2-1-2019

Jack Voltaic 2.0: Threats to Critical Infrastructure

Judy Esquibel
Army Cyber Institute

Erica Mitchell
Army Cyber Institute

JACK VOLTAIC 2.0

Threats to Critical Infrastructure

PREPARE ■ PREVENT ■ RESPOND

Executive Summary

Increasingly connected, ready to respond

Although digital connectivity has made our infrastructure more efficient, it has made it more vulnerable to attack. As a result, infrastructure resilience is more critical today than ever before. Cyberspace attacks rarely affect a single target; instead their effects, anticipated and unanticipated, ripple across interconnected infrastructure sectors. Differing abilities to recognize a cyberspace attack, limited information sharing, varying defense capabilities, and competing authorities complicate the response. These gaps in cybersecurity leave our Nation vulnerable to exploitation by a determined adversary.

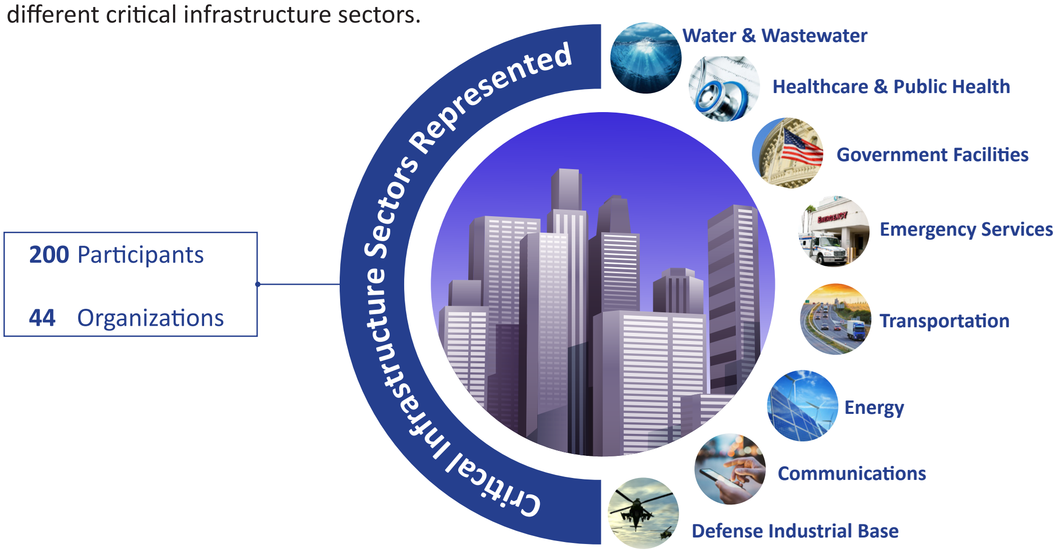
The Jack Voltaic 2.0 Cyber Research Project is an innovative, bottom-up approach to developing critical infrastructure resilience. Developed by the Army Cyber Institute at West Point and hosted by the City of Houston, in partnership with AECOM and Circadence, this research assembled critical infrastructure partners to study cybersecurity and protection gaps.

ARMY CYBER INSTITUTE AT WEST POINT

AECOM

SUMMARY

From the 24th to the 26th of July 2018, the City of Houston, in partnership with the Army Cyber Institute, AECOM, Circadence, the State of Texas, federal agencies, and regional public and private sectors, conducted the Jack Voltaic (JV) 2.0 Cyber Research Project. Its execution was the culmination of 13 months of planning, with the purpose of observing and assessing the ability of interdependent, critical infrastructure sectors to respond to combined cyber and physical attacks. The event involved 44 organizations and 200 participants from eight different critical infrastructure sectors.



JV 2.0 was an innovative, bottom-up approach to critical infrastructure resilience. The project assembled critical infrastructure partners to conduct a research experiment to identify gaps in critical infrastructure cybersecurity. The experiment employed a cyber exercise involving players from multiple sectors (noted above). The JV 2.0 Governance and Planning Committee, comprised of representatives from across eight critical infrastructure sectors, met to express their security priorities. Through analysis of their perceived strengths and weaknesses, participants tailored the exercise to stress specific aspects of their incident response and disaster recovery plans.

