SEI/CERT Support for NRMC's MDM Mission

Mark Sherman, TBD

March 3, 2022

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0198

Outline

Previous discussions proposing MDM work

Focus of today's discussion: responding to events

- Needs of NRMC
- SEI Assets
- Potential support projects

Next steps

New Opportunities for Collaboration – MDM

Understanding the Information Environment for Text

- Provenance and Pedigree of Information
- Sufficiency, Precision and Recall of Query Systems

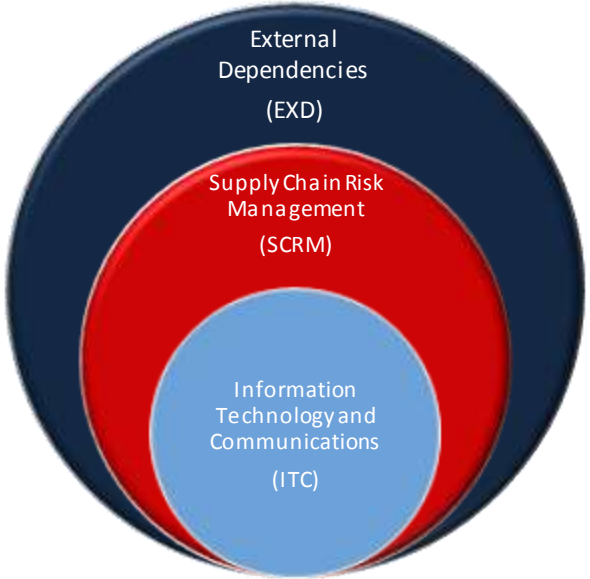
Understanding the Information Environment for Data

- Detection (Generation) of Deep Fakes
- Detection of Sensor Anomalies

Expanding Situational Awareness

- Sentiment Analysis of Text
- Biological Markers in Video
- Motivation Determination (reward function identification)
- Poisoning Detection

New Opportunities for Collaboration-Supply Chain Risk Mgmt.



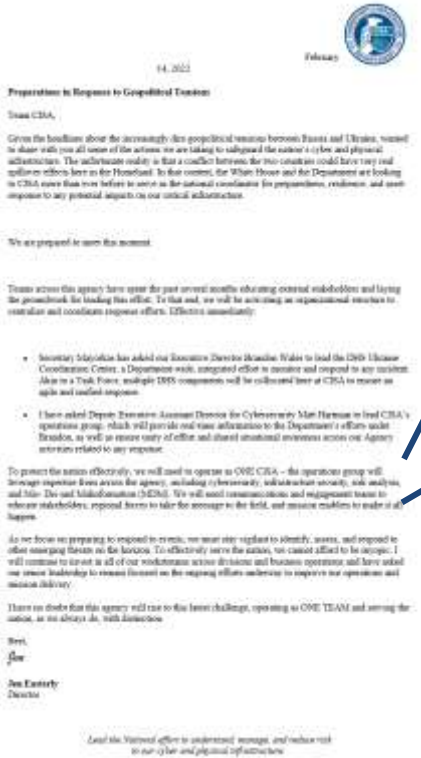
Improve Supply Chain Resilience

- Create lightweight tools for critical infrastructure owners/operators to prioritize and manage key external dependencies
- Identify and quantify the risk in complex multi-vendor ecosystems (i.e., “fourth-party” risk)

Secure the Software Supply Chain

- Supply chain risks of machine learning applications
- Supply chain risks in cloud development (i.e., DevSecOps) environments
- Tools and technology for detection of supply chain attacks

Responding to Immediate Needs



Preparations in Response to Geopolitical Tensions

Team CISA,

We are prepared to meet this moment.

- Secretary Mayorkas has asked our Executive Director Brandon Wales to lead the DHS Ukraine Coordination Center, a Department-wide, integrated effort to monitor and respond to any incident. Also in a Task Force, multiple DHS components will be collocated here at CISA to ensure an agile and unified response.
- I have asked Deputy Executive Assistant Director for Cybersecurity Matt Hartman to lead CISA's operations group, which will provide real-time information to the Department's efforts under Brandon, as well as ensure unity of effort and shared situational awareness across our Agency activities related to any response.

To protect the nation effectively, we will need to operate as ONE CISA – the operations group will leverage expertise from across the agency, including cybersecurity, infrastructure security, risk analysis, and Mis- Dis-and Malinformation (MDM). We will need communications and engagement teams to educate stakeholders, regional forces to take the message to the field, and mission enablers to make it all happen.

As we focus on preparing to respond to events, we must stay vigilant to identify, assess, and respond to other emerging threats on the horizon. To effectively serve the nation, we cannot afford to be myopic. I will continue to invest in all of our workforces across divisions and business operations and have asked our senior leadership to remain focused on the ongoing efforts underway to improve our operations and mission delivery.

I have no doubt that this agency will rise to this latest challenge, operating as ONE TEAM and serving the nation, as we always do, with distinction.

Best,

Jen

Jen Easterly
Director

Lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

To protect the nation effectively, we will need to operate as ONE CISA – the operations group will leverage expertise from across the agency, including cybersecurity, infrastructure security, risk analysis, and Mis- Dis-and Malinformation (MDM). We will need communications and engagement teams to educate stakeholders, regional forces to take the message to the field, and mission enablers to make it all happen.

SEI/CERT Data Science Skills

Analysis of "signal" content

- Image
- Video
- Audio
- Instrument

Analysis of "textual" content

- Web content
- Social media
- Incident reports
- Transcripts

Analysis of metadata

- Consistency of content and metadata
- Ontology generation

Working with CMU Centers (Prof Kathleen Carley)

- Center for Informed Democracy & Social - cybersecurity (IDeaS)
- Computational Analysis of Social and Organizational Systems (CASOS),
- BEND framework and ORA tool set

Working with other government organizations, e.g., ODNI Authentication Steering Committee

Responding to Immediate Needs

Example perceived needs:

- Guidance on fact-checking vs alteration detection
- Assemble list of assets for fake detection (per medium)
- Education on detecting MDM coming from conflict
- Guidance on how to create and distribute information to support authentication

Next steps

Priority interests and needs

Mechanics: what PWPs could be tapped

POC for DHS