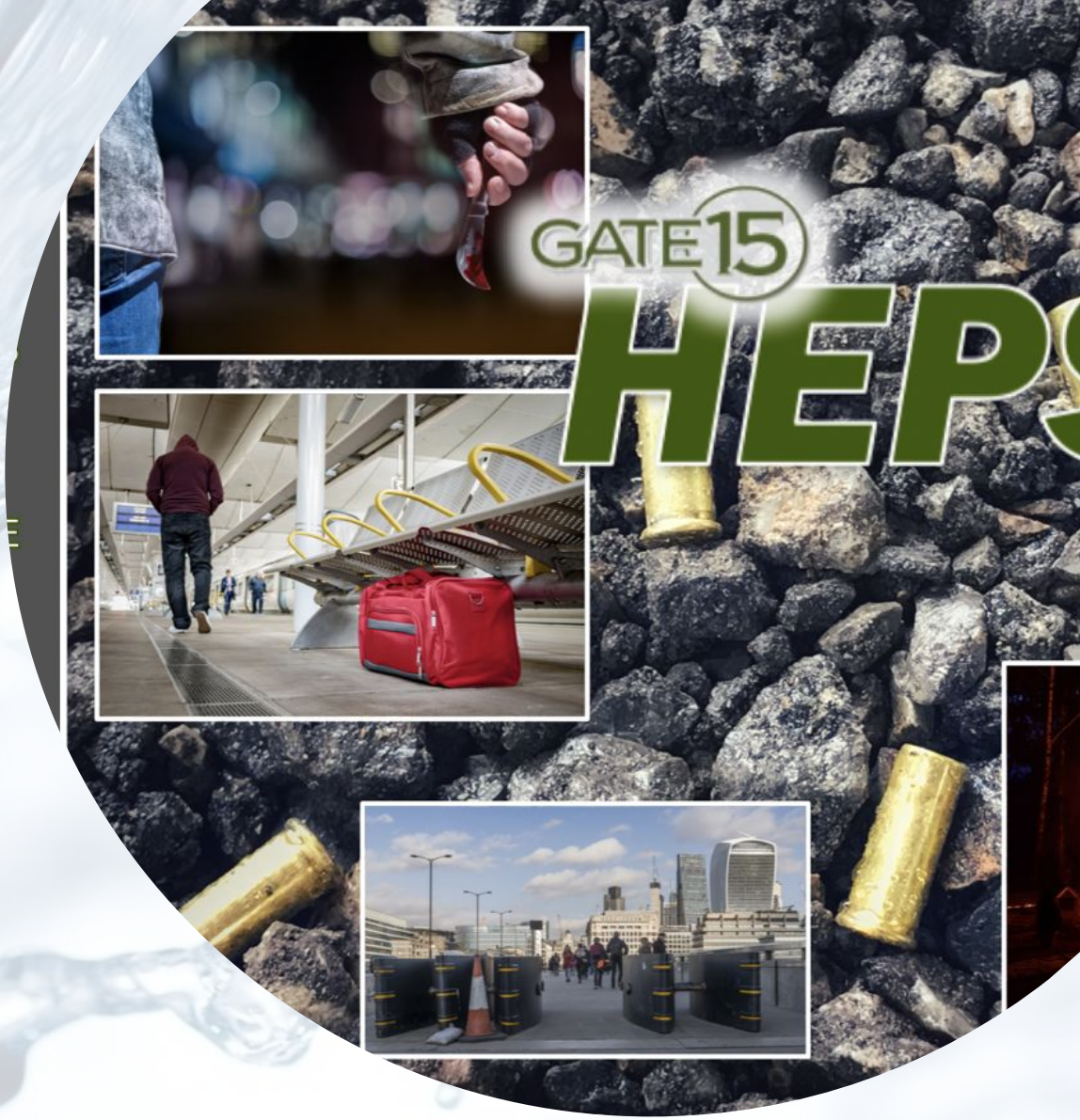
Session Structure

- This session will be conducted in **two modules**:
  - Module One: Selection & Surveillance & Attack Preparation
  - Module Two: Attack & Escape
- Each module will begin with a **situation update**.
- Facilitators will share **best practices**.
- Participants are invited to **comment and ask questions**.