Senior leaders from public and private organizations observed the exercise and discussed efforts for improving cyber resiliency. Representatives from the following organizations were present: Military – Army Cyber Institute, United States Army North (Fifth Army), Texas National Guard; City of Houston – Mayor's Office of Public Safety and Homeland Security, Houston Police, Houston Information Technology Services, Greater Houston Partnership Cyber Task Force, Houston Police; Industry – AECOM.

BACKGROUND

The Army Cyber Institute (ACI) is an outward-facing, partnership think tank of the United States Military Academy located at West Point, New York. The ACI commissioned this study to enable the Army's ability to leverage strategic partnerships and to develop a proof of concept. The need to evolve defense of the Department of Defense (DoD) Information Network entails understanding the role of the military in addressing a cyberspace attack by identifying the gaps and redundancies within responses. JV research includes exploration of how to synchronize DoD/United States Government and private sector capabilities in a cyberspace attack response.

The ACI is recognized in academia for its strategic-level thinking and served predominately as an advisor and facilitator for the JV 2.0 exercise. The idea for JV originated from a workshop conducted by the ACI in April 2016 known as the Cyber Mutual Assistance Workshop (CMAW).[1]

Jack Voltaic 1.0 – New York City: JV 1.0, the predecessor exercise to JV 2.0, was an ACI-led experiment conducted in August 2016 in the form of a cyber exercise developed alongside industry partner Citigroup to examine interdependencies among critical infrastructure. The ACI accomplished this by assessing the performance of the federal, state, and local governments, as well as the private industry, in the event of a "Cyber Worst Day" scenario.

U.S. ARMY INTEREST

To achieve its cyberspace vision, the U.S. Army must synchronize research efforts with a myriad of partners and focus them on challenges of mutual concern. The ACI enables the Army to collaborate in creative ways with industry and academic leaders and institutions, cybersecurity research centers, and policy groups. These partnerships critically enhance Army cyberspace operations.

- **Enable U.S. Army Readiness** – JV 2.0 enabled readiness across the U.S. Army and the Nation by researching the interdependencies among the Army and the DoD, industry, and local and state governments. The ACI developed and coordinated partnerships with industry, the City of Houston, and other regional partners, who joined advisors and participants from the U.S. Army Cyber Command, U.S. Army North, the Army Reserve, and the National Guard. Key partners from the private sector included AECOM and Circadence.
- **Reserve and Guard Integration** – JV 2.0 explored the employment of the Reserve and National Guard to defend the Nation by leveraging military cyber capabilities in its domestic response to cyberspace attacks. Integration of these capabilities allowed participants to gain a better understanding of how policies and legal authorities affect military responses to a cyberspace attack and develop policy recommendations. Potential gaps in skills, training, and equipment were identified to develop best practices. This framework explored how partnerships that leverage the insights and innovations of the public and private sectors can enhance Army cyberspace operations.

PURPOSE

JV 2.0 was an innovative plan to enhance U.S. military superiority by leveraging municipal and corporate partners to better understand unified land operations in megacities. The outcome of JV 2.0's research provided awareness and filled gaps regarding the impacts of a severe cyber event or persistent cyberspace attack against the critical infrastructure that supports major U.S. metropolitan areas.

SCOPE AND RESEARCH OBJECTIVES

JV 2.0 was an exercise event that demonstrated a physical attack and a cyberspace attack originating in Harris County, Texas, which impacted multiple critical infrastructure sectors in and around Harris County and the City of Houston, Texas. Research objectives included the following:

- Develop a framework to exercise a city's ability to respond to a multisector physical attack and cyberspace attack and to assess the ability of an urban Defense Industrial Base to respond to this type of attack.
- Showcase the City of Houston as an emerging national leader in cyber incident response.
- Evaluate and examine the U.S. military's cyber protection capabilities.

[1] Cyber Mutual Assistance Workshop Technical Report, Carnegie Mellon University Software Engineering Institute, February 2018, CMU-SEI-2018-SR-007.

DESIGN CONCEPT

For the exercise design, JV 2.0 involved planners from each organization who provided input into the development of a realistic, threat-based scenario which focused on local concerns. Both a live-fire exercise (LFX) and a tabletop exercise (TTX) provided an opportunity to explore cyber-related legal and policy issues while necessitating participation from both senior business and local government leadership. Military participation contributed to better understanding of the role of Reserve and Active components in tiered responses to major cyberspace attacks. The inclusion of essential federal partners such as the Department of Homeland Security (DHS) was critically important to the exercise's success.

