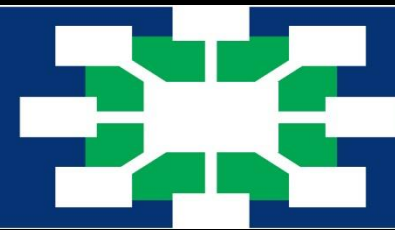# Information, Intelligence, and Human Factors

John Bryk

Downstream Natural Gas Information Sharing and Analysis Center
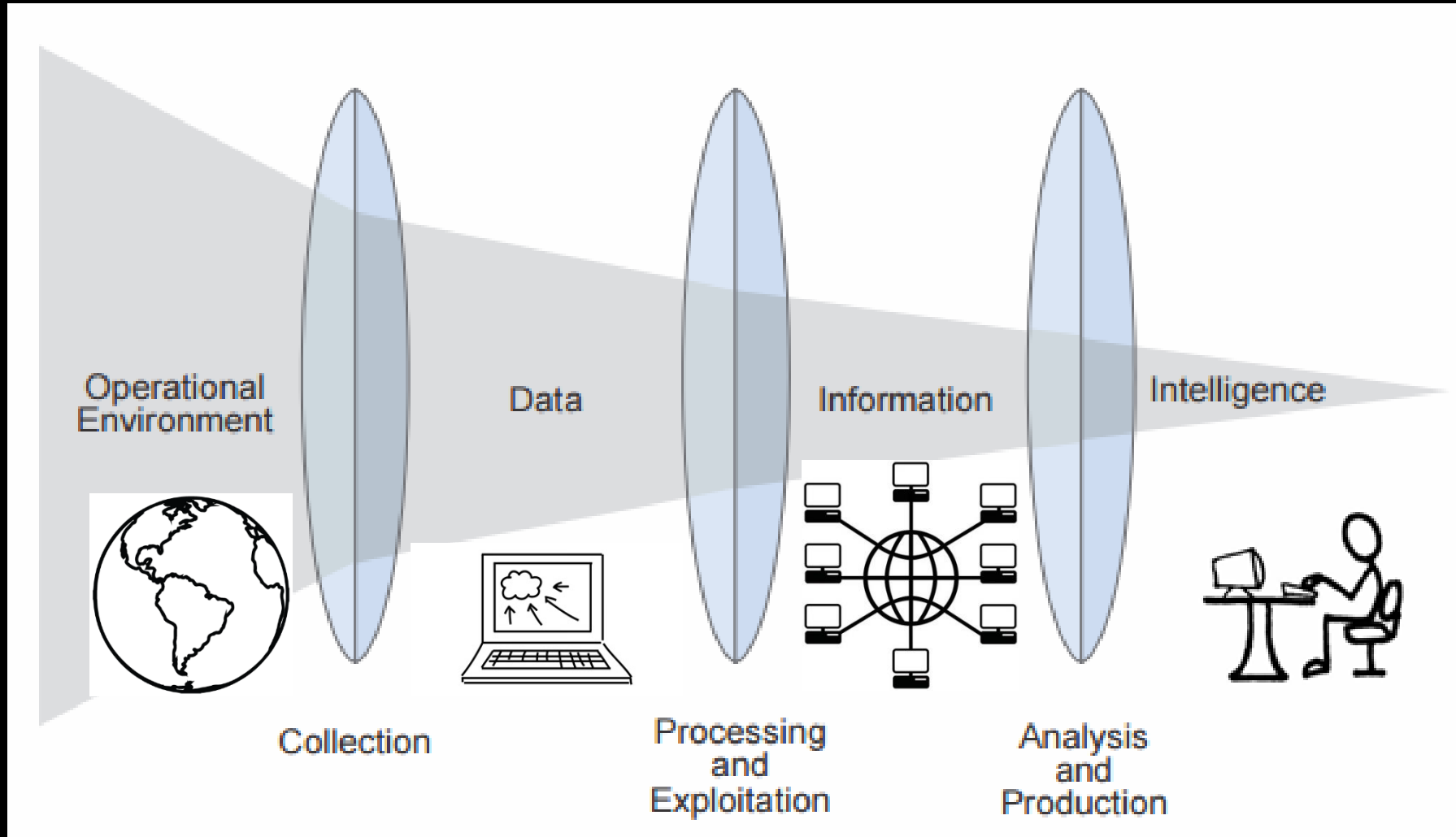
DNG-ISAC

