Soldiers, Airmen, National Guard State Partnership Program (SPP) partners, and civilian cyber professionals train together during Cyber Shield 2025 at the Virginia National Guard's State Military Reservation in Virginia Beach, VA, on June 11, 2025. (U.S. Army National Guard photo by Master Sgt. Arthur M. Wright)

Leveraging AI for a Decisive Cyber Advantage

By CW4 Rory J.H. Rankin

The technological advancement of Artificial Intelligence (AI)/Machine Learning (ML) remains fluid globally, which poses a constant challenge for the U.S. Army to keep pace throughout the competition, crisis, and conflict phases. To dynamically exceed action at the speed of war, we must excel in the AI/ML space to secure, defend, and protect the homeland against our adversaries through digital modernization. One of the most critical homeland assets to protect and defend is our Critical Infrastructure/Key Resources (CI/KR) and Operational Technology (OT) across all military and commercial domains. Recent cyber attacks that triggered societal panic include the Colonial Pipeline by Darkside from Russia and China's dual threat (Salt and Volt Typhoon) cyber-attacks on our power grids, water systems, ports, and telecommunications (CSIS, 2025). In response, we need to achieve digital modernization with agility at a dynamic pace to counter these cyber-attacks against our critical infrastructure. Artificial Intelligence can identify Indicators of Compromise (IOC) and Malicious Cyber Activity (MCA) at a faster pace than human speed, thereby preventing future cyber threats before they can become cyber attacks.

So, What is AI/ML?

Artificial Intelligence (AI) is only as good as the respective Machine Language (ML) and Learning Language Models (LLM) with accurate corresponding metadata it captures and feeds AI to self-learn. ML provides the core computing, reasoning, and data analytics that allow AI to predict correctly and to automate but not replace human intelligence. AI can integrate data analytics efficiently while collaborating with an agile and clear strategic approach. However, in some instances, such as advanced drones, AI/ML has reached full autonomy to self-learn and will only exponentiate in the future (Read, 2023).

Examples of Cyber Attacks

Several cyber attacks have paralyzed critical infrastructure and fall under several names such as Critical Infrastructure/Key Resources (CI/KR), Industrial

Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA), and what is now known as Operational Technology (OT) (FEMA, 2008). These cyber attacks include:

- Stuxnet in June 2009 was an offensive OT-targeted cyber attack by U.S. and Israel to target the programmable logic controllers (PLCs) of the gas centrifuges making them overheat, thereby shutting down the Natanz Nuclear Facility in Iran (CSIS, 2025).

Note: Congress just concluded a hearing on July 22, 2025, stating that our nation is not ready for a large-scale OT-targeted cyber-attack (Ribeiro, 2025).

- In 2015, Ukraine became a testing ground for cyber-attacks by Russia.
- Sandworm in 2016-2017 by Russia, which shut down 60 Ukrainian power substations causing 250,000 people to be with no electricity (CSIS, 2025).
- In Southeastern U.S. in May 2021, Colonial Oil Pipeline suffered a $4.4 million ransomware loss, resulting in policy updates with Executive Order 14028, which modernized safeguards and incident response (CSIS, 2025; Driscoll & George, 2025).
- Volt Typhoon from 2021 is a state-sponsored cyber-threat actor linked to China that has targeted energy, transportation, and water OT networks (CSIS, 2025).
- In November 2024, Salt Typhoon, also from China, breached 8 telecom providers. However, since 2019, more than 80 countries have been targeted (Times of India World Desk, 2025).

Overall, China's two-pronged strategy (Salt/Volt Typhoon) exploited vulnerabilities in our legacy OT technology that has no redundancy with vulnerable 3rd-party vendors.

Note: Center for Strategic and International Studies (CSIS) in February 2025 noted that China has increased OT-related cyber-attacks by 300% in 2024 (CSIS, 2025).

- Russia in January 2024 hacked residential webcams in Kiev, Ukraine, to gather information on critical infrastructure.

Overall, Russian cyber-attacks on Ukraine's critical infrastructure surged 70% in 2024, with 4,315 incidents targeting critical infrastructure (CSIS, 2025).

Following the February 28 strikes on Iran and the escalating conflict in the Middle East, the global-threat environment has shifted. Most of the commentary circulating right now focuses on IT-facing threats. The question that matters for operators of power grids, water systems, oil and gas pipelines, and manufacturing facilities is different: What does this escalation mean for OT and ICS? Dragos conducted an intelligence briefing on March 12, 2026, on Iranian Cyber Nation State Actors and hacktivist activity with demonstrated OT/ICS capabilities and how to defend and prioritize OT/ICS threat environment (Messare, 2026).

How do We Secure Critical Infrastructure?