COMPONENT 1
Governance and Planning Committee

- Trusted agents
- Planners knowledgeable in cyber and emergency planning procedures
- Members are representatives from their sector

COMPONENT 2
Tabletop Exercise (TTX)

CORRELATE

COMPONENT 3
Live-Fire Exercise (LFX)

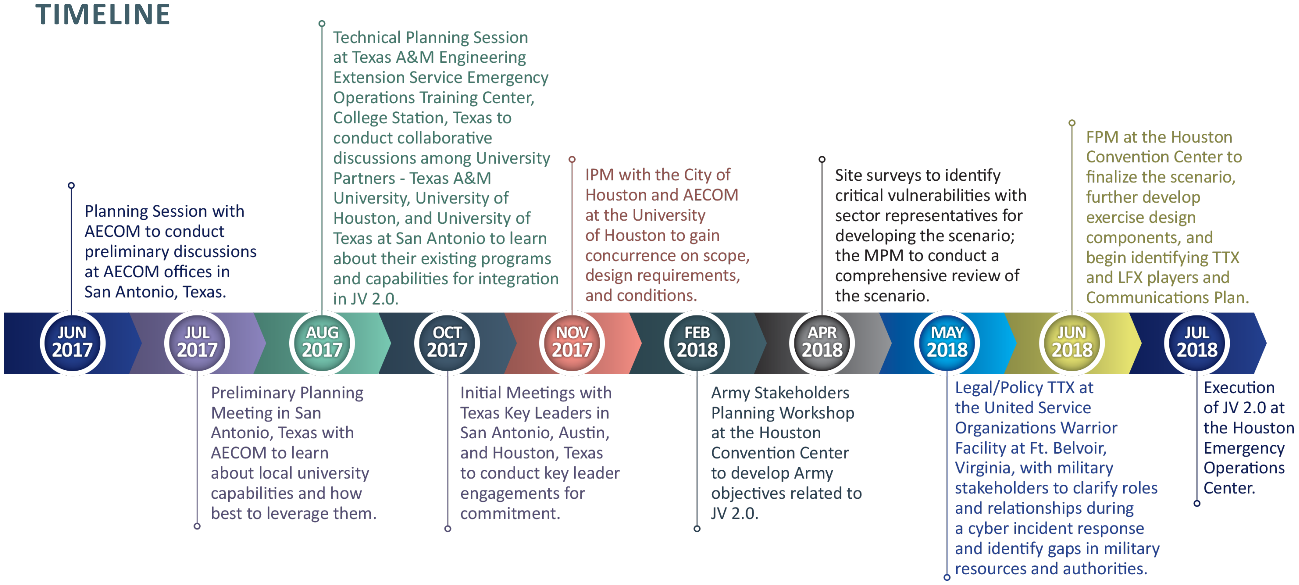
Notes: The exercise consisted of three components:
Component 1: The Governance and Planning Committee was comprised of representatives from sector-specific, critical infrastructure organizations. Committee members, also known as "trusted agents," were key to successful development and execution.
Component 2: TTX was a simulated and facilitated discussion based on a scenario that took participants through the process of dealing with a physical disaster blended with cyberspace attack events.
Component 3: LFX was an exercise that was comprised of an on-range, simulated virtual environment. The LFX scenario correlated with the TTX scenario. The LFX was used to test cyber equipment and response capabilities in real time.

The design integrated concepts from several existing cyber exercise frameworks. In general, there are three levels of players involved in an exercise. JV 2.0 focused on operational and mid-level players.

- **Category 3: Senior Executives** – senior leaders (*e.g., senior executive and general officer players*)
- **Category 2: Mid-level Management** – first-line supervisors (*e.g., TTX players*)
- **Category 1: Operational** – analysts and operators (*e.g., virtual range/LFX players*)

Cyber exercises are hindered by being too technical or too high-level, where managers, operators, and technical personnel are physically separated. JV 2.0 was designed to incorporate elements of both the LFX and the TTX, mimicking a real-world response in which mid-level managers would respond to threats detected by operators and disseminate threat intelligence received from peer organizations to operators. This approach ensured collective cybersecurity training and enhanced cross-sector information sharing practices, including coordinated, technical-level threat intelligence sharing.

