THE SENTINEL PROJECT
FOR GENOCIDE PREVENTION

For Analysts and Volunteers

THREATWIKI ANALYST'S GUIDE

Threatwiki V. 1.0

Copyright

Change Log

Version	Authors	Description of Change	Date
1.0	Daniel Friedman	Original author	6.30.2011

Purpose

This document is meant to instruct internal members of the Sentinel Project on how to use Threatwiki to help support our genocide monitoring efforts. It provides Research Analysts with instructions on how to:

- Access Threatwiki.
- Work with datapoints, locations, links, and tags.
- Tag datapoints according to the Sentinel Project's Operational Process model.
- Create and edit datapoints according to Threatwiki's online publishing guidelines.

This document will also be useful for Threatwiki administrators, who may at times be required to perform the procedures included. Administrators should also refer to the Threatwiki Administration Guide for instructions on procedures specific to them.

This document assumes that users are volunteers, members, or partners of the Sentinel Project that are familiar with the organization and its mission, values, and policies. Please see the 1 – For Volunteers folder on Dropbox for this information.

Feedback

If you have any comments or suggestions on how to improve this document, please email them to daniel@thesentinelproject.org.

TABLE OF CONTENTS

LIST OF FIGURES

1.0 THREATWIKI OVERVIEW

Threatwiki is a set of analytical tools used to support the Sentinel Project's genocide prevention efforts. Threatwiki is an open-source, online application that tracks event data and aggregates it into a coherent narrative. It stores and organizes event information sourced from news media, social media, official reports, and on-the-ground correspondents, and it presents this information using a visual interface that shows the connections between events, actors, locations, and genocidal processes. Threatwiki automatically generates maps and charts to assist our analysts in creating reports and suggesting preventive measures. The information contained in Threatwiki is published for free on our website, allowing access to the public as well as independent analysts and members of other organizations.

1.1 Supported Browsers and Known Compatibility Issues

Threatwiki is fully supported on up-to-date versions of Google Chrome, Mozilla Firefox, and Apple Safari. Users have noticed some errors when using Threatwiki in Internet Explorer, especially when running versions 8 or below.

Threatwiki is built according to common web standards, and our goal is for it to run on as many platforms and devices as possible. If you notice any errors with Threatwiki, feel free to post an issue notice on our github forum at https://github.com/thesentinelproject/threatwiki/issues. Use the Browser Compatibility tag to call out any bugs related to specific browser platforms or versions.

1.2 Threatwiki's Place in the Sentinel Project's Genocide Monitoring Efforts

The Sentinel Project for Genocide Prevention has developed an Early Warning System (EWS) for identifying and tracking the likelihood of genocide occurring in a Situation of Concern (SOC), a country or territory with an identified risk of genocide. SOC monitoring is conducted according to the four-stage framework shown below. The first two stages in this framework, Risk Assessment and Operational Process Monitoring, are focused on assessing the risk of genocide and monitoring genocidal processes in an SOC to inform preventive measures. The second two, Vunerability Assessment and Forecasting, are focused on projecting how genocide may occur and mitigating the risks faced by threatened

communities. Threatwiki supports the second stage in this process, Operational Process Monitoring.

OVERALL OPERATIONAL FRAMEWORK — DECEMBER 2010

STAGE	Risk Assessment	Operational Process Monitoring	Vulnerability Assessment	Forecasting
PHASE TYPE	Characteristics	Events	Characteristics	Analysis
FREQUENCY	Annual	Ongoing	Static / Annual	Annual / as needed
DATA	Risk factors	Indicators of: • Processes • Sub-processes • Intent	Factors such as: • Population distribution • Geography • Armed vs. unarmed • Fraternal groups • Wealth • Organization	Anticipation of future events, such as: • Threat courses-of-action (COA) • Timeline • Projected losses • Accelerators • Triggers • "Tactical" indicators of one COA or another
OUTPUT/IMPACT	• How likely is genocide? • How conducive to genocide is the environment?	• What is happening? • Who are the main actors?	• How resilient is the target group?	• How soon will genocide happen? • How severe will it be? • How will it unfold?
RESPONSE TYPES	Prevention		Mitigation	
	Structural	Operational	Building resilience	Response and evacuation planning