Framing: Hostile Events Attack Cycle

- Hostile Events include **active shooter incidents**, **workplace violence** and **workplace attacks**, **lone actor** and **low-tech terrorism**, **complex coordinated terrorist attacks**, **fire as a weapon**, **weapons of mass destruction**, and other related activities.

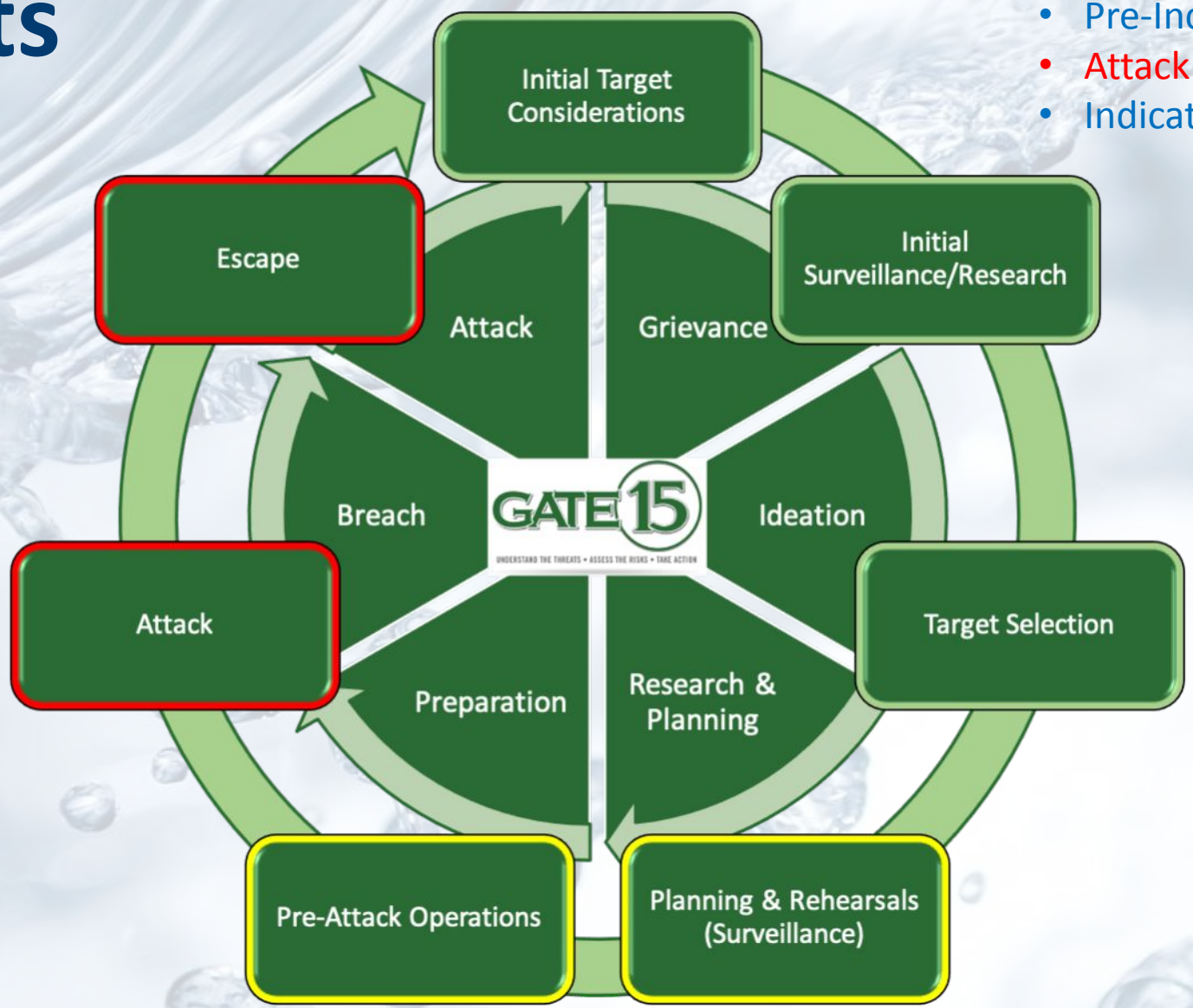
- Characterized by a variety of means, weapons, and tactics used to cause physical injury or death.