TIMELINE



JUN 2017
Planning Session with AECOM to conduct preliminary discussions at AECOM offices in San Antonio, Texas.

JUL 2017
Preliminary Planning Meeting in San Antonio, Texas with AECOM to learn about local university capabilities and how best to leverage them.

AUG 2017
Technical Planning Session at Texas A&M Engineering Extension Service Emergency Operations Training Center, College Station, Texas to conduct collaborative discussions among University Partners - Texas A&M University, University of Houston, and University of Texas at San Antonio to learn about their existing programs and capabilities for integration in JV 2.0.

OCT 2017
Initial Meetings with Texas Key Leaders in San Antonio, Austin, and Houston, Texas to conduct key leader engagements for commitment.

NOV 2017
IPM with the City of Houston and AECOM at the University of Houston to gain concurrence on scope, design requirements, and conditions.

FEB 2018
Army Stakeholders Planning Workshop at the Houston Convention Center to develop Army objectives related to JV 2.0.

APR 2018
Site surveys to identify critical vulnerabilities with sector representatives for developing the scenario; the MPM to conduct a comprehensive review of the scenario.

MAY 2018
Legal/Policy TTX at the United Service Organizations Warrior Facility at Ft. Belvoir, Virginia, with military stakeholders to clarify roles and relationships during a cyber incident response and identify gaps in military resources and authorities.

JUN 2018
FPM at the Houston Convention Center to finalize the scenario, further develop exercise design components, and begin identifying TTX and LFX players and Communications Plan.

JUL 2018
Execution of JV 2.0 at the Houston Emergency Operations Center.

Lieutenant General (Ret.) Rhett Hernandez, United States Military Academy Cyber Chair, provides opening remarks at the JV 2.0 Legal Policy TTX in Fort Belvoir, Virginia.

FINDINGS AND RECOMMENDATIONS

- **Finding #1**: Growing physical and cyber risk to cities requires a different framework for risk mitigation due to current frameworks being inadequate to meet the changing and growing threat to urban communities. For the Nation to defend itself, U.S. cities need an adaptable and scalable model to improve the cybersecurity posture. A bottom-up approach is required to integrate a risk management framework that is replicable and adaptive to the rapidly evolving threat to urban communities.

  Cyberspace attacks can quickly overwhelm unprepared governments, in light of their limited resources. According to a 2016 cybersecurity survey[2], only 33 percent of local governments had a formal, written cyber incident response plan. In February and March 2018, ransomware attacks seriously impacted online services in Atlanta; 911 dispatch services in Baltimore; and government networks in Davidson County, North Carolina. This demonstrated the need for increased preparedness.

  » **Recommendation**: The JV approach can serve as a learning system and development effort. Undertake a series of JV exercises and hold educational workshops and conferences in key cities and localities to identify vulnerabilities, develop solutions, propose actions, and share best practices.

  » **Recommendation**: The Federal Emergency Management Agency (FEMA), DHS, DoD, and the Department of Energy (DOE) should work together to develop a campaign to integrate the JV risk incident response model into an exercise framework at the national level (i.e., collaboratively among DHS, DoD, and DOE). Ensure that military reserve component forces are incorporated as part of this effort.

  » **Recommendation**: Develop technology offerings that enable the scaling of the JV 2.0 LFX component, in support of the National Defense Authorization Act Section 1649 - Pilot Program on Modeling and Simulation in Support of Military Homeland Defense Operations in Connection with Cyber Attacks on Critical Infrastructure.

  » **Recommendation**: States, cities, and localities should seek research and development support from the Executive Branch and Congress to develop appropriate systemic approaches to cybersecurity.

  » **Recommendation**: Municipal and local cybersecurity efforts should better integrate the private sector, particularly critical infrastructure (e.g., electric grid, telecoms, water, and transportation). Public-private partnerships should evolve (i.e., move beyond service-level agreements) to induce a cultural change in the building of trusted relationships and working together.

[2] https://icma.org/documents/cybersecurity-survey-snapshot

FINDINGS AND RECOMMENDATIONS

- **Finding #2**: The U.S. military and its allies are dependent on civil and commercial infrastructure. U.S. infrastructure requires greater protection due to its vulnerability to sophisticated physical and cyberspace attacks.