Washington, DC

Information Sharing and Analysis Center (ISAC)

- John Bryk, Cyber and Physical Threat Intelligence Analyst at the Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC)

- DNG-ISAC serves natural gas utility (distribution) and pipeline (transmission) companies

- Coordinates closely with the electric industry (E-ISAC)

- Promptly disseminates threat information and indicators

- Administered by the American Gas Association (AGA) in partnership with the Interstate Natural Gas Association of America (INGAA) and Canadian Gas Association (CGA)

DNG-**ISAC**

Key points

- Threat data, information, and intelligence are all very different

- In the progression from data to information to intelligence, the *volume* of outputs reduces while the *value* of those outputs increases

- Computers can't produce threat *intelligence* while humans aren't suited for collecting and processing large volumes of threat *data*

- *Action* must always be the end goal

DNG-**ISAC**

Data ⟶ information ⟶ intelligence

Operational Environment — Collection — Data — Processing and Exploitation — Information — Analysis and Production — Intelligence

Data

- **Fact without meaning; meaning must be assigned**

- **Individual elements that when put together create contextual information**

da·ta

/ˈdadə,ˈdādə/

noun

facts and statistics collected together for reference or analysis.
*synonyms:* facts, figures, **statistics**, details, particulars, specifics; More

- COMPUTING
  the quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.
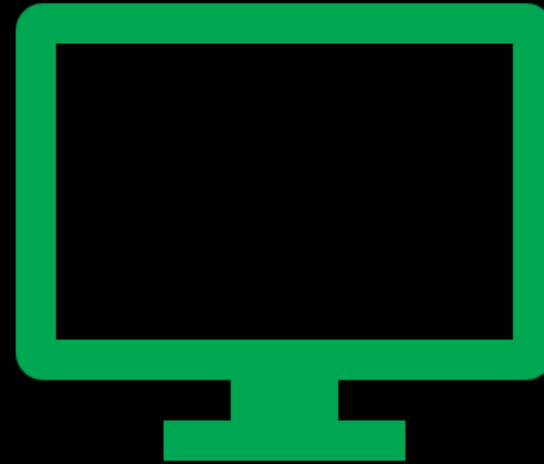
- PHILOSOPHY
  things known or assumed as facts, making the basis of reasoning or calculation.

DNG-ISAC

Human speed v. computer speed
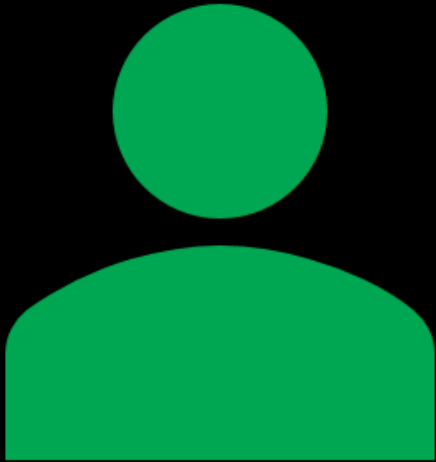
140 words per minute in Morse code