WATER ISAC

Hostile Events Attack Cycle

Module I:
- Selection & Surveillance
- Pre-Incident Preparedness
- Attack Preparation
- Indicators, Reporting



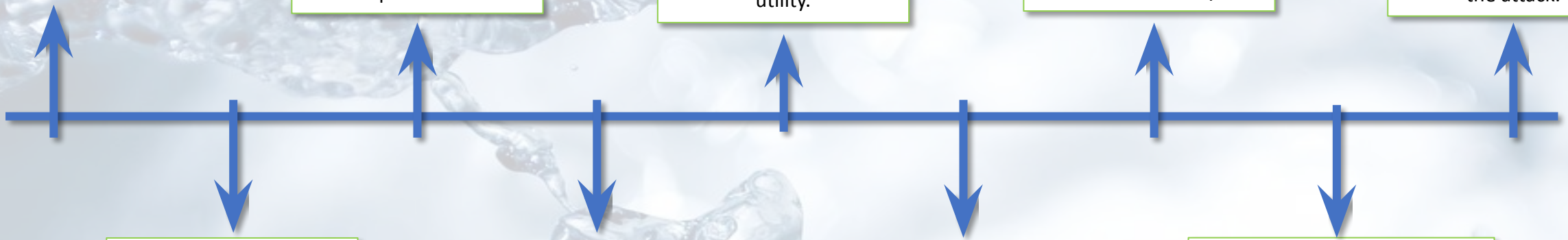
Module II:
- Attack & Escape
- Response, Immediate Actions

WATER ISAC

Module One

Selection & Surveillance & Attack Preparation

Selection & Surveillance & Attack Preparation - Timeline



January 2023
Jack Ryan is a disgruntled 34-year-old engineer at a water/wastewater utility.

January 2023
He recently created a website where he posts short rants and links, often expressing frustration with political issues, as well as affinity with neo-Nazi and white supremacist ideology.

February 2023
At work, Ryan neglected his responsibilities and began to spend time researching and posting about political issues.

March 2023
He joins a violent extremist run telegram channel where he starts communicating and exchanging ideas with other like-minded individuals.

May 2023
He continues to self-radicalize and communicate with users in the extremist Telegram channel, with whom he starts to plot an attack against his utility.

June 2023
Ryan starts conducting pre-operational activities, such as taking photos of sensitive areas and what he considers to be security vulnerabilities and posting them to the group chat.

August 2023
Assisted by other violent extremists in his group chat, Ryan engages in deliberate planning to attack his utility.

September 2023
He displays numerous suspicious activities, increasingly poor work performance, and irritability around others.

November 2023
Ryan gets into a fight with a coworker, ultimately resulting in him quitting. He decides to move up the date of the attack.

WATER ISAC

Hostile Events Preparedness

1. Are your personnel aware of the diverse threats your utility may encounter (e.g., Homegrown Violent Extremists, Domestic Violent Extremists, Racially Motivated Violent Extremists, Common Criminals).
    a. Do you receive and review threat, incident, and / or suspicious activity reports from local law enforcement, fusion centers, other government entities, or other partners?
    b. Are you working with neighboring utilities or other infrastructure organizations?

2. Are your organization's personnel trained to look for and report suspicious activities and potential pre-operational indicators?

Insider Threat Awareness

3. Do you have policies for reporting insider threats at your organization?
    a. Does your organization regularly train and/or remind employees about reporting insider threats?

