Strategic Cyber Threat Intelligence - building the situational picture with emerging technologies

Janne Voutilainen, Martti Kari
University of Jyväskylä, Jyväskylä, Finland
japevout@student.jyu.fi
martti.j.kari@jyu.fi

Abstract: In 2019, e-criminals adopted new tactics to demand enormous ransoms from large organizations by using ransomware, a phenomenon known as "big game hunting." Big game hunting is an excellent example of a sophisticated and coordinated modern cyber-attack that has a significant impact on the target. Cyber threat intelligence (CTI) increases the possibilities to detect and prevent cyber-attacks and gives defenders more time to act. CTI is a combination of incident response and traditional intelligence. Intelligence modifies raw data into information for decision-making and action. CTI consists of strategic, operational, or tactical intelligence on cyber threats. Security event monitoring, event-based response, and anomaly and signature-based detection can create the basis of the situation in cyberspace.

To achieve a uniform situational picture, long-term assessment is required. Strategic CTI informs broad or long-term issues and provides situation awareness as well as an analyzed overview of the threat landscape and early warning of cyber threats. This paper describes how the implementation of artificial intelligence (AI) and machine learning (ML) can be utilized in strategic CTI.

The results were arrived at using the design science research methodology. We propose a solution that uses AI as a component of strategic CTI. Furthermore, the paper is a literature survey, integrating research literature on intelligence, cybersecurity, and AI. The paper presents the concept of CTI and its relation to the situational picture of cyberspace. It also addresses the possibilities of natural language understanding for large-scale content analysis and introduces a solution in which an existing enriched dataset provided valuable strategic-level information about an ongoing malicious cyber event.

The paper is part of PhD research concerning comprehensive CTI. Other articles in the dissertation discuss emerging technologies in operational and tactical CTI.

Keywords: Strategic Cyber Threat Intelligence, Machine Learning, Artificial Intelligence

1.Introduction

During the 2000s, cyberspace matured into the fifth domain of warfare, and the volume of criminal activity in cyberspace increased considerably. Cyberspace is not only a technical issue, but it also has a strategic dimension. Cyberspace has expanded warfare to a global scale, beyond the traditional use of military force. The use of force in cyberspace to cause a strategic-level malicious impact does not require state-level resources. The cyber domain differs from other domains of warfare because actors in cyber conflicts are not always military. State actors, criminals, and terrorists attack state authorities, the media, companies, universities, and critical infrastructure. State actors and private cybersecurity companies are fighting against these attackers. The detection of attacks, intelligence collection on them as well as the analysis and attribution of the attacker is often difficult or impossible to do.

A cyber-attack is defined as "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or destroying the integrity of the data or stealing controlled information." Cybersecurity is a process of protecting information by preventing, detecting, and responding to cyber-attacks. The cyber threat is an event or condition that has the potential to cause asset loss and the undesirable consequences or impact of such loss (NISTIR 7298, 2019). Cybersecurity has been based on incident response and security operations (ENISA, 2018) where the focus has been on monitoring security events and incidents and in reacting to detected incidents. Internal threat monitoring has not always provided sufficient time for the defender to be proactive.

Incident response has been the methodology of cybersecurity since the 2010s. Incident response or incident handling means the mitigation of an adverse event in a computer system or network caused by the failure of a security mechanism or an attempted or threatened breach of these mechanisms. In cyber defense based on incident response, the attacker always seems to be a few steps ahead. The prevailing methods of cybersecurity, such as security event monitoring, event-based response, and the anomaly or signature-based detection, will

not improve the situation. The development and implementation of tactics, techniques, and procedures (TTP) of cyber threat intelligence, including intent-based response and detection based on an attacker's behaviour, improve the situation and give a defender the possibility to get ahead of the threat actor.

CTI consists of strategic, operational, or tactical intelligence on cyber threats. Security event monitoring, event-based response, and anomaly and signature-based detection can create the basis of the situation in cyberspace. To achieve a comprehensive situation picture, long-term assessment is required. Strategic CTI informs broad or long-term issues and provides situation awareness as well as an analyzed overview of the threat landscape and early warning of cyber threats. This paper describes how the implementation of artificial intelligence (AI) and machine learning (ML) can be utilized in strategic CTI. The results were arrived at using the design science research methodology. We propose a solution that uses AI as a component of strategic CTI. In 2019 the Finnish Parliament passed new intelligence laws, the implementation of which requires new methods to achieve the goals of national CTI. For that reason, the call for the study stems from practical needs.