4000 events per second

DNG-**ISAC**

Information

- **Pieces of data that have been collected**

- **Produced when a series of points are combined to answer a simple question**

- **Easily shared within the industry**

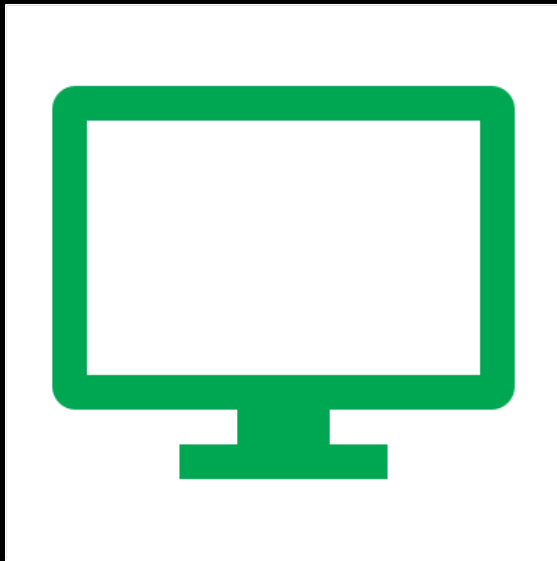- **Sometimes shared with government**

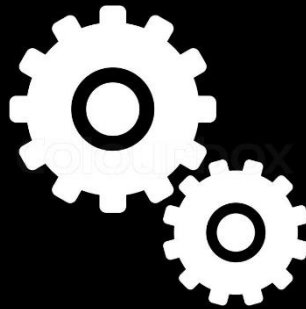in·for·ma·tion

/ˌinfərˈmāSH(ə)n/

noun

1. facts provided or learned about something or someone.
   "a vital piece of information"
   synonyms: details, particulars, facts, figures, statistics, data; More

2. what is conveyed or represented by a particular arrangement or sequence of things.
   "genetically transmitted information"

Volume v. value
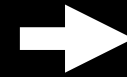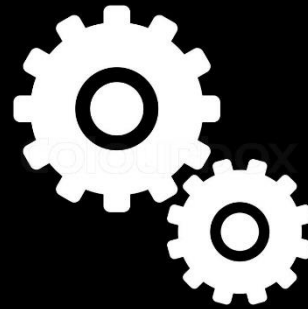

1,000,000,000 data events

10,000 threat platform indicators

DNG-**ISAC**

Human factors - volume v. value

10,000 threat platform indicators

1 actionable intelligence report

DNG-**ISAC**

Intelligence

- **Magic Formulas:**

  - **Information + Analysis = Intelligence**
  - **Requirements + Intelligence = Action**

- **U.S. Department of Defense defines intelligence as:**

  The product resulting from the collection, processing, evaluation, analysis, and interpretation of available information concerning hostile or potentially hostile elements or areas of actual or potential operations

THE INTELLIGENCE PROCESS

Evaluation...

Dissemination and Integration — Planning and Direction

Analysis and Production — Mission — Collection

Processing and Exploitation

...and Feedback

SOURCE: JOINT INTELLIGENCE / JOINT PUBLICATION 2-0 (JOINT CHIEFS OF STAFF)

DNG-**ISAC**

Human factors - requirements

- Only humans can determine *what* actions should be taken and *why*

- Creating good requirements is a uniquely human function

- Good requirements:

  - *Ask only one question*

  - *Focus on a specific fact, event, or activity*

  - *Provide intelligence required to support a single decision*

  - *Are tied to key decisions that have to be made*

  - *Supply the latest time the information is of value (LTIOV)*

DNG-**ISAC**

Validating requirements

- Only humans can determine *what* actions should be taken and *why*

- Necessity

- Feasibility

- Specificity

- Timeliness

DNG-**ISAC**

Intelligence challenges

- Incomplete threat landscape understanding and qualified workforce shortage

- Collection bias in U.S. Intelligence Community and information security community

- Reacting to *threat du jour* instead of following a structured intelligence cycle

DNG-ISAC

Key takeaways

- Threat data, information, and intelligence are all very different

- In the progression from data to information to intelligence, the volume of outputs reduces while the value of those outputs increases

- Threat intelligence platforms produce data and information which human analysts can use to produce and share actionable (operational) threat intelligence

- Computers can't produce threat intelligence while humans aren't suited for collecting and processing huge volumes of threat data

- Action must always be the end goal

DNG-ISAC

Key takeaways

The entire presentation boiled down to two points:

- Information and intelligence are not the same thing

- Intelligence must be actionable

Questions?

John Bryk

DNG-ISAC Cyber and Physical Threat Analyst

American Gas Association

jbryk@dngisac.com