Cybersecurity requires continued coordination between local network defenders (LND), mission owners (MO), and Cybersecurity Security Providers (CSSP) to continue to have the persistent, continuous monitoring tools automated by AI that help identify anomalies rapidly before anomalies are handed over to DCO for further forensics. Regional Cyber Centers (RCCs) must remain vigilant (Department of the Army, 2023; United States, Joint Chiefs of Staff, 2022b).

How do We Defend Critical Infrastructure?

Once LND (Local Network Defenders), MO (Mission Owners), or CSSP (Cybersecurity Service Provider) identify an anomaly, it is then handed off to the Defensive Cyberspace Operations (DCO) in the blue space for incident response and/or hunt-forward missions. DCO will set a baseline to assess, then clear and harden the network, then finish the operation with a risk-mitigation plan (United States, Joint Chiefs of Staff, 2022b). Dragos is the automated, comprehensive OT tool that is used within the Cyber Protection Brigade to immediately detect intrusion and then mitigate OT vulnerabilities. Having the CEO and co-founder of Dragos, LTC Rob Lee, direct commission to the Virginia National Guard on March 1, 2025, will help sustain and advocate growth to defend OT by utilizing AI. To keep pace with future technologies, ARCYBER Science and Technology, Program Manager RDT&E (Research Development Test & Evaluation), ATEC (Army Training and Evaluation Command), Operational Assessments, Developmental Testing, and Soldier Touch Points (STP) are leading the efforts in experimentation with AI in OT. Based on those assessments, the Program Manager (PM) DCO was able to purchase the Dragos OT Tool to meet the requirements under our DCO Tool Suite RDP (Requirements Development Program) and Program of Record (PoR) ahead of our OT Capability Drop (CD) being approved. This is another great example of acquisition translating operational needs into actionable requirements, thus meeting the critical cyber needs of our warfighters. Acquisition needs to be nested with training (U.S. Department of Defense, 2020; U.S. Department of Defense, 2022). The need for Dragos Training in future OT tools with AI will be vital. There are Job Qualification Specialties (JQS) on OT with four Cyber Protection Teams (CPTs). There are multiple training centers focusing on defending OT with the Indiana National Guard at Atterbury-Muscatatuck Training Center and Cyber Battle Lab (CBL) at Fort Gordon, GA conducting OT Table Top Exercise (TTX) in June 2026. Additionally, ICS Certification Exercises hosted by the U.S. Army Corps of Engineers (USACE) with state power companies, Department of Energy, Bureau of Reclamation, and USACE Critical Infrastructure Cybersecurity (UCIC) stakeholders continue to forge ahead to outpace our adversaries in AI to defend OT. Other exercises focusing on OT are Cyber Shield and Yankee hosted by the National Guard and EGZ hosted annually by the active component Cyber

Army Transformation in Contact (TiC) 1.0 lets brigades rapidly test drones and electronic warfare, improving battlefield awareness, threat detection, and mission success. (Picture of Sergeant Jordan Telting by Adams Guerrero.)

Protection Brigade conducting terrain mapping of OT environment. On the commercial side, Idaho National Labs is a premier training center specializing in OT (OT Lab: Idaho National Laboratory, 2025). Continuous experimentation is ongoing and critical to maintain technological advantage.

How do We Disrupt Critical Infrastructure?

Offensive Cyber Operations (OCO) conducts keyboard fire effects to gain advantage over our adversaries through disruption, degrading, or destroying in relation to the Stuxnet example noted earlier. Nesting operational graphics terminology with soldiers who are at the tip of the spear is purposeful. OCO can also influence adversaries with false information and kinetic effects. Identifying BOTs with AI over Social Media Platforms to manipulate public opinion through information advantage and information dimension is another strategy (United States, Joint Chiefs of Staff, 2022b). In December 2024, China claimed that we weaponized cyber attacks since May 2023 targeting Chinese companies specializing in energy and digital information, which coincided with heightened U.S. and China tensions over export controls on semiconductors and AI technologies (CSIS, 2025).

How do We Deliver OT Capabilities to the Warfighter?

The recently signed Army Transformation Initiative (ATI) memo by the Secretary of Defense on April 30, 2025, will get after continuous transformation. ATI will build upon the Transformation in Contact (TiC) effort, through rapid Commercial over the Shelf (COTS) prototyping while streamlining acquisition coupled with integrating AI with emerging OT technologies faster. Agile funding already provided rapid procurement of the Dragos OT tool by adapting how we fight, train, organize, and buy equipment. Army Futures Command and Training and Doctrine Command will merge into Transformation and Training Command (T2COM) to align force generation, force design, and force development under a single headquarters on October 1, 2025 (Driscoll & George, 2025).

How will Strategy Deliver OT Capabilities to the Warfighter?