2. Methodology

The methodology used in this paper is a combination of the intelligence question and the design science research process (DSRP). The study focuses on the phenomenon known as *big game hunting*. The intelligence question for the study was provided by the National Cyber Security Centre Finland (NCSC-FI). The purpose of the intelligence question was to initiate the intelligence process.

The DSRP is a set of analytical techniques and perspectives for information systems (IS) research. There are two activities in DSRP for improving knowledge in the IS domain: the generation of knowledge through the design of new and innovative things or processes and the analysis of things and processes via reflection and abduction. In the scope of DSRP, an example of things and processes mean algorithms, human/computer interfaces, and system design methods or languages. A common term for objects and processes in the DSRP is an artifact (Vaishnavi, Kuechler et al., 2004).

The DSRP cycle begins with *awareness of the problem*. Usually, the dilemma comes from industry or various areas within the information technology sector. In this study, the problem was initiated by the National Cyber Security Centre Finland (NCSC-FI): the need for a comprehensive threat analysis of the emerging cyberspace phenomenon known as big game hunting. The *proposal* for solving the problem was research concerning emerging technologies in the CTI process.

The second phase of DSRP is the *suggestion* and *tentative design*. For the study, the second phase included the utilization of IBM cloud capabilities in collecting, processing, and analyzing information on strategic cyber intelligence processes.

The *development* of an artifact is based on various questions concerning IBM cloud capabilities. According to McDowell, the data collection for strategic intelligence should be comprehensive, from various sources, with the collected data often being qualitative (McDowell, 2009). For that reason, the selected artificial intelligence subtype was IBM Watson Natural Language Understanding (NLU). As a result of this process, an *artifact* is created. The artifact in this study was a combination of an IBM Watson NLU machine learning model and the strategic cyber threat intelligence process.

The artifact was evaluated with *performance measures*. The purpose of the study was to evaluate the suitability of IBM Watson when used in CTI. The performance measures were based on the following questions: Can the artifact find related information from the data? Can the artifact analyze and process the collected data? Can the artifact provide enough information for the intelligence direction and its sub-questions?

The *conclusion* from the first DSR cycle was that the ML model created according to the intelligence direction did not provide enough reasonable information for the intelligence question. As a result of insufficient data, a new DSR cycle was initiated. According to DSRP knowledge flows in figure 1 (Vaishnavi, Kuechler et al., 2004), in the development of the improved artifact the missing properties were improved by using a IBM Watson Discovery News pre-enriched dataset. The second solution fulfilled *performance measures.* As a result of the queries conducted from the data, new and valuable information about big game hunting was found.

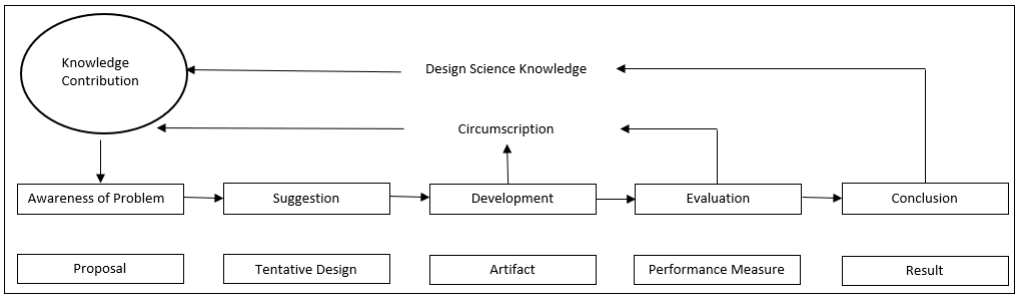

Figure 1: design science research process

3. Cyber Threat Intelligence

According to European Union Agency for Cybersecurity (ENISA, 2018), cyber threat intelligence, even though it is still evolving and in the early adoption phase, is becoming a critical part of cybersecurity capabilities and activities. There is no widely accepted definition of cyber threat intelligence (CTI). ENISA's definition of CTI is as follows: "Cyber threat intelligence is the process and product resulting from the interpretation of raw data into information that meets a requirement as it relates to the adversaries that have the intent, opportunity, and capability to harm" (ENISA, 2018).

