Designing Cyber Profiling of Terrorism using TelegramBot and Open Source Intelligent (OSINT)

Preprint · January 2020

DOI: 10.31227/osf.io/2g4fk

3 authors, including:

Faulinda Nastiti
Universitas Duta Bangsa Surakarta
15 PUBLICATIONS **38** CITATIONS
SEE PROFILE

Dedy Hariyadi
Universitas Jenderal Achmad Yani Yogyakarta, Indonesia
65 PUBLICATIONS **149** CITATIONS
SEE PROFILE

Designing Cyber Profiling of Terrorism using TelegramBot and Open Source Intelligent (OSINT) – IIDSS2019

Faulinda Ely Nastiti[1], Fazlurrahman[2] and Dedy Hariyadi[3]

[1]Universitas Duta Bangsa Surakarta, Indonesia
[2]Komunitas NgeSec Yogyakarta, Indonesia
[3]Universitas Jenderal Achmad Yani Yogyakarta, Indonesia

E-mail: [1]faulinda.en@gmail.com, [2]fazlurbima@gmail.com, [3]milisdad@gmail.com

Abstract. The pattern of communication by cellular service users has changed. This also affects the communication media used. Short Message Service (SMS) used to be quite popular as a communication media. However, at this time began to shift its use to instant messengers. SMS was used as a notification system but has now used instant messenger. The use of Bots makes it easy for software developers to create notification systems using instant messengers. Telegram is an instant messenger that makes it easier for software developers to use the Bots API. Given free access to the Telegram Bots API (BotFather) developers can make various kinds of Bots. In this study the Bots API was used to distribute information from OSINT Source regarding acts of terrorism in Indonesia. OSINT Source which is unstructured data is extracted and processed into structured data, then the data can be accessed as information via mobile via Telegram instant messenger.

1. Introduction

Terrorism is an action taken by an organized person or group of people, through means / ways of violence, with the aim that their wishes are heard and can be implemented by the government. [1]. The characteristics of acts of terrorism include creating fear by means of violence and threats. The action is directed to all elements, both individual and mass, instructing its members to terrorize too. The actions taken aim to show that the actions carried out are organized and systematic [2]. The strategy to prevent terrorism can be done with two approaches, namely the hard approach and soft approach. Hard approach can be in the form of prosecution and law enforcement against perpetrators of acts of terrorism. Soft approach can be in the form of guidance to the community through deradicalisation programs, monitoring the flow of suspected terrorist funds or networks and mapping patterns of movement through social media platforms [3].

In our previous research on Malware attacks, we identified that the use of OSINT Source in terrorism crimes can determine patterns of movement of perpetrators of crime [4]. This can be categorized as criminal profiling in cyberspace [5]. Criminal Profiling is a forensic technique that seeks to provide specific information to investigative institutions that will help focus attention on individuals with personality traits that are parallel to other actors who have committed other similar violations [6]. By utilizing OSINT Source about terrorism crime, in this study we propose making TelegramBot to assist in the process of Cyber Profiling acts of terrorism in Indonesia.

Criminal profiling does not only have a role in investigating traditional crime. However, criminal profiling in cyberspace can help investigators provide clues to previous patterns of crime [7]. Criminal profiling in cyberspace or cyber profiling is one of the efforts made by investigators, to find out the allegations of violators through analysis of data patterns covering aspects of technology, investigation, psychology, and sociology. The benefits of cyber profiling on a crime include [8]:

1. Identification of perpetrators of crimes related to previous crimes.
2. Mapping family subjects, social life, work, or network-based organizations, including those who work for them.
3. Provision of information about users about their abilities, threat levels, and how vulnerable they are to threats.

Telegram Instant Messenger via Bot API makes it easy to develop short message-based applications via Telegram as its interface. Bots that are created can run code with a specific purpose that has been prepared on the server. Communication with Bot API with Bot server through simple HTTPS-interface [9]. TelegramBot has been used as a tool to support various main applications, such as notifications or reminder that run automatically, crawling data on malware attacks in Indonesia [4] and so on. In this study TelegramBot was used as an information medium to support cyber profiling related to acts of terrorism.