Section 811: Modernizing the Department of Defense Requirements Process Final Report to Congress on July 14, 2025, is lockstep with ATI through increased timely equipment fielding and accelerated innovation cycles through experimentation. Additionally, the FY 2024 National Defense Authorization Act (NDAA) stated NLT October 1, 2025 the Army will modernize requirements and streamline acquisition processes to deliver agile, reliable, and combat-ready capabilities at speed and scale through COTS and rapid prototyping, while the 2025 National Defense Strategy (NDS) dated May 2, 2025, will prioritize defense of the U.S. homeland (Fiscal Year, 2025). The Digital Modernization Strategy will also align with the NDS on artificial intelligence to shift from hardware to more adaptable software enterprise with the cloud-based Big Data Platform (BDP). Gabriel Nimbus (GN) is the Army repository for OT anomalies and OT adversarial threat TTPs on the Army Gov Cloud BDP. We can now get after the low bandwidth at the tactical edge by parsing metadata at tactical edge to push and ingest large data from the BDP. Consequently, the AI Delivery of AI-enabled capabilities can be a force multiplier to support critical infrastructure in cooperation with DHS and cut the red tape with Generative AI. We need to have a technical computing advantage over China in advanced semiconductors during the competition phase to produce powerful GPUs (Graphics Processing Units). AI-capability development requires tremendous computing power and the large electrical footprint with hydroelectric dams and/or nuclear energy to power those data centers.

On August 21, 2025, the disestablishment of JCIDS (Joint Capability Integration and Development System) prioritized agile delivery capabilities at speed of relevance to the warfighter by streamlining the acquisition process. In the past, the acquisition guidance to approve a capability was 103 days but took up to 2 years; consequently, the technology that was approved could not keep pace with evolving threats and emerging tech. Now it can take 30 days. The speed of delivery and continuous improvement will eliminate the stovepipes and promote cross-functional collaboration (Driscoll & George, 2025).

How will Policy Deliver OT Capabilities to the Warfighter?

Policy addresses all elements of Doctrine, Organization, Training, Materiel, Leadership and Education (DOTmLPF-P). Executive Order (EO) 14179 signed January 23, 2025, revokes previous barriers to AI innovation (Fiscal Year, 2025). This allowed the ATI to follow COTS free market to pursue future AI technology. The end state is the opportunity to overmatch our adversaries exponentially while our adversaries are constantly adapting and evolving their respective cyber threats. Another EO 14028 signed May 12, 2021, following the Colonial Pipeline ransomware cyber-attack ensured stronger baseline cybersecurity measures such as Zero Trust Architecture (ZTA). This policy has already created ZTA curriculum and training at the respective schoolhouse under Cyber Center of Excellence, providing a competitive automated-edge solution with AI called Security Orchestration Automated Response (SOAR). Both EO policies directed AI governance to keep pace with technology. Policy on OT vulnerabilities also led to Senator Eric Schmitt (MO) reaching out to ACM-Cyber. On December 5, 2024, Sen. Schmitt also introduced a bi-partisan bill to encourage competition in AI procurement aligning with EO 14179 (Office of U.S. Senator Eric Schmitt, 2024).

US Critical Infrastructure Remains Exposed as Congress Confronts OT Cybersecurity Gaps

In closing, to continue moving AI innovation forward will require continuous transformation. T2COM is one of the leaders to meet these AI with OT capability gaps through Concept-Focused Warfighter Experiments (CFWE) and Project Convergence Capstone to discover AI/OT advanced technology through experimentation. There is recognition at the highest levels of U.S. government on the importance of AI and OT.

We must be postured effectively to avoid technological surprises. We must be predictive and adaptive. We must keep pace with rapid changes in the operational environment and the force employment phase of the continuum of strategic direction described in CJCSI 3100.01e and Joint Doctrine Note 2-19 (United States, Joint Chiefs of Staff, 2019). Continuous transformation will get us across the finish line. Continuous transformation (3 phases) will train through exercises, equip through experimentation, and exceed the pace of adversaries during the competition phase. We must stay flexible, agile, and adaptive to new and emerging technologies in AI and OT. First, we must demonstrate tangible near-term results while innovating new capabilities through rapid acquisition in 18-24 months. Second, deliberate transformation will deliver capabilities to the total force in 2-7 years. Finally, with concept-driven transformation, we will invest in future capabilities driven by experimentation through Science and Technology (ARCYBER S&T) in 7-15 years towards the Army 2030/2040 concept (Driscoll & George, 2025). If we don't, our adversaries will likely target a hydroelectric dam that could flood a city, cause a blackout, and shut down transportation systems all at the same time.