CTI includes information on a threat actor's TTPs, threat indicators on impending or ongoing cyber-attacks or on successful compromise, and security alerts and threat reports (Jasper, 2017). TTPs describe the tactical and technical activities of an actor, including their tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism (e.g., phishing or watering hole attack), or exploit. Tactics are the description of the way an adversary carries out his attack from the beginning, i.e., from reconnaissance to the end, command, control, and action on objectives inside the compromised information system. Techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, more highly detailed description in the context of a technique.

The challenge for CTI is the enormous volume, velocity, and diversity of different data sources. An organization's network can generate petabytes of data per second and CTI has to be capable of detecting a threat from among all of this traffic. The data are collected from many sources, and the format of the collected data may vary as well. This requires a process for collecting and analyzing data in a timely fashion and creating CTI products which adequately support decision-making. The sources of CTI are typically open data sources, commercial feeds, shared intelligence, and asset information (Doerr, 2018).

CTI can be considered a combination of incident response and traditional intelligence. The purpose of CTI-based defense is, in the best case, to get ahead of the malefactor or to at least be ready if a cyber-attack occurs. Alan Breakspear, the President of the Canadian Association for Security and Intelligence Studies (CASIS), has stated that intelligence is misunderstood and too often focused only on threats, missing opportunities for advantage. His proposal for a definition of intelligence is the following: "Intelligence is a corporate capability to forecast change in time to do something about it. The capability involves foresight and insight, and is intended to identify impending change which may be positive, representing opportunity, or negative, representing a threat" (Breakspear, 2012).

Intelligence is a process, described by the intelligence cycle. The intelligence cycle is the process of developing raw data into information and delivering this information (i.e., intelligence) to policymakers to use in decision-making and action. The aim is to increase the knowledge and, in the best case, the wisdom of decision-makers by providing them with objective intelligence at the right time. The intelligence cycle consists of several steps, with Mark Lowenthal presenting a cycle that consists of seven phases. These phases are identifying and setting requirements, collection, processing and exploitation, analysis and production, dissemination, consumption, and feedback. In this paper, the information collection, procession, exploitation, and analysis are included in the evaluation of the AI capabilities.

Identifying and setting requirements means defining and prioritizing requests for information by the clients, that is, the questions to which intelligence is expected to answer. Collection means information or data gathering

from diverse sources, including open-source data. Processing and exploitation mean the process of converting the collected data for analysis. Conversion can include translations, decryption, interpretation, and evaluation of data. Evaluation means assessment of the type, quality, and format of data (information) in a way that promotes reliability and prevents supposition. In the analysis and production process the collected data is processed by appropriate analysis techniques and compiled to the intelligence product. In dissemination, the intelligence product, responding to the client's request for intelligence, is distributed to clients. A dialogue between clients and intelligence producers should continue during the whole process. Feedback from the client indicates how well their intelligence requirements are being met.

CTI is the process of collecting, analyzing, and disseminating intelligence on cyber threats to protect information and information systems by preventing and detecting cyber-attacks. The purpose of CTI is to understand the attacker and attacks, help anticipate future actions and plan a response and cyber defense. CTI can be illustrated and explained in the seven-phase process described by Lowenthal. Like all intelligence, CTI produces accurate, timely, and relevant intelligence, improves cyber threat information and supports the client in identifying threats and opportunities. CTI can be strategic, operational, or tactical.

Strategic cyber threat intelligence is typically non-technical, risk-based intelligence on broad or long-term issues and provides an overview of the threat landscape. It might also provide early warning of threats. Strategic cyber threat intelligence constructs a situation picture of the intent and capability of cyber threats. A strategic cyber threat picture can include information on geopolitical events and trends, combining cyber-attacks on geopolitical conflicts and events, information on malicious actors, threat actor tactics and targets, tools, and Tactics, Techniques and Procedures (TTP)s and their changes over time, and trends and patterns of emerging threats and risks (CIS, 2019). Strategic CTI analyses trends, emerging risks while creating and updating a strategic-level situation picture of the possible broad impacts and consequences of cyber-attacks. Strategic CTI differs from other CTI categories because it is mainly non-technical and produced for senior leadership instead of technical personnel. Typical strategic CTI products are policy papers, white papers, assessments, and threat reports which present a strategic cyber threat picture.

