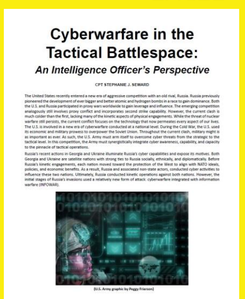
U.S. MILITARY OFFENSIVE CYBER CAPABILITIES

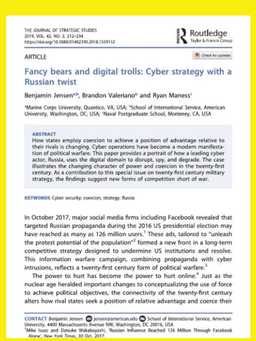
BY MACY SCHOWALTER AND TYLER MORAVEC

OUR PROBLEM

The advent of cybersecurity threats has increased exponentially over the last decade. Attacks are no longer affected by lone individuals but are state-sponsored and target commercial, academic, and military sectors alike. Adversaries continue to grow, and they are helping to change the geopolitical landscape through what is now known as the fifth domain of warfare engagement. The cyber warfare domain is large and complex, requiring new innovative ways to create knowledge out of information. New advances in graphical databases allow us to represent this complex and heterogeneous information in ways that allow us to query a corpus of knowledge to find cause-and-effect connections that previously required significant computational power. We conducted a literature review of 50 peer-reviewed articles to extract relevant elements of data that helped informed a knowledge base of facts. Herein we present the results of our work and exemplify its operational usage through simple queries to demonstrate capacity.

1. BY DISECTING 50+ PEER REVIEWED PAPERS, WE WERE ABLE TO BRING FACTUAL DATA INTO EXCEL

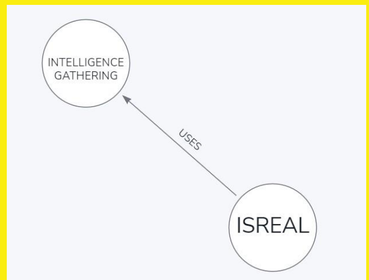

Cyberwarfare in the Tactical Battlespace:
An Intelligence Officer's Perspective


Fancy bears and digital trolls: Cyber strategy with a Russian twist

2. WE ORGANIZED OUR EXCEL TABLES INTO COLUMNS, SUCH AS ATTACK NAME, CAPABILITY, KEY PLAYERS, AND COUNTRY ATTACKED

NAME	CAPABILITY
FLAME	INTELLIGENCE GATHERING
DUQU TROJEN	INTELLIGENCE GATHERING
OPERATION ORCHARD	INTELLIGENCE GATHERING
FOURTH PARTY INTELL	INTELLIGENCE GATHERING
XKEYSCORE	INTELLIGENCE GATHERING
EO 12333	INTELLIGENCE GATHERING
TeDi	INTELLIGENCE GATHERING

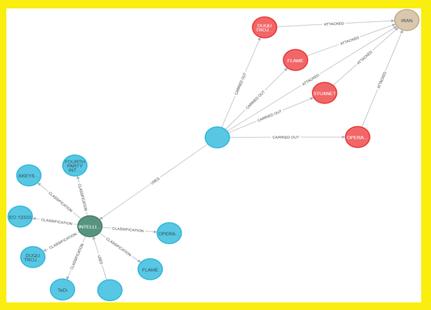
3. ONCE OUR EXCEL FILES WERE UPLOADED AS .CSV FILES INTO NEO4J, WE COULD THEN START MAKING NODES OF OUR DATA THAT HAD CONNECTIONS



4. WE RAN OUR IMPORTS AND BEGAN WRITING QUERIES IN A LANGUAGE NEO4J WOULD UNDERSTAND

```
MATCH p=()-->() RETURN p LIMIT 5
MATCH p=()-[r:`CARRIED OUT`]-
>() RETURN p LIMIT 25
MATCH p=(:`KEY PLAYERS`)-[r:USES]-
>() RETURN p LIMIT 25
MATCH p=()-[r:`TOOK ADVANTAGE OF`]-
>() RETURN p LIMIT 25
MATCH (n:VULNERABILITY) RETURN n LIMIT 25
```