4. Do you have policies regarding:
    a. Employees bringing firearms to work
    b. Photography of the utility

5. What are your procedures for employee termination and revoking access privileges?

Operational Preparedness

6. Would you share information about suspicious activities and incidents with partners (e.g., local law enforcement, fusion centers, WaterISAC)?

7. Are you working with hometown security partners – including law enforcement, neighboring utilities, and any other community organizations to develop and enhance preparedness?

    a. Have you conducted a physical security assessment?

Best Practices

- Email inbox for employees to report security issues
  - Insider Threat Mitigation (U.S. DHS)
  - U.S. Violent Extremist Mobilization Indicators 2021 (U.S. ODNI)
  - Nationwide SAR Initiative (U.S. DHS)

ELICITING INFORMATION
Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about an event or particular facets of a facility's purpose, operations, security procedures, etc.

TESTING OR PROBING OF SECURITY
Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities.

RECRUITING/FINANCING
Providing direct financial support to criminals and/or criminal/terror organizations; compiling personnel data, banking data, travel data, or contacts to build operational teams.

OBSERVATION/ SURVEILLANCE
Demonstrating prolonged interest in facilities, buildings, or infrastructure beyond casual or professional interest.

PHOTOGRAPHY
Taking pictures of persons facilities, buildings, or infrastructure in an unusual or covert manner.

MATERIALS ACQUISITION/ STORAGE
Acquisition and/or storage of unusual quantities of precursor materials (fuel, chemicals, toxic materials, timers, cell phones, or other triggering devices).

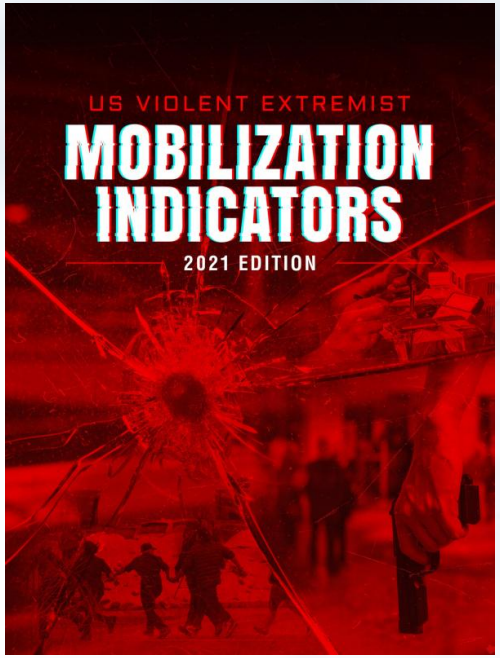
ACQUISITION OF EXPERTISE
Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities.

WEAPONS COLLECTION/ DISCOVERY
Collection or discovery of unusual amounts or types of weapons, explosives, chemicals, or shows evidence of, detonations or other residue, wounds, or chemical burns.

SECTOR-SPECIFIC INCIDENT
Actions associated with a characteristic of unique concern to specific sectors (e.g., the education, public health, government, etc.), with regard to their personnel, facilities, systems, or functions.