Strategic CTI requires a human element because it is time-consuming to evaluate and test new adversary TTPs against existing security controls. Parts of the process of strategic threat intelligence can be automated, but an intelligence analyst is needed for the production. Strategic CTI focuses on assessing and mitigating current and future risks to operations and businesses by answering the questions of who is causing the cyber threat and why.

The products of strategic CTI include assumptions about the nature and role of the cyber-attacks and the attacker, and about the threat posed by the attacker. The aim is to support decision-making about which defensive measures will be the most effective. Strategic CTI also supports security policy planning and implementation as well as resource allocation.

Operational CTI assesses specific, potential incidents related to events, investigations, or activities. Operational CTI relates to specific attacks or campaigns and answers the questions of how the threat is created and where it is projected. It helps defenders understand the nature, intent, and timing of a specific attack, and also provides insight into the nature and sophistication of the groups) responsible. In many cases, however, only partial context can be obtained (Recorded Future, 2018). Operational intelligence is often related to campaigns, malware, and tools, and may come in the form of forensic reports. Operational intelligence is also referred to as technical threat intelligence because it can include technical information about cyber attacks. Technical information can include attack vectors, exploited vulnerabilities, and command and control domains used by the attacker.

Tactical CTI is intelligence on real-time events, investigations, or activities. It answers the question of why and provides support for day-to-day operations and events, such as the development of signatures and indicators of compromise. Typical indicators of compromise are the presence of malware, signatures, exploits, vulnerabilities, and IP addresses. Indicators of an attack, such as code execution, persistence, stealth, command control, and lateral movement within a network, are early warning signs that an attack may be underway or has already occurred.

The cyber kill chain model, published by Lockheed Martin in 2011, has been the most used framework to explain the phases and process of a cyber-attack. In the kill chain model, the cyber-attack consists of seven phases. In reconnaissance, the attacker selects and researches a target and identifies vulnerabilities of the target network. In weaponization, the attacker creates remote access malware weapons tailored for the identified vulnerability. The attacker delivers the malware to the target system where the malware exploits the identified vulnerability and installs access points to the target system. The attacker then uses this access point to gain command and control of the target system and starts actions to achieve their goals as data exfiltration, data destruction, or encryption for ransom (Hutchins, Cloppert & Amin, 2011). The ultimate goal of the CTI process is to produce a situational picture of cyberspace. Notably, it is the changes in events that belong to the scope of the process.

Since the beginning of the decade, defining a cyberspace situational picture has been one of the most popular topics in research on cyberspace. From the perspective of this paper, we are interested in the *change* for in cyberspace situational pictures and AI-based technologies that can be used to create the situational picture with CTI. Finally, we want to find a solution for evaluating the shift in the situational picture. According to Bartch et al (2018), with a decent situational picture, it is possible to obtain situational awareness that contains the latest information about risk landscape, vulnerabilities, and cyber defense capability readiness (Bartch et a,l 2018).
According to JP 3-12, a detailed, accurate and comprehensive situational picture of cyberspace operations is the key element for correct decision-making in a dynamic and continuously developing environment. The observation of adversarial behavior is based on signals intelligence (SIGINT) and analysis of exploitations (Joint Chiefs of Staff, 2018)
As in Figure 2, the JP 3-12 definition of the observation of adversarial behavior positions itself as tactical CTI, analyzing the dataflow. Tactical CTI is the most critical way to make observations from cyberspace, but operational and strategic CTI should not be underrated.