  While military installations have their own internal critical infrastructure providers, they still rely on service delivery from outside of the installations' boundaries. For example, electrical service is delivered through commercial providers to the installation, where it is distributed by the internal utility company. In the event that the commercial provider cannot supply electricity, an installation can only run on backup power for a finite period, and generally does so at a diminished capacity.[3]

  » **Recommendation**: Improve Transportation and Maritime Sector Cybersecurity[4] by collaborating with the Office of the Secretary of Defense (OSD), the Joint Chiefs of Staff (JCS), and related Combatant Commands to develop an operational risk management framework that better enables the protection of critical force protection elements. Ensure collaboration and planning include the Reserve, the National Guard, DHS, and DOE.

  » **Recommendation**: Work with allies to develop similar integrated protection frameworks in transload areas abroad and with frontline states. As a starting place, develop these efforts within the North Atlantic Treaty Organization (NATO) through the development of support networks.

- **Finding #3**: National Guard units are providing physical security to support cities and developing cyber capabilities. State military departments are currently working to evolve cyber response processes (including partnership strategies) and capabilities more rapidly.

  For example, the Major General Tim Lowenberg National Guard Cyber Defenders Act has been proposed to create National Guard Civil Support Teams that serve at the discretion of state governors.[5] If passed, the act may provide a mechanism and funding to assist local authorities in establishing these teams and thereby bridge federal and non-federal response efforts during cyber incidents.

  » **Recommendation**: As cyber response procedural handbooks are developed, they should be shared across state military departments. Train the National Guard on procedures and assess the effectiveness of U.S. Northern Command, U.S. Cyber Command, and FEMA exercise programs.

  » **Recommendation**: The DoD should maintain an inventory of existing and emerging, critical, National Guard and Reserve, cyber capabilities, which could be leveraged by state military departments, thereby enabling better coordination between DoD and DHS. These capabilities should be tracked as they are developed.

- **Finding #4:** States play a critical role in supporting municipal responses to physical and cyber events. States must develop campaign plans for more scalable incident responses and rapid information sharing. Several states are in the process of establishing fusion centers and Information Sharing and Analysis Organizations (ISAOs).

  As an example, the State of Connecticut issued the Connecticut Cybersecurity Strategy in 2017 and the Cybersecurity Action Plan in 2018. The plan includes sections for state government, municipal governments, business, higher education, and law enforcement to address the following goals: cyber literacy, preparation, response, recovery, communications, and verification. In addition, other states (e.g., California, Maryland, Michigan, New Jersey, New York, Texas, Virginia, and Washington) have also emerged as leaders within the cybersecurity realm, setting examples for other states to follow.[6]

  » **Recommendation**: Develop, fund, and implement state-wide incident response campaigns that leverage the JV 2.0 model. Working with other state agencies and community leaders, state emergency response coordinators should lead this effort and serve as the central resource for cities and localities in requesting assistance from state and federal governments.

  » **Recommendation**: DHS and associated, sector-specific agencies should ensure that DHS maintains accountability of these new assets e.g., ISAOs, as they develop to evolve information sharing and ensure state and local homeland protection. Moreover, the DoD should have the ability to leverage this capability to evolve campaign plans to defend the Nation.

» **Recommendation**: Leverage best practices and lessons learned from the financial sector's Financial Systemic Analysis & Resilience Center (FSARC) to implement a similar model at the local and state levels. Over time, integrate municipalities into the Intelligence Community process.

[3] https://www.defensenews.com/pentagon/2017/11/29/pentagon-weighs-new-requirements-to-secure-militarys-vulnerable-power-grid

[4] The National Cyber Strategy of the United States of America, The White House, September 2018, pg. 9.

[5] https://www.congress.gov/bill/115th-congress/house-bill/3712/all-info?r=60

[6] https://sentinelips.com/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf

FINDINGS AND RECOMMENDATIONS

- **Finding #5**: Policy and legal authorities at the federal and state levels do not sufficiently empower cities to respond to cyber incidents. Policies and authorities need to be reviewed and adjusted to better help cities defend against sophisticated physical and cyber threats. Currently, the exploration of cyber mutual assistance is only practiced within the energy sector.