Chief Warrant Officer 4 Rory J.H. Rankin is currently assigned with the newly established Cyber Future Capabilities Directorate (FCD) resulting from recent Transformation and Training Command (T2COM) re-organization. He was previously dual-hatted as DCO Branch Chief and the Senior Technical Advisor (STA) for Army Capability Manager-Cyber (ACM-Cy) from August 2023 to January 2026. With aggregated knowledge and understanding, he has accumulated over 25 years in special forces, tactical, operational, strategic, and combat environments on leadership assignments for five sister services at all COMPOs and at all echelons (Joint, Corps, Division, Regiment, Brigade, Battalion, Company, and Mobile Training Teams (MTT) Squad levels) with an additional 18 years at one company in the corporate Information Technology (IT) field. Throughout his career, he has interacted with 18 inter-agencies of the Intelligence Community (IC) and 14 different foreign militaries, which has provided him conceptual knowledge and understanding. He has been trained at 15 professional military education courses spanning five different MOS's in Signal, Military Intelligence, and Cyber with an ASI in Capability Development, and a PDSI (Senior Host Analyst). The National Defense Strategy (NDS) remains fluid as technological capabilities constantly evolve across funding, policy, and doctrine. Within this environment, CW4 Rankin continues to inform and assist decision-making within the Army. His goal is to form relationships with the community of interest and respective stakeholders to build the bridge between cutting-edge technologies such as Artificial Intelligence/Machine Learning (AI/ML) in the public sector and partner collectively to enable the DoW (Department of War) to be effective.

References

Center for Strategic and International Studies (CSIS). (2025). CSIS Significant Cyber Incidents Since 2006. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Department of the Army. (2023). Information (ADP 3-13) https://armypubs.army.mil/epubs/dr_pubs/dr_a/arn39736-adp_3-13-000-web-1.pdf

Driscoll, D., & George, R. (2025, May 1). Letter to the force: Army transformation initiative. www.army.mil. https://www.army.mil/article/285100/letter_to_the_force_army_transformation_initiative

FEMA. (2008). CISA: Critical Infrastructure and Key Resources Support Annex [PDF]. FEMA. https://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf

Fiscal Year 2024 National Defense Authorization Act, Section 811: Modernizing the Department of Defense Requirements Process. (2025). https://www.jcs.mil/portals/36/fy24%20ndaa%20section%20811%20report%20to%20congress.pdf

Messare, M. (2026, March 12). Middle East escalation: Assessing spillover threats to OT/ICS [Intelligence Briefing]. Dragos.com. https://hub.dragos.com/on-demand/middle-east-escalation-assessing-spillover-threats-to-ot-ics?utm_campaign=34250564-2026+year+in+review+full+report&utm_medium=email&_hsenc=p2anqtz-_oshx2ne06skdulwfantjz_kww4yrqcg9t1hdkgjzava_gg3d_1bt-852p2osz9mdrv78l3rtttsdm6hvuocd7fsov-0ifhvptehszgq8q7dwtcuq&_hsmi=41031165&utm_content=41031165&utm_source=hs_automation

Office of U.S. Senator Eric Schmitt. (2024, December 5). Senator Schmitt and Senator Warren Introduce Bipartisan Bill to Encourage Resiliency, Competition in Department of Defense's Procurement of AI, Cloud Computing Tools [Press Release]. https://www.schmitt.senate.gov/media/press-releases/senator-schmitt-and-senator-warren-introduce-bipartisan-bill-to-encourage-resiliency-competition-in-department-of-defenses-procurement-of-ai-cloud-computing-tools/

OT Lab: Idaho National Laboratory. (2025). https://inl.gov/national-security/

OT Lab: Indiana National Guard Camp Atterbury. (2025). https://www.in.gov/indiana-national-guard/camp-atterbury/

Times of India World Desk. (2025, September 5). 'Salt Typhoon' attack: How China hackers may have accessed sensitive US data; tapped into power grids. Times of India. https://www.msn.com/en-in/news/world/salt-typhoon-attack-how-china-hackers-may-have-accessed-sensitive-us-data-tapped-into-power-grids/ar-aa1lveud?ocid=bingnewsserp

Ribeiro, A. (2025, July 22). US critical infrastructure remains exposed as Congress confronts OT cybersecurity gaps, fifteen years after Stuxnet. Industrial Cyber. https://industrialcyber.co/industrial-cyber-attacks/us-critical-infrastructure-remains-exposed-as-congress-confronts-ot-cybersecurity-gaps-fifteen-years-after-stuxnet/

Read. (2023). The National Academies Press. https://www.nationalacademies.org/read/27503/chapter/8

United States, Joint Chiefs of Staff. (2022a). Joint strategic planning system (CJCSI 3100.01E).

United States, Joint Chiefs of Staff. (2022b). Cyberspace operations (JP 3-12) https://irp.fas.org/doddir/dod/jp3_12r.pdf

United States, Joint Chiefs of Staff. (2019). Strategy [Joint Doctrine Note 2-19].

U.S. Department of Defense. (2020, September 9). The Defense Acquisition System (DoDD 5000.01)

U.S. Department of Defense. (2022, July 28). Operation of the Defense Acquisition Framework (DoDI 5000.02