Spring Design Studio 2024

Scene, Personas, Dataset & Tools

Setting the Scene

The Disaster

In 2019 a bombing killed two people and injured others in the city of Macondo, a mountain town in Oceania. A commercially made drone fitted with an IED targeted a coffee shop on North Duke Street in the morning hours of April 10th, 2019.

Two employees and the owner of Kaffeinate, a coffee shop located on North Duke Street, were inside getting ready for the busy morning rush. All three died in the explosion. A third employee died two weeks later from his injuries. At least 5 others were injured, including one firefighter. The Macondo community was left shaken and stunned.

The blast destroyed the coffee shop and damaged several surrounding buildings. In the early moments of the response, the cause of the explosion was unknown and thought to potentially be the result of a natural gas explosion. As more information from the disaster scene came in, however, intelligence indicates that the event was likely the result of a hostile bombing by the Republic of Zendia. Leaders of Oceania quickly reached out to intelligence experts at the Big Government Intelligence Agency (BGIA) to analyze the bombing to help prepare a national response.

The Counterterrorism team at BGIA is responsible for producing reliable and robust intelligence on events such as the bombing described above. The team must find data that helps tell the story of what happened before, during and after the bombing in order to inform the Leaders of Oceania so that they can provide the residents of Macondo and Oceania with timely and accurate information.

The Analysis

The intelligence analysts responsible for finding and making sense of the technical data that will be used to inform the Leaders of Oceania, via a final intelligence analysis report, are Target Digital Network Analysts (TDNAs)[1]. For this semester's work we have described the varied and

[1] TDNAs are often referenced by other titles and in the documentation for this course, you may also see them referred to as Digital Network Analysts, Target Network Analysts, Cryptologic Intelligence Analysts, and Discovery Analysts.

complex work of TDNAs, via four scenarios that seek to describe facets, tasks, scenarios and levels of expertise representative of the broad range of TDNA skillsets and experiences. The four personas are:

- **Group1: 'Hello world'** – Describes an analyst's first query from the perspective of a novice TDNA.

- **Group 2: 'Mind the Gap'** – Describes how an analyst determines what data they are missing from the perspective of a TDNA with more intermediate experience.

- **Group 3: 'You Can't Do That'** – Describes what happens when an analyst queries something the BGIA does not have authority for, from the perspective of a seasoned TDNA.

- **Group 4: 'Crossing the Streams'** – Describes how an analyst may approach synthesizing data from the perspective of an expert TDNA.

Personas

'Hello world' – An Analyst's First Query

Scenario
While Susie started her TDNA job a couple of weeks ago, most of the time since has been spent in training classes. Today Susie has arrived at her first development tour in the Counterterrorism organization within BGIA. For the next few weeks she will be working with the Zendian team looking at a Zendian terrorist grouIntelTechniques Search Toolp for possible connections to the Macondo bombing. Her mentor has given her an email address that has recently been in communication with the terrorist group and they suspect belongs to a new operative. Susie's first task is to analyze recent traffic with the email address to characterize how this address is used by the Zendian group. This first query is pretty straightforward, having only one address. But interpreting the results is challenging to Susie as she doesn't understand technical data and quickly gets overwhelmed by all of the volume.

Persona (Susie)

- Susie just started two weeks ago as a network analyst.
- Susie has a bachelor's degree in International Relations.
- Susie has no knowledge of global telecommunications.

Examples

- Susie does not know where to go to find information about the information in her results.
- How does she manipulate her results (i.e. filter, sort, rearrange) so that she can make sense of them and then get to what she is looking for?
- Once she understands the information, she is not sure what her follow on actions should be.

'Mind the Gap' - How An Analyst Discovers the Data is Missing

Scenario

Josh is a fairly new network analyst who recently joined the Counterterrorism Tradecraft Support office. He has an Associate Degree in Computer Studies and is very comfortable working with uncertainty. He chose this position because he loves disentangling data and piecing clues together to answer questions. In investigating the bombing in Macondo, Josh uses specialized analysis tools each with their own unique syntax requirements. In one tool, Josh may, for example, use query language that exposes relationships between entities and in another use network protocols to filter data for a granular examination of packets. His queries often return zero results which leaves him questioning if the data does not exist or if his query syntax was wrong. His analysis stalls while he digs into other databases to check for the additional tradecraft help or dataflow information that could indicate system problems. When his queries do produce results, piecing together geographic information, technical network details, and other data to form a more complete picture is a challenge because the tools he relies on were not designed with this type of discovery and analysis in mind. As he works through his analysis, Josh uses note fields built into tools and standard business productivity tools (similar to Google Docs) to articulate his findings and gaps in data that could change his analysis process or his overall analytic conclusions. He saves and uploads this document to the relevant project website so his team can access it.