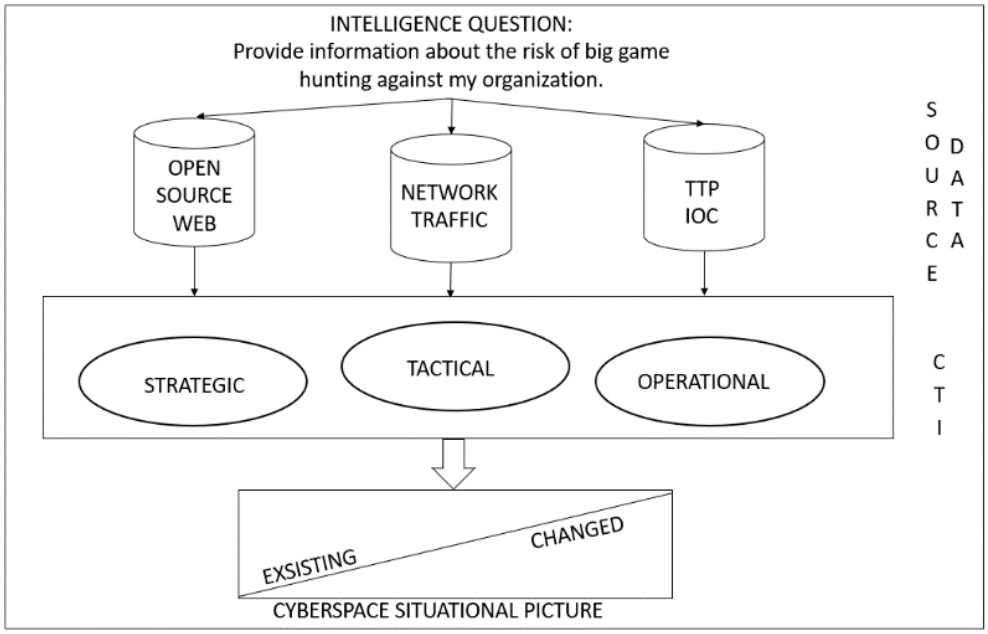

Figure 2: Relation of CTI and cyberspace situational picture

4. AI based solutions for strategic CTI

When the phases of the strategic cyber intelligence process are observed from the perspective of AI-based technologies, the first phase, intelligence direction, requires human capabilities to initiate the intelligence process. Despite the continually growing speed of the technology, initiation requires a human. Intelligence direction is usually a task that is shaped as an intelligence question. In the 2019 cyber threat landscape, the malicious phenomenon known as big game hunting appeared. It refers to the launching of ransomware attacks against large organizations to obtain a significant amount of money in bitcoins (Feeley, Hartley et al., 2019). The intelligence direction from decision-makers in large organizations might be, for example, “Provide information about the risk of big game hunting against my organization.”

The idea of using AI in strategic intelligence is presented in *Strategic Intelligence: Business Intelligence, Competitive Intelligence, and Knowledge Management* (Liebowitz, 2006) It states that AI can improve knowledge management for making strategic decisions in various organizations.
The first point in the strategic intelligence cycle where AI-based technology can be used is information collection. According to McDowell, the volume of collected data for strategic intelligence might be significant and the data requirements are complicated. Furthermore, the collection should happen from all possible sources and the collected data might be qualitative, anecdotal, or even impressionistic (McDowell, 2009).
In this study, two alternatives for utilizing AI for strategic cyber intelligence are presented. Both solutions were arrived at using the DSRP. The first solution did not pass the performance measures. For that reason, the DSR cycle was initiated again. In the second solution, the approach was dissimilar. Instead of using limited source data, a dataset called IBM Watson Discovery News, which updates continuously, was used. As a result, the second solution proved to be suitable for strategic CTI.

4.1. The first solution

In the first solution, the source data were provided by NCSC-FI. The data included 1,300 cybersecurity documents from various internet sources. For analyzing the data and documents, an ML-type system was created in the IBM cloud. The type system consists of entities and their relations. The selection of entities and relations was based on an estimate of how the type could support the intelligence question in the best way. The type system used is presented in Figure 3.

The type system was annotated with reliable ransomware-related documents published by the European Union Agency for Cybersecurity (ENISA). Annotation is a task where the training data words and relations are linked to the correct entity and relation as in figure 4. Finally, the model was trained to find entities and relations from new documents. Once adequate accuracy was achieved, the model was deployed to Watson Discovery, where the queries were conducted from the 1,300 documents that NSCS-FI provided.