5. ONCE NEO4J DISPLAYED OUR QUERY, WE ANALYZED OUR GRAPHS AND CAME TO A FEW CONCLUSIONS

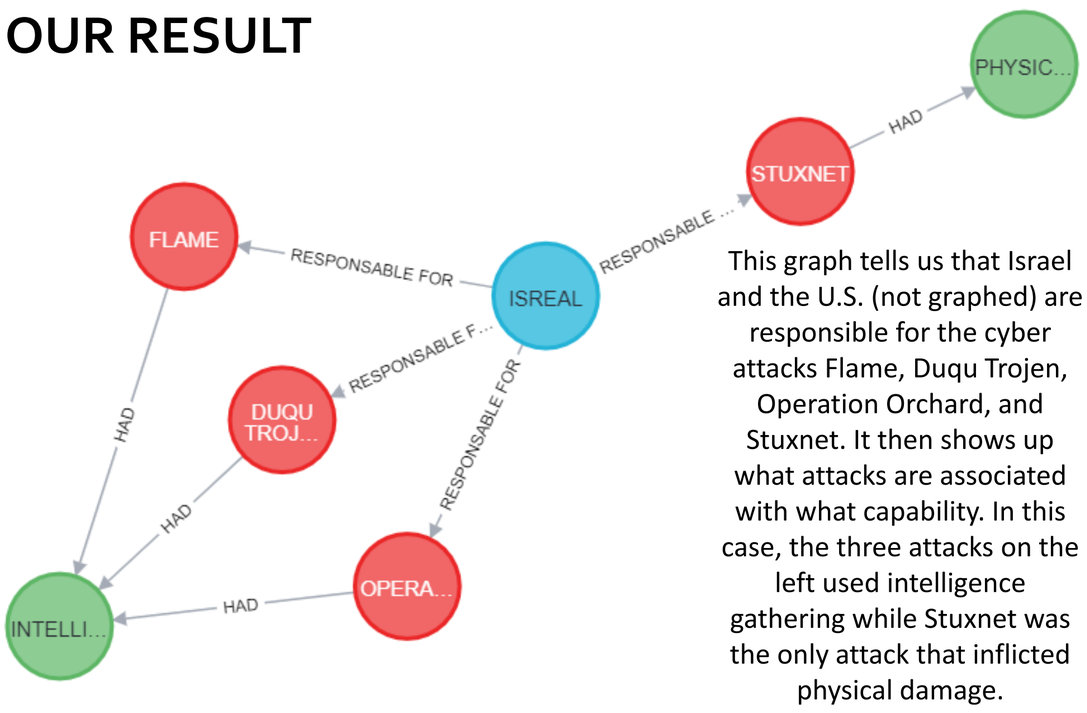


OUR FIRST QUESTION WE WANTED TO ASK NEO4J: WHAT ARE THE ATTACKS WHERE ISRAEL AND THE UNITED STATE HAVE USED CYBER IN AN OFFENSIVE WAY? WHAT WERE THE CAPABILITIES OF EACH ATTACK?

WHAT WE PUT INTO NEO4J

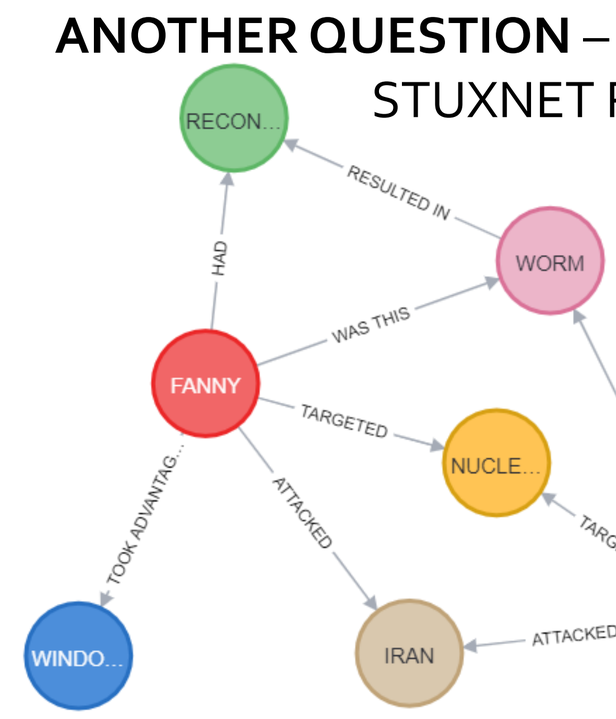
```
neo4j$ match (p:`KEY PLAYERS`{PLAYERS:'ISREAL'})-[:`RESPONSABLE FOR`]→(n:`ATTACK NAME`)-[:HAD]→
       (C:CAPABILITY)  RETURN p,n,C
```

OUR RESULT



This graph tells us that Israel and the U.S. (not graphed) are responsible for the cyber attacks Flame, Duqu Trojen, Operation Orchard, and Stuxnet. It then shows up what attacks are associated with what capability. In this case, the three attacks on the left used intelligence gathering while Stuxnet was the only attack that inflicted physical damage.

ANOTHER QUESTION – HOW ARE FANNY AND STUXNET RELATED



This graph tells us how the attacks Fanny and Stuxnet are related. What we discovered is that they are both worms that assisted in a cyber reconnaissance. Both attacked Iran. What is interesting is that each exploited a different vulnerability in either Windows or Microsoft.