Persona (Josh)

- Josh has been working for about 7 months as a network analyst
- He is taking college classes after-hours for a degree in Data Science.

- He has limited knowledge of global telecommunications all of which was acquired through just-in-time training events.

Examples

- Josh often has to utilize several different tools that each contain different datasets. He may be very familiar with how to query and analyze data from a couple of the tools, but new to the others. He cannot ignore the data as it may be crucial in piecing together the information. He must utilize his experience and creativity, along with tradecraft that has been documented by other analysts, in order to piece the information together. In this scenario, it is often difficult to determine how to query for the right data and analyze the data altogether.

- Josh may query against data from CCTVs that he knows are on the buildings in the vicinity of Kaffeinate. That said, he may not know that, during the week of the bombing, the CCTVs were being serviced for maintenance and therefore not operational. This is a collection gap.

- Josh has to manually push data to another analytic tool he uses, but unfortunately the data he wants to analyze is in varying formats. He does his best to "clean" the data and ingests it into the tool…or so he thought. The tool, unbeknownst to Josh, removed a couple hundred rows of data that it could not read and did not provide an error pop-up indicating such. Josh eventually notices the error, but it takes him thirty minutes of time he does not have, in order to investigate the error.

'You Can't Do That' - When An Analyst Gets the Authority Wrong

Scenario

Michele started at BGIA 10 years ago, after college. Most of her analytic experience has been spent doing Zendian language translation until the Zendian-Macondian war broke out three years ago. Since the war started, more of her work has focused on intelligence analysis of Zendian groups and she has slowly been exposed to more and more of the technical data as a result of seeking to understand Zendian activities. She recently joined a team that is looking at new Zendian military tactics, particularly the use of drones in armed conflict. This team has started to notice Zendia posting publicly available propaganda videos of SkyOne Drones. Through research, Michele has learned that SkyOne Drones are manufactured by Zendia. On one key date when there was a particularly large attack on a power plant in Oceania, Michele finds a lot of "skyone" activity using a single IP address. Michele suspects she has found a key piece of evidence related to Zendian drones and wants to run a follow-on query, but before

conducting further analysis, Michele does her due diligence to verify the compliance of said query. An hour later her auditor runs over to inform her that her IP search is a violation of the compliance policy because of the way she constructed her query. As such, Michele will have to sanitize her workspace and fill out a compliance violation report. Michele is immediately upset as she always completes her required compliance training, conducts her due diligence and adheres to organizational standard operating procedures. Her auditor takes some time to demonstrate how she should have better qualified her query and helps Michele fill out the violation report.

Persona (Michele)

- Michele has been working for about 7 months on the network analyst team she joined after wanting to try a diversity tour from her work as a language analyst.
- Michele has a bachelor's degree in Zendian.
- Michele has no background in global telecommunications but has worked in intelligence her whole career and has picked up some familiarity with high level terms.

Examples

- Michele is able to query for SkyOne traffic in DATABASES A, C, and D, but not in DATABASES B and E. Additionally, results returned from Michele's original queries will likely include new information that she may want to query on and investigate further, but which may have different requirements on where and how she can query. Given the esoteric and constantly evolving nature of each TDNA's office and mission set, knowing where and how to query takes experience and skill, even with thorough documentation. If Michele forgets and slips up that is an incident that must be reported.

- Michele has assessed that the SkyOne IP is vitally important to collect in order to answer the intelligence questions posed by Oceania Leadership. While Michele has a lot of experience at BGIA, she has not previously dealt with this scenario before and does not know how to proceed. Michele must find the relevant documentation and consult with her Compliance and Policy contacts in order to figure out the legal process and required documentation to determine whether she and her team can proceed.