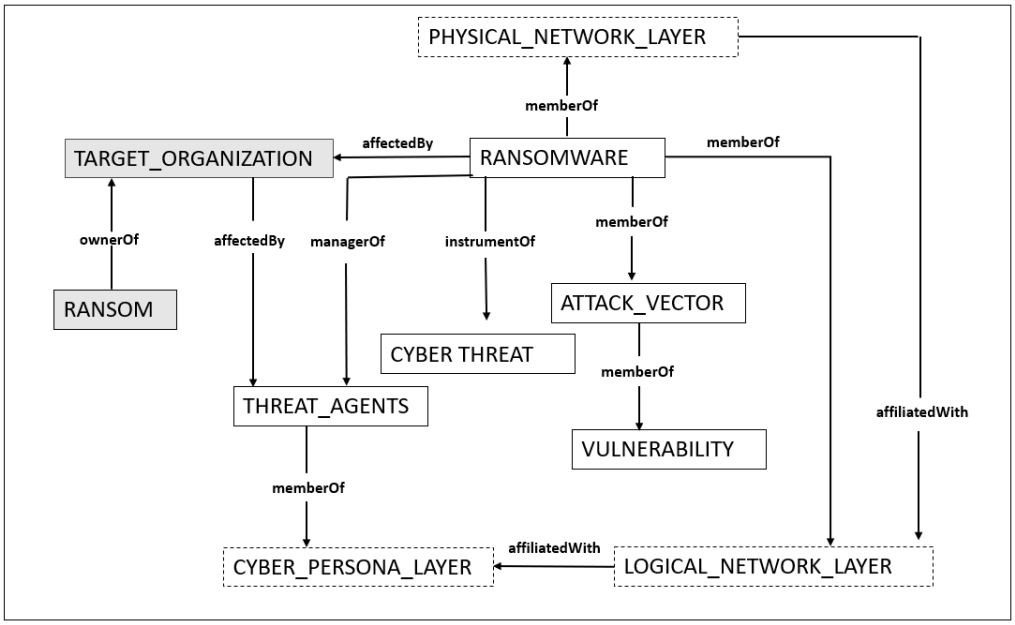

Figure 3: Type system

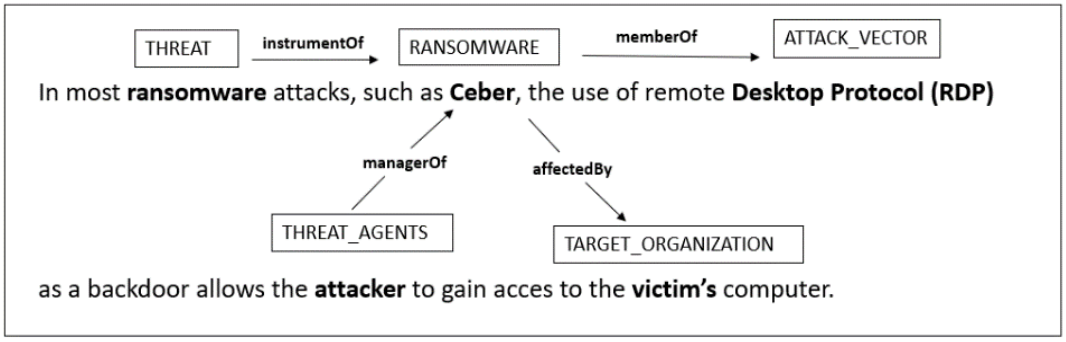

Figure 4: Annotation

As a result, the model was able to find new information from the documents. An interesting observation was the passages. Passages are short sentences that match the best way to the query. For example, when the data was queried with the words *ransomware* and *big game hunting*, Watson returned passage: *"Both INDRIK SPIDER (with BitPaymer ransomware) and GRIM SPIDER (with Ryuk ransomware) have made headlines with their high-profile victims and ransom profits, that big game hunting is a lucrative enterprise."* The disadvantage in the first solution was the amount of data. The 1,300 documents used were insufficient for the required in-depth analysis of strategic cyber intelligence. Instead, the corresponding approach would be suitable for operational cyber threat intelligence, where the source data might be, for example, forensic reports. The organizations that require high security for data might use similar solutions for tracking phenomena similar to big game hunting by using their data. The conclusion from the first solution was that IBM Watson can be used for information processing and analyzing phases of the strategic intelligence process. In the solution, the collection phase of the strategic intelligence process was not tested since NCSC-FI initially vetted the dataset. There is an application programming interface (API) included, but it was not used in the solution. Theoretically, it is possible to disseminate intelligence information via the API to the appropriate application.