Contextual factors: leadership profiles, group profiles, perpetrator capabilities, international relations

Figure 1: EWS Framework

The first stage of this process is to create a formal Risk Assessment for the SOC. Analysts compile a risk assessment report detailing the likelihood that genocide will occur in the SOC in the near-to-medium term based on structural factors such as macroeconomic indicators, political trends, and historical instances of genocide or conflict. This report is published on our website and sent out to partner human rights organizations and Non-Governmental Organizations (NGOs). It is intended to both serve as a warning and also to inform structural prevention efforts.

After the Risk Assessment is completed, an Operational Process Monitoring effort is launched for the SOC. Operational Process Monitoring is a continuous process of tracking events in an SOC to identify event patterns and key actors involved. Events are classified according to the Operational Process model, which defines seven processes that underlie every historical instance of genocide. These processes, defined in detail in the section Tagging Datapoints Using the Operational Process Model, all contribute to planning or implementing genocide.

Threatwiki supports Operational Process Monitoring by allowing analysts to classify events as indicators of one of the seven operational processes. Threatwiki organizes and stores this information, using it to create visual displays through the

Threatwiki Toolbox. These visual displays show the patterns of events in an SOC, and they assist Sentinel Project analysts in creating regular threat reports. These threat reports support prevention efforts by providing a detailed picture of events on the ground.

1.3 Threatwiki Toolbox

Threatwiki contains a number of different tools that are used to manage and analyse the information contained in an SOC. Event information is managed through a data entry interface, available at http://threatwiki.thesentinelproject.org/admin/.

Each SOC has a visual display that shows its event data. This visual display is accessible through the homepage for the SOC and is available to both internal Sentinel Project analysts and members of the public. The screenshots below are taken from the Kenya SOC, available at http://thesentinelproject.org/situations-of-concern-2/kenya/. A full list of SOC homepages is available at http://thesentinelproject.org/situations-of-concern-2/.

The visual display shown on an SOC homepage is broken up into three tabs. Click on the tabs to see the information contained within.

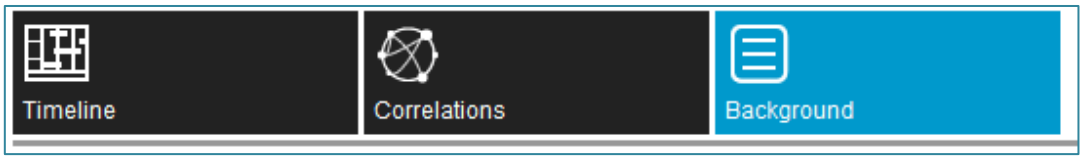


Figure 2: Threatwiki Tabs

1.3.1 Background Tab

The background tab provides background information for the SOC. It contains the initial risk assessment in PDF format to help contextualize the Operational Process Monitoring. The background tab is shown first in new SOCs where Operational Process Monitoring may not yet be initiated.

1.3.2 Timeline Tab

The timeline tab shows a list of events, or datapoints, and shows their position on a timeline and map. The timelines are organized according to the Operational Process model; datapoints are placed on one of the timelines based on the Operational Process tags they have been given by research analysts and the date they occurred. The short lines on the timeline represent a single datapoint, and

the long lines represent more than one datapoint. Datapoints for events that span multiple days are given a line for each day they encompass. You can use the arrows on the bottom-left of the timelines to change the date range.