  In the course of the legal and policy TTX, key issues and shortfalls in current Defense Support to Civil Authorities surfaced. Additionally, the panel found that policies were inadequate (e.g., cyber mutual assistance through National Guard and industry sectors across state lines). Additional progress is needed for continuously assessing comprehensive physical and cyber risk to cities and military installations.

  » **Recommendation**: Joint military organizations (e.g., National Guard Bureau) should explore possibilities in cyber mutual assistance practice. This would involve developing policy and associated implementation guidance that would enable more proactive and sustained national military support to cities and localities defending against physical and cyberspace attacks.

  » **Recommendation**: Support appropriate policy and implementation guidance development for local communities and state and national organizations. Annually develop and update the national intelligence assessment of the cyber capabilities of nation-state and terrorist adversaries who exploit predictable natural and threat-based, human-generated events. The newly-created DHS National Risk Management Center and the Cybersecurity and Infrastructure Security Agency (CISA) should also be engaged.

- **Finding #6**: The private sector is affected by sophisticated, adversarial, cyber threats. The private sector can inform, develop, and provide solutions that benefit the public sector.

  The private sector is frequently targeted by adversaries looking to profit from breaches. These attacks can result in a significant loss of business intelligence and intellectual property; therefore, establishment of a public-private partnership and increased regulation is essential. In addition, profit is not our adversaries' only motive, as evidenced by the misinformation campaign during the 2016 U.S. presidential election and the Sony Pictures cyberspace attack. The private sector has incentives to cooperate with public and other private sector companies in the name of increased security.[7]

  » **Recommendation**: Key private sector representatives across multiple infrastructure sectors should gather (often) in a single group to learn about and receive the same answers and thereby understand the appropriate context.

  » **Recommendation**: Further explore the idea to create private sector "certified defenders" who have significant cybersecurity capabilities and who would work under government authorization to help prepare for and respond to adversarial cyber threats.

ACADEMIC FINDINGS

- Although the JV series has helped make significant strides in critical infrastructure and public-private partnership research, future research should focus on remaining gaps, such as coordinating among jurisdictions, entities, and governments.
- To improve upon the success of the JV series, the project should develop a cyber education program. This program should incorporate cybersecurity lessons learned and be shared with the wider community. The impact of this educational program on exercise performance should be measured.
- To better understand incident identification, communication, and response, as well as improve strategic cyber decision-making, integration must be strengthened between information technology and operational technology (IT/OT) personnel and senior leadership must be included as participants in future research.
- Data collection (obtained from cyber-ranges) procedures and metrics need further exploration. As primarily qualitative research, observers and evaluators should collect the majority of data throughout the JV series, with a focus on collecting consistent, nonattributable data to inform a replicable framework for future critical infrastructure research. Additionally, exploration of an increased role of quantitative data collection may provide further insights.
- Research efforts should be dedicated to better understanding today's workforce skillsets for identifying gaps. An example: the energy, water, chemical, and Defense Industrial Base sectors all rely on Industrial Control Systems which are becoming more connected to the Internet. As these systems continue to modernize, this will introduce vulnerabilities through the radio frequency spectrum. The United States will continue to remain challenged to train a workforce in these blended environments. Training must become more available and affordable. With the advent of the Internet of Things (IoT), the required skillsets (i.e., the blending of cybersecurity with IT/OT and radio frequency) related to these technologies have yet to be identified.

[7] https://www.mindpointgroup.com/wp-content/uploads/2014/08/Impact-of-Cyber-Attacks-on-the-Private-Sector.pdf

WAY AHEAD

- Educate others and scale research and exercise activity with follow-on JV work.
- Partner with the Armed Forces Communications and Electronics Association (AFCEA) for follow-on public awareness activities.
- Work with stakeholders to address findings and operationalize recommendations.
- Develop and publish academic reports concerning cyber threats and responses.

ACRONYMS

ACI	Army Cyber Institute
AFCEA	Armed Forces Communications and Electronics Association
CMAW	Cyber Mutual Assistance Workshop
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
FEMA	Federal Emergency Management Agency
FSARC	Financial Systemic Analysis & Resilience Center
IoT	Internet of Things
ISAO	Information Sharing and Analysis Organizations
IT	Information Technology
JCS	Joint Chiefs of Staff
JV	Jack Voltaic
LFX	Live-Fire Exercise
NATO	North Atlantic Treaty Organization
OT	Operational Technology
TTX	Tabletop Exercise