Source: U.S. DHS National Threat Evaluation and Reporting Office Presentation

Source: C. Egli



Source: U.S. ODNI

WATER ISAC

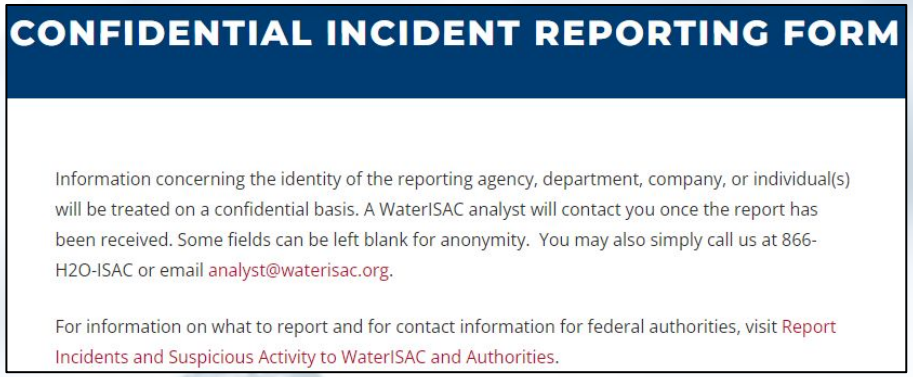
Best Practices

- Utility plans and policies
  - Insider threat, workplace violence, emergency response, drone
  - Prohibited items policy
  - Employee separation protocol
    - Retrieve/disable badges
    - Periodic badge audit
    - Utility-wide notice
    - Contractor challenges

Source: U.S. Navy

Best Practices

- Participation in information sharing communities (fusion centers, local law enforcement, other utilities, ISACs)
  - Royal Canadian Mounted Police
  - WaterISAC reporting tools
    - Call 1-866-H2O-ISAC (1-866-426-4722)
    - Email analyst@waterisac.org
    - Submit a report online
- Physical security assessments