4.2 The second solution

The approach to the second solution was different and it proved to be more efficient. The IBM Watson Discovery News dataset was used as source data for the second solution. The data are public, including over 14,000,000 documents, and the sources for the dataset are in five languages. The majority of the documents are from English news sites that are updated continuously. The oldest information in the Watson Discovery data is 60 days old. The data changes every day, with IBM adding approximately 300,000 new articles from news and blogs daily (Scherping, 2017).

The main difference compared to the data that were used in the first solution is that Watson Discovery News does not support corresponding custom models that were used in the first solution. Further, Discovery News cannot be trained, so there is no possibility to add documents and the dataset cannot be configured for specific use cases. Still, according to IBM documentation, the proposed use cases for Discovery News are news alerts, event detection and obtaining data from trending topics (IBM, 2019). These features are a good fit for strategic cyber threat intelligence. The data in Watson Discovery News include multiple issues from various areas, in addition to cybersecurity-related documents.

Various queries were tested in the second solution. When the correct queries were found, Watson Discovery News quickly provided the required information. The Discovery service uses a query language that is based on JavaScript Object Notation (JSON). In addition, the queries can be made with a graphical interface. The following example query was used to obtain information about the intensity, geographical location, and time perspective of the phenomenon: "Find the number of documents that include the words *big game hunting* and *ransomware*. Aggregate the results by the publishing date and the country where the document has been published and show the top five results." The returned information is presented in figure 5. The result gives a rough guideline of how big game hunting has developed during the first half of 2019. The obtained trend proved to be correct even when the time and geolocation were compared to the number of documents.

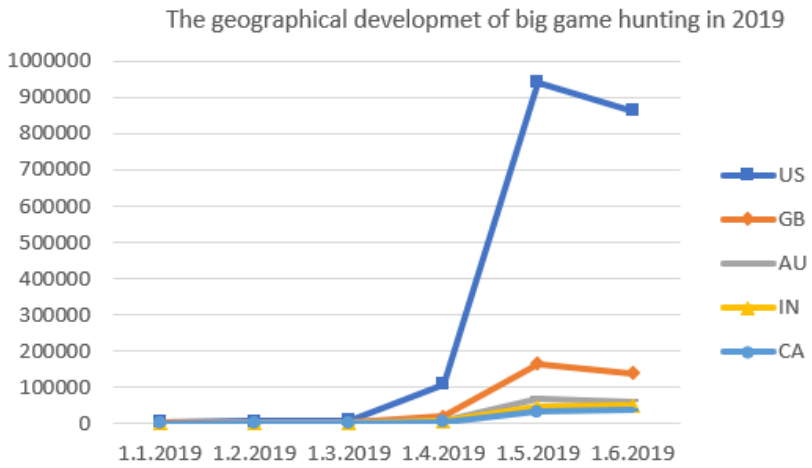

Figure 5: The geographical development of big game hunting in 2019

5. Conclusions

To achieve a uniform situational picture from cyberspace events, the need for emerging technologies is evident. All three components – strategic, operational and tactical – are equally important. Strategic CTI requires information from all available sources. The amount of data is enormous and, with human capabilities, it might be extremely difficult to find the required intelligence information from the source data.

In the study, IBM cloud was used as a platform to collect, process and analyze the data for intelligence direction. Both presented solutions based on machine learning. In the first solution, *An ML model that is planned according to intelligence direction to provide information about big game hunting*, the restricted dataset was queried with an NLU-based model from initially vetted data. The model functioned, but it did not provide enough information that could be used for the intelligence question. It was based on supervised learning, where the data labels are created for the training data. When new data was ingested in Watson Discovery News, the service classified the documents according to the labels. Moreover, during the ingestion, the service created labels using unsupervised learning. The queries that were conducted with unsupervised learning based on labels produced during ingestion provided almost identical answers to the queries. From that perspective, unsupervised learning is a better alternative, because creating a supervised learning-based model is laborious. The model in the first solution might be used in organizations that use closed environments and require high data security.