War in Ukraine

Cyber warfare has not progressed as a replacement for conventional warfare

Key cyber events
- Industroyer Blackout 2016
- DDoS 23FEB22
- Foxblade 23FEB22

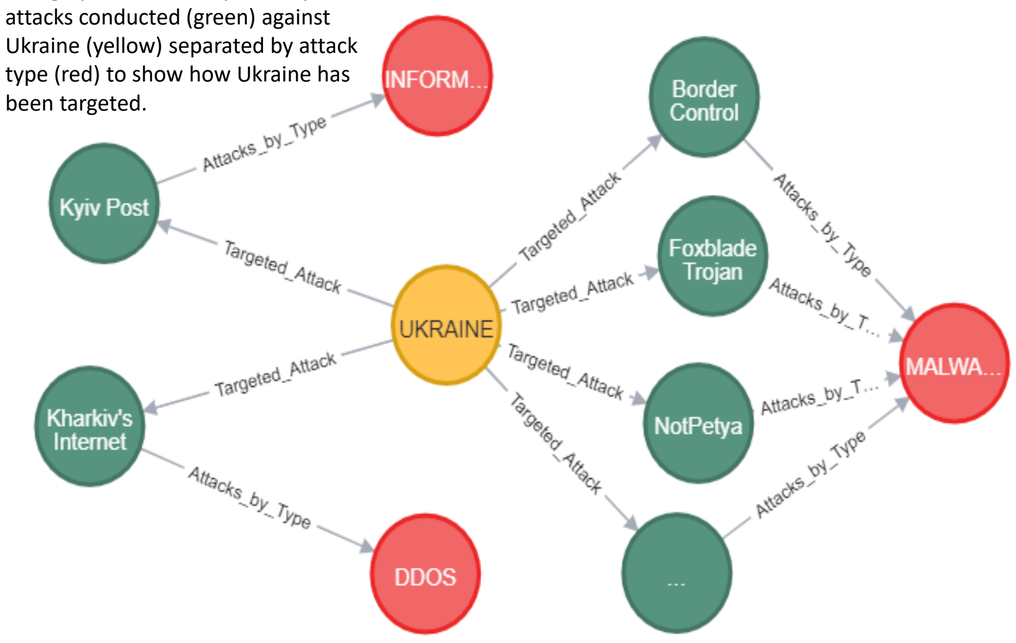
Cyber warfare has focused more on the collection of intelligence and the spread of dis/information.

Russia has depended on Ukrainian cell towers to assist in communication.

What have been the major cyber-attacks on Ukraine prior to and just after the Russian invasion? Based upon the type of attack, is there a specific target Russia has on Ukraine?

```
neo4j$ match (p:`Country`{COUNTRY:'UKRAINE'})-[:Targeted_Attack]→(n:Name)-[:Attacks_by_Type]→(C:Type) Return p,n,C
```

This graph shows the specific cyber-attacks conducted (green) against Ukraine (yellow) separated by attack type (red) to show how Ukraine has been targeted.

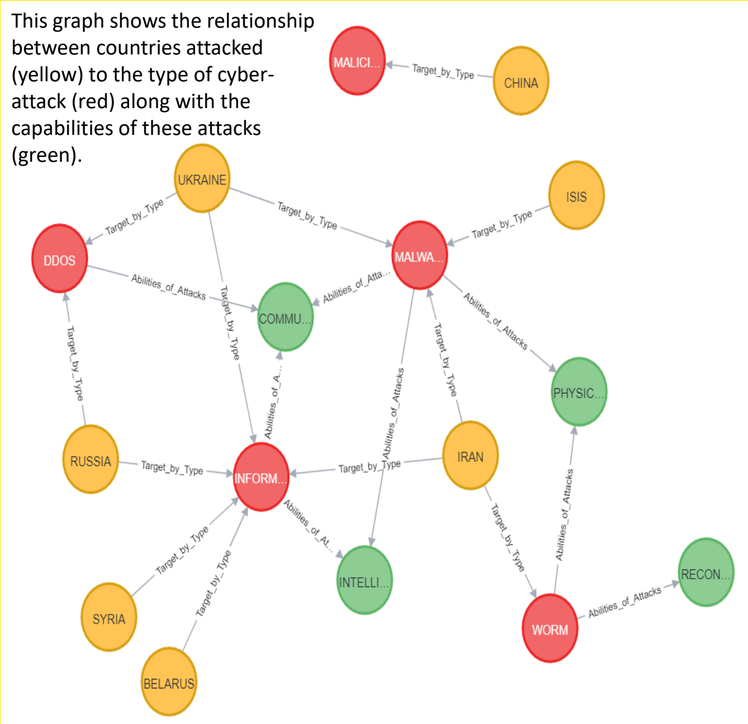


Geopolitics

In geopolitics, the cyberspace presents a secretive and far distant strategy to spy and disrupt both on our adversaries as well as allies. Geopolitical strategies can consist of cyber espionage, cyber attacks, and cyber defense. Key examples are the United States Government worm; Stuxnet and the establishment of the five eyes alliance.

How are the attack capabilities and attack type related the countries attacked?

This graph shows the relationship between countries attacked (yellow) to the type of cyber-attack (red) along with the capabilities of these attacks (green).



OUR SPONSORS

DR. CLEMENTE IZURIETA

ANDREW FALLIN

MONTANA STATE UNIVERSITY

LEADERSHIP EXCELLENCE ARMY ROTC