Source: WaterISAC

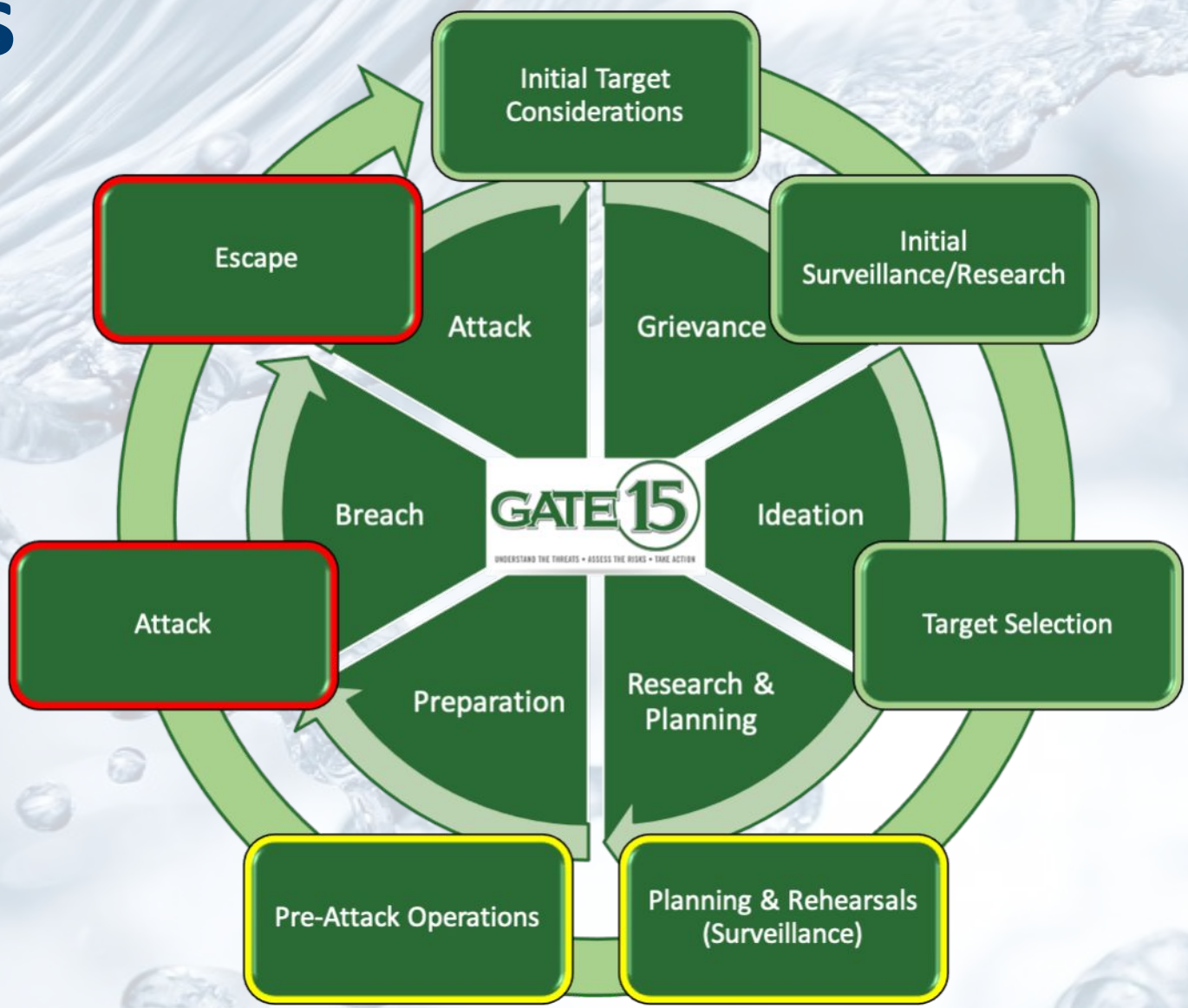
Module Two

Attack & Escape

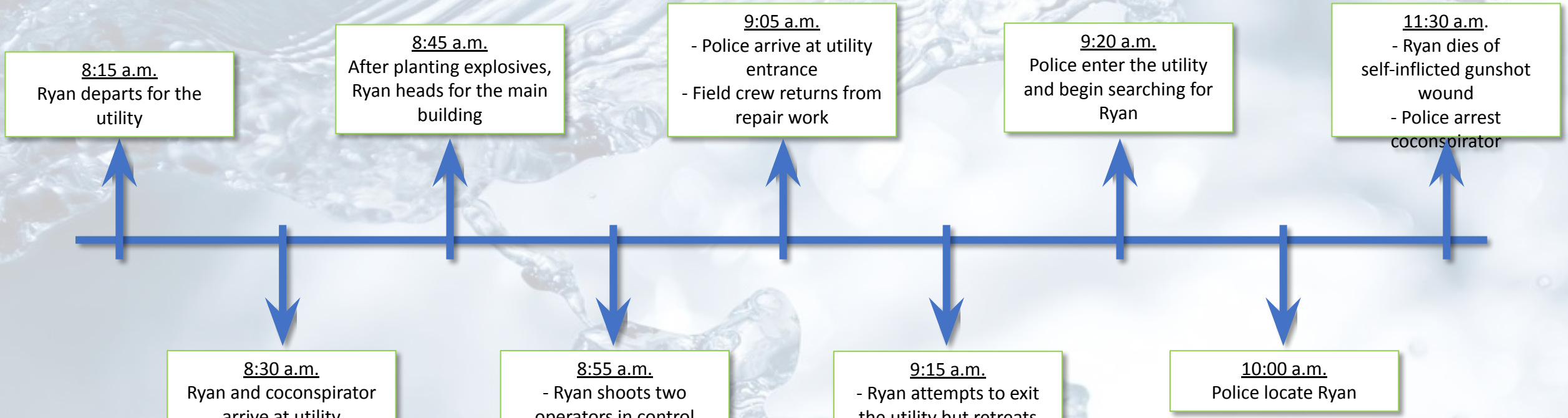
Hostile Events Attack Cycle

Module II:

- Attack & Escape
- Response, Immediate Actions



Attack & Escape - Timeline



Hostile Events Response

1. What security measures (equipment, technology) do you have in place to counter the threat and reduce the risks of hostile events?

2. What kind of access controls/barriers do you have at your facility?
   a. Can the public easily enter your facility?

3. To what extent have you coordinated with law enforcement beforehand?
   a. Site familiarization
   b. Key card access and use

Operational Response

4. Do you have a security team at your facility?
   a. If not, who provides security?

5. How do you communicate incidents (from spills to hazards to incidents and attacks) within your organization?

6. Have your utility's personnel been trained on how to respond to an active shooter incident?
   a. Do you conduct exercises?
   b. Have they been trained in basic first aid?