'Crossing the Streams' – When an Analyst has to Synthesize Data

Scenario

Miguel is a Senior TDNA leading the team investigating the Macondo bombing. He has been in this role for about two years, though has been a TDNA since joining BGIA 15 years ago. His daily work deals with understanding current intelligence topics worked by BGIA's Zendian Office as well as acquiring access to data to meet the intelligence needs. His work can cover a wide range of data types and priorities frequently change as events occur. For example, one day his team may work on a network infrastructure project, and the next they shift priorities to investigate technology and data linked to an attack like the Macondo bombing. To manage the team's efforts, Miguel utilizes a workflow management tool to prioritize and assign tasks. Being the senior TDNA, others approach him throughout the day with questions to make sense of technical information and for help finding creative query strategies to look for data to fill identified gaps. Because of the variety of sources they draw information from, he and his team find it easiest to use chat for these impromptu brainstorming sessions so they can share screens, copy and paste lead information, and discuss other anomalies that emerge during analysis.

Part of Miguel's day is also spent on his projects. He works to connect the results of his team's analysis to form a holistic picture of the bombing incident that connects the Zendian groups, the weapons they used, and networks used to operate the drones. This could involve several actions depending on what gaps he sees. For example, he could take the results and perform more advanced technical analysis; he could summarize the data and create a request for additional collection – a time intensive task requiring him to copy and paste results saved in BGIA tools and shared files in addition to combining such with reports, news, and add technical knowledge explaining why these are valuable. No matter what he chooses, at the end of each day, he will write a summary to present during the next day's stand up where he will receive feedback and/or new information from colleagues that could alter the course of his team's work.

Additionally, as the senior TDNA, Miguel has several oversight and administrative responsibilities. Every day he audits queries made by his team and mentors junior analysts on his team. He ensures that the Office of the Director of National Intelligence (ODNI) Analytic Integrity Standards are followed throughout the entire analytic process and BGIAs compliance policies are maintained.

Persona (Miguel)

- Miguel joined BGIA 15 years ago after earning a BSc in Information Technology. He recently completed a Master of Science in Information Security (MSIS).
- Miguel plans and oversees his team's activities, but is not a supervisor.
- Miguel is regarded as a Subject Matter Expert (SME) in Zendian affairs.

Examples

- Miguel recently sat in on a 'tradecraft lunch' with some of his TDNA colleagues who work in various organizations across BGIA. During the lunch, one of the TDNA's provided an overview on Jupyter Notebooks and how they could be used to make aspects of their analysis more efficient and effective. Given his python coding experience, Miguel was able to take what he learned and write a notebook within a couple of days. Now, Miguel is able to combine various disparate data objects and their attributes in a way that sheds new light on critical intelligence. Miguel is also able to share the notebook with the rest of his team, many of which are more junior, which grants greater resilience across the team. In the future, Miguel hopes to incorporate some visualization outputs as well.

- Miguel's daily tasks include opening up 3 of his primary analytic tools to get started. He may review information from yesterday's queries or create new queries. As a part of his query generation, Miguel will utilize another set of tools to verify and lookup information to be included in his queries. Once he has information returning, he must start triaging the data for what is relevant and possibly merge disparate data objects from other queries in order to make sense of the information. This is cognitively demanding and requires a lot of context switching, various tabs, outputs, visualizations, etc. Miguel often references BGIA's tradecraft repository to find better and more efficient ways of doing analysis.

- Given Miguel's extensive experience as a TDNA as well as a Zendian SME, he is often asked to brief both his and his team's work, to organizational leadership, policymakers, and at BGIA tradecraft conferences, etc. Said presentations and interactions can take a considerable amount of time to prepare and Miguel often has to be judicious in prioritizing his tasks in order to ensure that the particular day's pressing tasks are completed on time. Additionally, as a result of these various interactions, Miguel often receives valuable feedback and questions that may reprioritize his team's efforts. Miguel will have to leverage his technical knowledge in order to appropriately manage and inform expectations surrounding such.

Dataset

The primary dataset for this semester's task includes the types of digital data objects (sourced from publicly available CRAWDAD datasets) that each persona would have access to query. Notably, however, not all of the data included in the dataset will be relevant to each persona (i.e. may vary based on the scenario).

Proxy Tools

The following are commercially available analytic tools that we have identified as proxies to the types of tools and related data that TDNA's may interact with. Please note that they are provided here as reference material to use when generating your design work; their inclusion in this document does not constitute an endorsement of them.

- Wireshark (demo video)
- Jupyter Notebooks (demo video)
- Xplico
- Domain Tools
- Google Image Search
- IntelTechniques