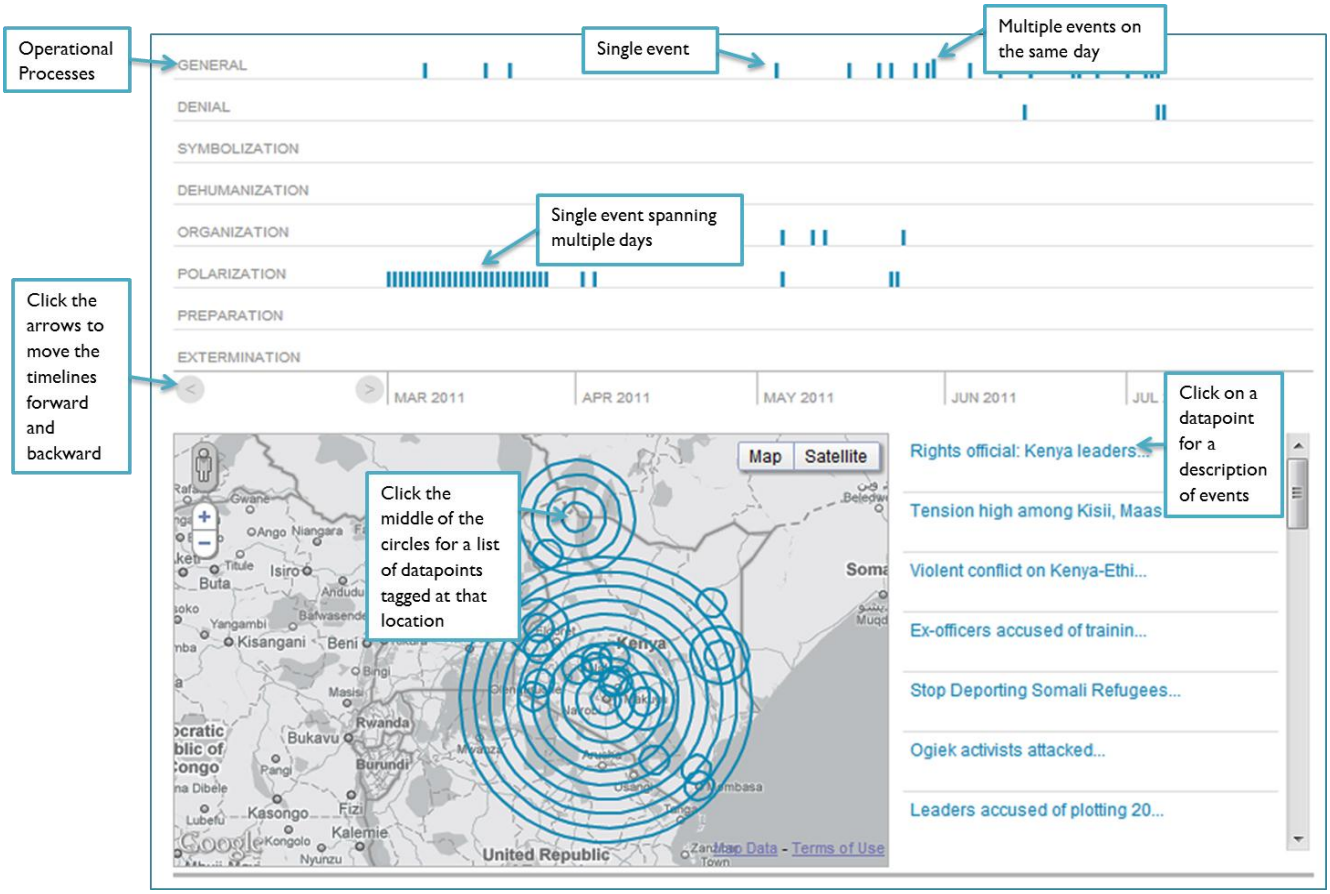


Figure 3: Timeline Tab

Datapoints are also shown in a list on the right. You can click on the title of a datapoint to see a description of its events, the source, and any tags that have been given to it. When you do this, Threatwiki highlights the datapoint's location on the map.

