# HACSAW: A Trusted Framework for Cyber Situational Awareness

Leslie Leonard, William Glodek
Department of Defense (DoD)
High Performance Computing Modernization Program (HPCMP)
{leslie.c.leonard, william.j.glodek}@erdc.dren.mil

## ABSTRACT

The HPC Architecture for Cyber Situational Awareness (HACSAW) was established by the Department of Defense (DoD) High Performance Computing Modernization Program (HPCMP) to combine a rich computational environment with operationally relevant data to perform cutting-edge cybersecurity research that will increase HPCMP's current and predictive understanding of cyberspace on the Defense Research and Engineering Network (DREN). The data repository created by this unique environment includes the collection of unclassified data sources from the edge of the network (i.e., Internet Access Points) down to the host-level, across more than one hundred (100) different DoD enclaves. Through the application of high performance computing (HPC) resources, HACSAW explores novel and innovative analytical capabilities based on a comprehensive cybersecurity dataset. The integration of HPC within the cyber workflow provides an opportunity for fusion and assessments of disparate data streams and real-time analysis using data science algorithms and machine learning (both structured and unstructured data). Our approach is designed to ultimately leverage HPC resources to significantly reduce the time to respond to changes in the cyber environment from days to minutes.

Understanding the operational status of information systems, the missions (friendly and adversary) being pursued, and the threats and vulnerabilities that impact them is essential for effective mission accomplishment. This understanding is referred to as Cyberspace Situational Awareness (Cyber SA). Today's decision makers require meaningful Cyber SA to safeguard sensitive data, sustain fundamental operations, and protect national infrastructure [2]. The need and responsibility of Cyber SA spans multiple organizations within the DoD, across the entire government and in the private sector.

The lack of relevant and recent real-world network enterprise data has hampered many cybersecurity research efforts to develop and validate algorithms or methods under realistic conditions. HACSAW has reduced this technical barrier with a development environment that provides computational and data-rich information to researchers to test, develop, model, measure and refine data-driven analytics. This environment is the proving ground for novel ideas, algorithms and approaches that are suitable for large scale execution in a dedicated HPC environment. Currently, HACSAW as an aggregation of over one (1) petabyte of DREN data to include network-based monitoring and intrusion detection results, web content filtering, vulnerability scanning, firewall, sensor health, etc. Context is applied to each cyber event through the use of custom enrichments that provide downstream analytical processes with information that may be useful in determining the nature of the event.

During this talk, we will discuss HPCMP's initial approach to addressing Cyber SA through a Call for Proposals (CFP) to the data science, cyber, and HPC communities. Selected collaborators will receive funding for a one-year effort that demonstrates potential for integration into DREN's Cyber SA operational environment and aligns with identified Mission Essential Tasks (METs). METs will ensure decision makers have the understanding necessary to make effective decisions. Such tasks include monitoring, detection, alerting, cyber threat analysis, cyber risk and event analysis, and sharing and collaboration. Initial and future contributions in the areas of modeling and simulation [4], clustering [3] and deep learning [1] are anticipated and results will be shared at a later date.


*HoTSoS '18,* April 10-11, 2018, Raleigh, NC, USA

ACM ISBN 978-1-4503-6455-3/18/04
https://doi.org/10.1145/3190619.3190641

## 1. REFERENCES

[1] J. Ezick, M. Baskaran, D. Bruns-Smith, A. Commike, T. Henretty, M. H. Langston, J. Ros-Giralt, and R. Lethin. Discovering deep patterns in large-scale network flows using tensor decompositions. FloCon '17, 2017.

[2] C. Onwubiko and T. Owens. *Situational Awareness in Computer Network Defense: Principles, Methods and Applications*. IGI Global, Hershey, PA, USA, 1st edition, 2012.

[3] C. Savkli, J. Lin, P. Graff, and M. Kinsey. Galileo: A generalized low-entropy mixture model. The 13th International Conference on Data Mining, 08 2017.

[4] N. Wagner, R. Lippmann, M. Winterrose, J. Riordan, T. Yu, and W. W. Streilein. Agent-based simulation for assessing network security risk due to unauthorized hardware. In *Proceedings of the Symposium on Agent-Directed Simulation*, pages 18–26, 2015.