The definition of Open-source Intelligence (OSINT) according to the US Department of the Army is an intelligence discipline related to intelligence that results from publicly available information that is collected,

exploited, and disseminated in a timely manner to the right audience for the purpose of addressing information needs and special intelligence. OSINT's characteristics in supporting defense operations include providing an open information platform to support the sustainability of intelligence information, the availability of information without technical capabilities, strengthening information gathering, and increasing productivity [10]. Corporate Computer Security Incident Response Team (CSIRT) from NTT Secure Platrform Laboratories every day collects information sources or OSINT Source which are then analyzed and presented in the form of information trends [11]. Similar to the framework of the Cyber Threat Inspection Framework for Critical Infrastructure in Korea which divides four stages, namely: Establishment of OSINT Plan, Preparation of OSINT, Collecting Information from Open Source, and Generating Security Intelligence [12].

2. Methods

In this study there are two main actors namely user and operator. The user is the accessor of information about the acts of terrorism in Indonesia through Telegram instant messenger. Operators are people behind the scenes who are looking for information sources of terrorism crime, especially in Indonesia, using a crawler agent and collecting that information to be processed into information that is ready to be presented through Server Bot. The actor's workflow on this system can be seen in Figure 1.

Bot Server is built on the GNU/Linux operating system with the Python programming language which has a lot of library support. Therefore Python has been named the most popular programming language according to TIOBE [13]. The library used in this study is Telepot which functions to call API Tokens from BotFather [14]. Information on acts of terrorism in Indonesia is presented in accordance with the Telegram Client interface on each user's device. Telegram Client can use a Smartphone or web-based Client Telegram.

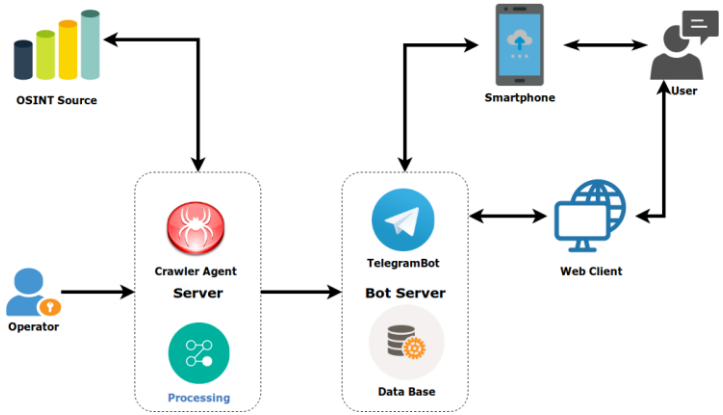

Figure 1. Cyber Profiling Workflow Using TelegramBots

3. Result and Discussion

The implementation of cyber profiling of terrorism crimes using TelegramBot is divided into three scope of work, namely Main Server, Server Bot and User. OSINT Source which is currently used is still one source, namely the Global Terrorism Database (GTD). GTD is an OSINT Source product from the National Consortium for the Study of Terrorism and Response to Terrorism University Maryland America which records terrorist acts in the world from 1970 to 2017 [15].

3.1 Main Server

This section requires an operator that extracts data from OSINT Source, the Global Terrorism Database using a crawler agent. Files generated from the data extraction process are in the form of Comma Separate Value (CSV) [16]. The data extraction results are processed to produce more structured data, mainly focused on acts of terrorism that occurred in Indonesia. The data structures compiled are Events, Cities, Terrorism Groups, Target Types, Attack Types, and Weapon Types. If the data is in accordance with the structure, the data is exported to Server Bot.