Best Practices

- Specialized training
  - Active shooter response (e.g., ALICE)
  - STOP THE BLEED (American College of Surgeons)

Source: StoptheBleed.org

Best Practices

- Crisis communications
  - Employee emergency alert system (e.g., Everbridge)

Source: Ready.gov

Best Practices

- Working with local law enforcement
  - Additional training and exercise opportunities
  - Facility walk-throughs
  - Use of facilities for training, including by SWAT teams
  - Key box (e.g., KnoxBox®)

Source: Wikimedia Commons

Source: The Knox Company

Sector Areas for Improvement

- Ability to monitor social media
- Threat awareness
  - Contract security and high turnover rate
- Thresholds for information sharing
- Regular training and exercises

Other Challenges

- Responding to:
  - A HAZMAT release
  - Manipulation of the treatment process
- Infrastructure/equipment vulnerabilities to gunfire
- Security of remote facilities
- Physical layout of facility available on the Internet
- Visitors
- Recovery

Intentional Attacks on North Carolina Electric Substations Result in Power Disruptions for Thousands (WaterISAC)

Source: The News & Observer

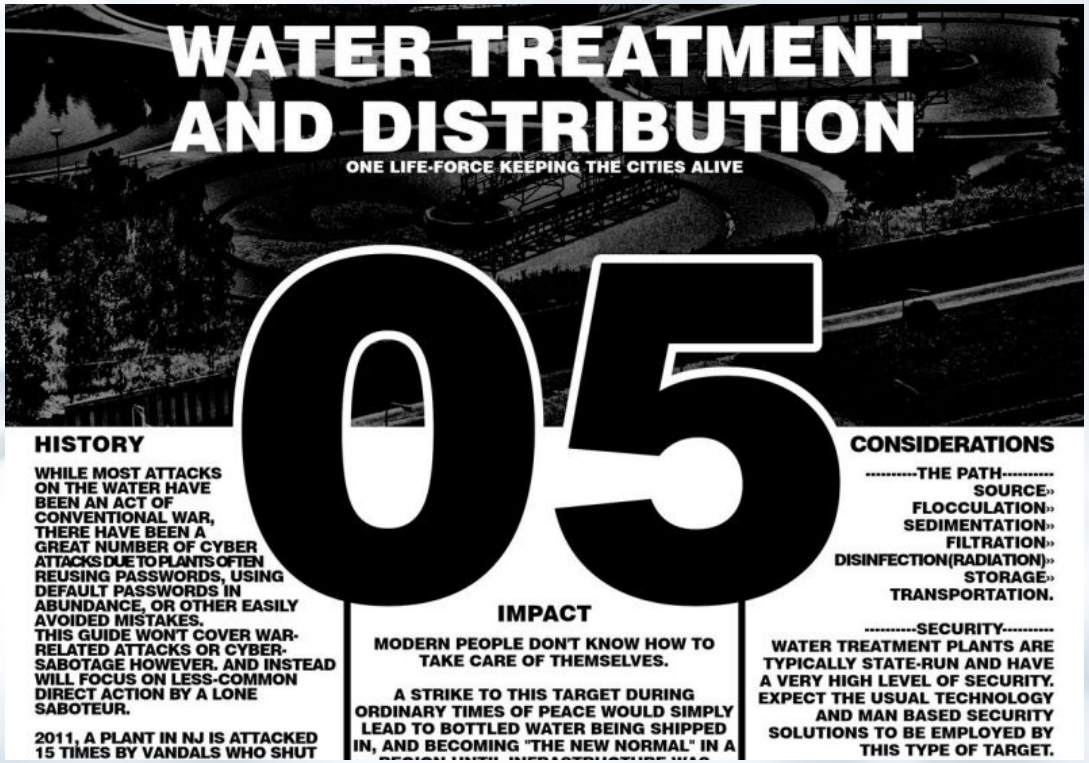
WATER ISAC

Notable Terrorist/Extremist Plots and Incidents involving the Sector

- Feb. 2014: Georgia – Plot by militia members to trigger violent conflict against the government by attacking water utilities.
- Jun. 2018: Wisconsin – An Islamic State supporter used a pro-Islamic State social media account to encourage a suspected Islamic State follower to poison water reservoirs with ricin.
- Nov. 2021: Maryland – Members of the neo-Nazi group "The Base" were sentenced to nine years in prison for planning to poison water supplies and engage in other terrorist activities.
- Jun. 2021: Unknown – Domestic violent extremists shot at a purported water treatment plant in a video.