The second solution, *Targeted queries from Watson Discovery News to answer an intelligence question concerning big game hunting*, proved to be useful for strategic CTI. First, the amount of data met the requirement for source data. Second, the data are updated continuously, which means the ability to obtain an almost real-time situational picture of the investigated phenomenon. Finally, the pre-enriched dataset does not require a separate ML model. In the second solution, the ML capabilities of Watson Discovery News happens when data are crawled from the available sources. The documentation of the IBM CLOUD does not provide details on how the source documents are labelled. Yet, depending on the multiple possibilities of the queries, valuable information within the scope of the intelligence question can be obtained.

The main finding of this paper is the suitability of NLU and text analytics for strategic CTI. There exist multiple similar cloud services where corresponding queries can be made with various documents. Traditionally, data security is an essential role in intelligence, but government intelligence agencies cannot use cloud services that are connected to the internet. They therefore require a service that is as secure as possible for their use. Such cases provide the possibility to develop a tailored text analytics engine for specific needs.

References

Bartsch, M., Frey, S, ed, (2018). Cybersecurity Best Practices. 1 edn. Bern, Swizerland: Springer Vieweg.

Breakspear, A. (2012) A New Definition of Intelligence. *Intelligence & National Security*, Volume 28, 2013 - Issue 5, p678-693. [Online]. Available at: https://doi.org/10.1080/02684527.2012.699285 (Accessed: 05 November 2019).

CIS. (2019) Center for Internet Security, Inc. What is Cyber Threat Intelligence? [Online]. Available at: https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/ (Accessed: 05 November 2019)
Doerr, C. (2018) Cyber Threat Intelligence Standards. - A high-level overview. TU Delft. [Online]. Available at: https://www.enisa.europa.eu › cti-eu-2018-presentations (Accessed: 21 December 2019).
ENISA. (2018) Exploring the opportunities and limitations of current Threat Intelligence Platforms. [Online]. Available at: https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms (Accessed: 05 November 2019).
Feeley, B., Hartley, B. and Frankof, S., -03-06T00:04:48+00:00, 2019-last update, PINCHY SPIDER Adopts "Big Game Hunting" to Distribute GandCrab. Available at: https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/ (Accessed: 05 July 2019).
Hutchins, E, Cloppert M and Amin, R 2011. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Lockheed Martin Corporation*. [Online]. Available at: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf (Accessed: 05 November 2019).
IBM. (2019) IBM Cloud Docs. Available at: https://cloud.ibm.com/docs/services/discovery?topic=discovery-about (Accessed: 02 July 2019).
Jasper, S. (2017) *Strategic Cyber Deterrence: The Active Cyber Defense Option*. London: Rowman & Littlefield Publishers.
JOINT CHIEF OF STAFF, 2018-last update, JP 3-12, Cyberspace Operations, 8 June 2018 - jp3_12.pdf. Available: https://fas.org/irp/doddir/dod/jp3_12.pdf. (Accessed: 10 November 2019)
Liebowiz, J., (2006) *Strategic Intelligence : Business Intelligence, Competitive Intelligence, and Knowledge Management.* London: Auerbach Publications.
Lowenthal, M. (2006) Intelligence Cycle and Process. [Online]. Available at: https://www.e-education.psu.edu/sgam/node/15 (Accessed: 07 November 2019).
McDowell, D., (2009) *Strategic intelligence: a handbook for practitioners, managers, and users.* Rev. edn. Lanham (Md.): Scarecrow Press.
NIST. (2018) SP 800-150 GUIDE TO CYBER THREAT INFORMATION SHARING. [Online]. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf (Accessed: 05 November 2019)
NISTIR. (2019) NISTIR 7298. National Institute of Standards and Technology. [Online]. Available at: https://csrc.nist.gov/glossary/term/Cyber-Attack (Accessed: 05 November 2019).
Recorded Future. (2018) How Operational Threat Intelligence Blocks Attacks Before They Happen. THE RECORDED FUTURE TEAM. [Online]. Available at: https://www.recordedfuture.com/operational-threat-intelligence/ (Accessed: 05 November 2019).
Scherping, J., -04-13, 2017-last update, Out of the box, Discovery provides a pre-enriched collection of 2 months of internet news content. Available: https://www.ibm.com/blogs/watson/2017/04/box-discovery-provides-pre-enriched-collection-2-months-internet-news-content/ (Accessed: 05 May 2019).
Vaishnavi, V., Kuechler, B. and Petter, S., 2004. Design Science Research in Information Systems. (2004/17), pp. 1-62.