Data on acts of terrorism that have occurred in Indonesia since 1977 until 2017 amounted to 761 attacks. The focus of this study presents information related to Target Type, Attack Type and Weapon Type. Source data from GTD Type Targets that have occurred in Indonesia are twenty-one types, namely: Business, Religious Figures / Institutions, Police, Business, Private Citizens & Property, Government (Diplomatic), Government (General), Maritime, Utilities, Journalists & Media, Military, NGOs, Educational Institutions, Transportation, Tourists, Violent Political Party, Food or Water Supply, Airports and Aircraft, Terrorists / Non-state Militia, Western Europe, and unidentified attacks. The attack type is divided into nine attacks, namely Armed Assault, Bombing / Explosion, Hostage Taking (Barricade Incident), Facility / Infrastructure Attack, Assassination, Unarmed Assault, Hostage Taking (Kidnapping), Hijacking, and unidentified attacks. While the target type is divided into eight targets Firearms, Explosives / Bombs / Dynamite, Melee, Firearms, Incendiary, Chemical, Vehicle, and random targets.

3.2 Bot Server

Bot Server that is built based on services, while the main services are TelegramBots and Databases. TelegramBot is built using the Python programming language with the support of Telepot libraries. This research is still in the design stage so that the database system still uses text files. Future research can use a more complex database system such as Relational Database Management System or Non Relational Database.

Bot activation is done by the operator by installing Telegram Instant Messenger first. Then request the API Token by chatting with the BotFahter account. API tokens that have been obtained are called using Telepot libraries such as more or less the code as below.

```
import telepot

bot =
telepot.Bot('123123123121:AAAAVVVBBGV2vchhGGSgg_v
sgdvgs')

bot.getMe()
```

In addition to functioning to call API Tokens, Telepot libraries also have a Custom Keyboard function. In the Bot Server the Custom Keyboard function is used to make a selection button that makes it easier for the User to choose a predetermined Menu. The list of options menu can be seen while the general process from the TelegramBot Menu appears in Figure 2.

Table 1. Register the TelegramBot Command Menu

No	Menu	Description
1.	Target	View a list of target types
2.	Attack	See a list of types of attacks
3.	Weapon	See a list of types of weapons used

TelegramBot that is designed in research is a bot that can only be accessed on a Chat Groups. The purpose of Bots can only be accessed on Chat Groups is to reduce the burden of Bots in processing the information presented. In addition, the data presented can be used as material for discussion at the Chat Groups of Terrorist Crime Analysts.