Violent Extremist Publications

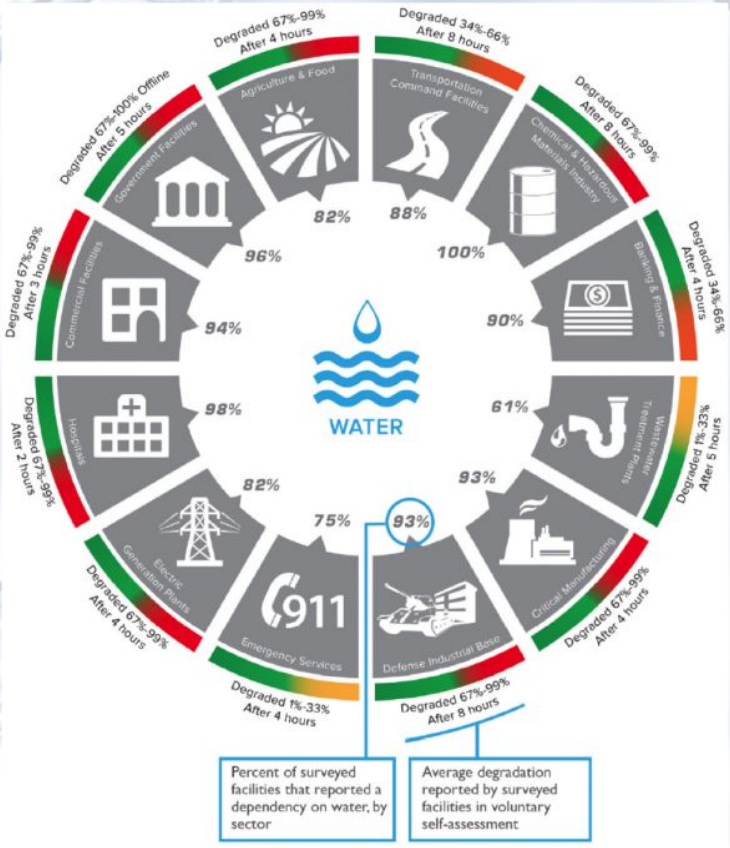
- Militant Accelerationism
- Make It Count: A Guide for the 21st Century Accelerationist
- Do it For the ‘Gram
- The Hard Reset



Other Critical Infrastructure Sectors

- Dec. 2022: North Carolina Substation Attacks
- Apr. 2023: “How To Blow Up A Pipeline” Film
- Jun. 2023: Idaho/Oregon Dam Attacks

Source: City of Virginia Beach, Virginia



Source: U.S. NIAC, July 2016

WATER ISAC

Additional Resources

- National Strategy on Countering Radicalization to Violence (Public Safety Canada)
- Prevention and Intervention Programs (Public Safety Canada)
- Active Shooter Preparedness (U.S. Cybersecurity and Infrastructure Security Agency)
- Know the Signs: A Guide for Identifying Signs of Violent Extremism (New Zealand Security Intelligence Services)
- Hostile Event Attack Cycle (Gate 15)

Questions and Comments?

Contact information

60-DAY FREE MEMBERSHIPS AVAILABLE!

Chuck Egli
Director of Preparedness and Response
egli@waterisac.org

Alec Davison
Analyst
davison@waterisac.org

Website | www.waterisac.org
Incident Reporting Form | https://www.waterisac.org/report-incident
24 Hour Line | 866-H2O-ISAC
Email | analyst@waterisac.org

Thank you!