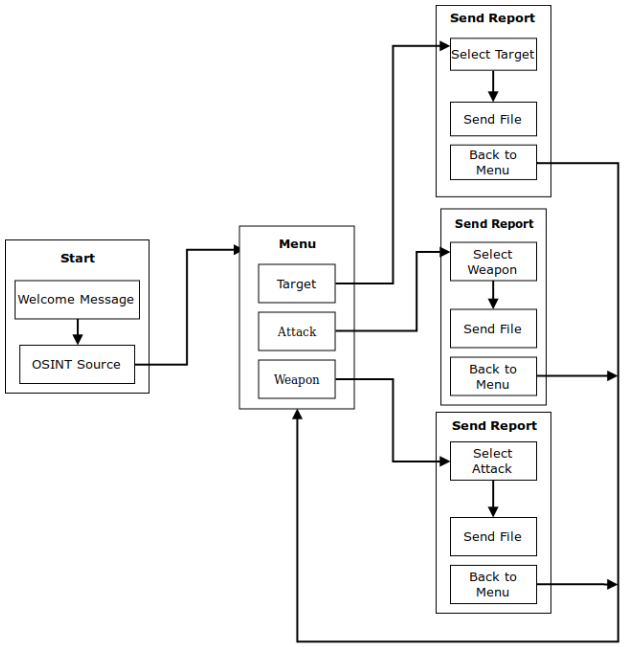

Figure 2. General Process TelegramBot

The bot server is also equipped with an information access log. This aims to facilitate monitoring or investigation if there is misuse of information that does not comply with the rules that apply to an organization. The format of the user log information on Terrorism Crime Bots is Date, Time, User ID and Request Message as shown in Figure 3.

```
24-5-2019 09:34:45 Chat-id - 575519994 Text - target Sender - UnjaniYK
24-5-2019 09:34:45 Chat-id - 575519994 Text - back Sender - UnjaniYK
24-5-2019 09:46:09 Chat-id - 575519994 Text - senjata Sender - orangmiliter
24-5-2019 09:47:21 Chat-id - 575519994 Text - back Sender - orangmiliter
24-5-2019 09:47:21 Chat-id - 575519994 Text - serangan Sender - orangmiliter
24-5-2019 09:47:21 Chat-id - -223857708 Text - back Sender - orangmiliter
24-5-2019 09:47:21 Chat-id - -223857708 Text - senjata Sender - UnjaniYK
24-5-2019 09:47:21 Chat-id - -223857708 Text - target Sender - milisdad
24-5-2019 09:47:21 Chat-id - -223857708 Text - back Sender - milisdad
24-5-2019 09:47:21 Chat-id - -223857708 Text - back Sender - UnjaniYK
24-5-2019 09:47:21 Chat-id - -223857708 Text - serangan Sender - UnjaniYK
24-5-2019 09:47:21 Chat-id - -223857708 Text - back Sender - UnjaniYK
```

Figure 3. Examples of Access Logs on Bot Server

3.3 User

From the user side who access information on terrorism crime can use two devices, namely smartphones or web clients. The advantages of Telegram instant messenger are that one user does not need to have a smartphone so that it can use the web client from Telegram. Therefore Telegram does not have dependence on Telegram applications on cellphones that must always be on. Users can also access Telegram via smartphones and web clients simultaneously.

To obtain information on acts of terrorism a user must be entered into a chat groupw, for example the "Terrorism Analyst ID". Because the interface is message-based on instant messenger a user can use the TelegramBot menu list. Figure 4 example from the Target menu from TelegramBot, the user can choose the desired target.

Figure 4. Target Menu of TelegramBot

4. Conclusions

TelegramBot was made to facilitate getting information about acts of terrorism that occurred in Indonesia. However, this research still has many shortcomings including still relying on an OSINT Source, the Global Terrorism Database (GTD), not yet implementing a database system in either RDBMS or Non RDBMS, not yet available menu searching for information by date and terrorism groups, and not yet providing data visualization. Currently the information submitted is in the form of text files that are sent via Chat Groups. We hope that these shortcomings can be realized in further research.

References

[1] Armawi A and Anggoro T 2010 Terorisme dan Intelijen *J. Ketahanan Nas.* **XV**

[2] Zamzami S 2013 *Analisis Fatwa MUI Nomor 3 Tahun 2004 Tentang Terorisme* (Universitas Islam Negeri Walisongo Semarang)

[3] Jazuli A 2016 Strategi Pencegahan Radikalisme dalam Rangka Pemberantasan Tindak Pidana Terorisme *J. Ilm. Kebijak. Huk.* **10**

[4] Nastiti F E, Hariyadi D and Fazlurrahman 2019 TelegramBot : Crawling Data Serangan Malware dengan Telegram *J. Comput. Eng. Syst. Sci.* **4**

[5] Papahit H I 2015 Profiling Cyber Pedofil: Saran Pencegahan Kejahatan

[6] Korcis R N 2006 *Criminal Profiling* (Totowa, NJ: Humana Press)

[7] Balogun A M and Zuva T 2018 Criminal Profiling in Digital Forensics : Assumptions , Challenges and Probable Solution *International Conference on Intelligent and Innovative Computing Applications (ICONIC)* (IEEE) pp 1–7

[8] Zulfadhilah M, Prayudi Y and Riadi I 2016 Cyber Profiling using Log Analysis and K-Means Clustering A Case Study Higher Education in Indonesia *Int. J. Adv. Comput. Sci. Appl.* **7** 430–5

[9] Telegram Telegram APIs

[10] U.S.A. Department of the Army 2012 Open-Source Intelligence ATP 2-22.9 **2-22.9** 91

[11] Kamiya I 2016 OSINT (Open Source Intelligence) Activities in Corporate CSIRT

[12] Lee S and Shon T 2016 Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures *FTC 2016 - Proc. Futur. Technol. Conf.* 1030–3

[13] TIOBE February Headline: Groovy re-enters the TIOBE index top 20

[14] Telepot Introduction — telepot 12.7 documentation

[15] University of Maryland Overview of the GTD

[16] Shafranovich Y 2005 *Common Format and MIME Type for Comma-Separated Values (CSV) Files*