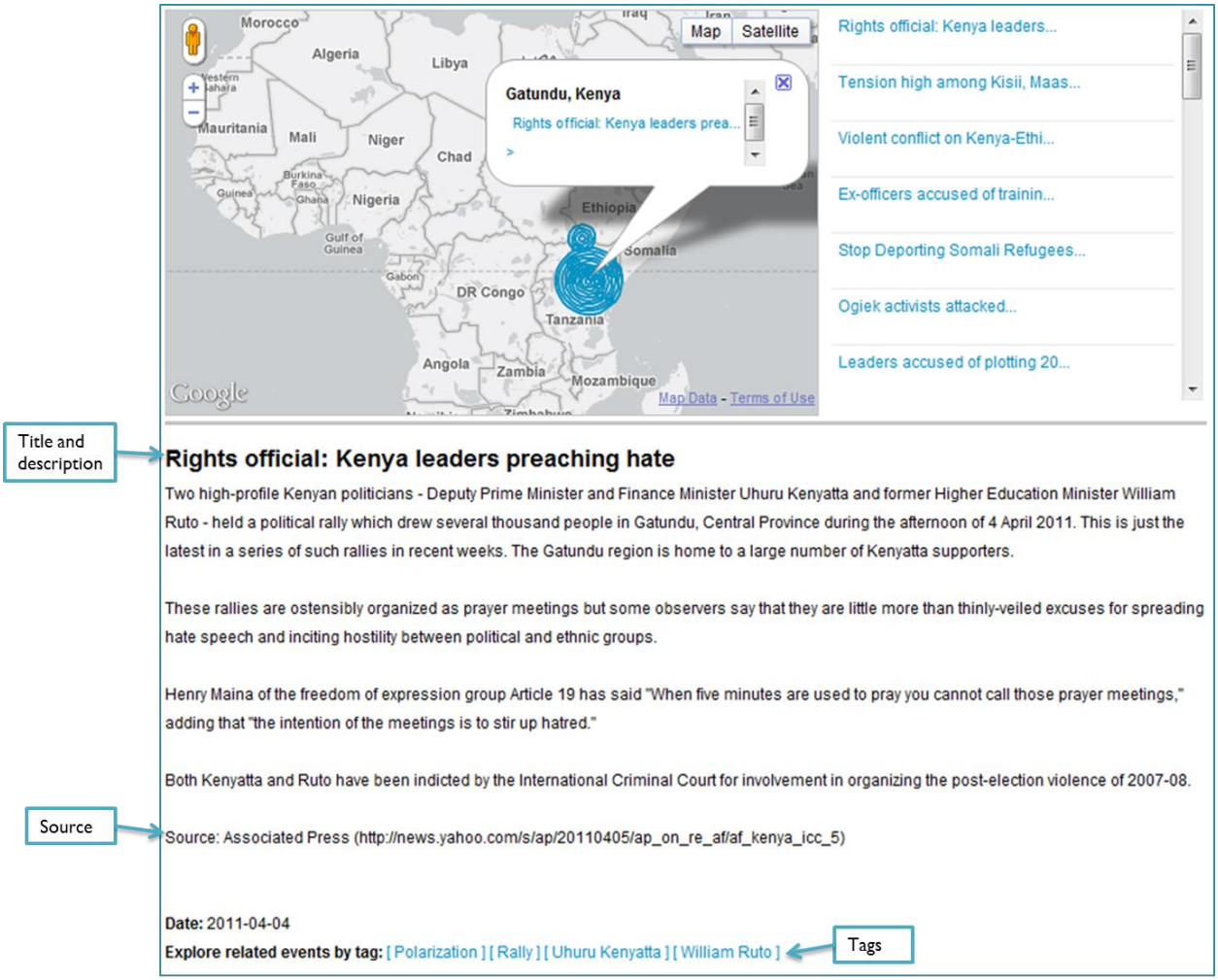


Figure 4: Timeline Tab with Datapoint Expanded

The timeline tab is shown first in ongoing monitoring efforts.

1.3.3 Correlations Tab

The correlations tab shows the relationships between different tags in Threatwiki. Tags are used for Operational Processes, key actors, groups, locations, and specific types of events. The correlations tab shows two things. First, it shows the number of datapoints that have received a particular tag. It represents each tag as a circle, which increases in size when a new datapoint has been added for that datapoint. You may click on the tag labels to bring up a timeline and list of all available datapoints for that tag.

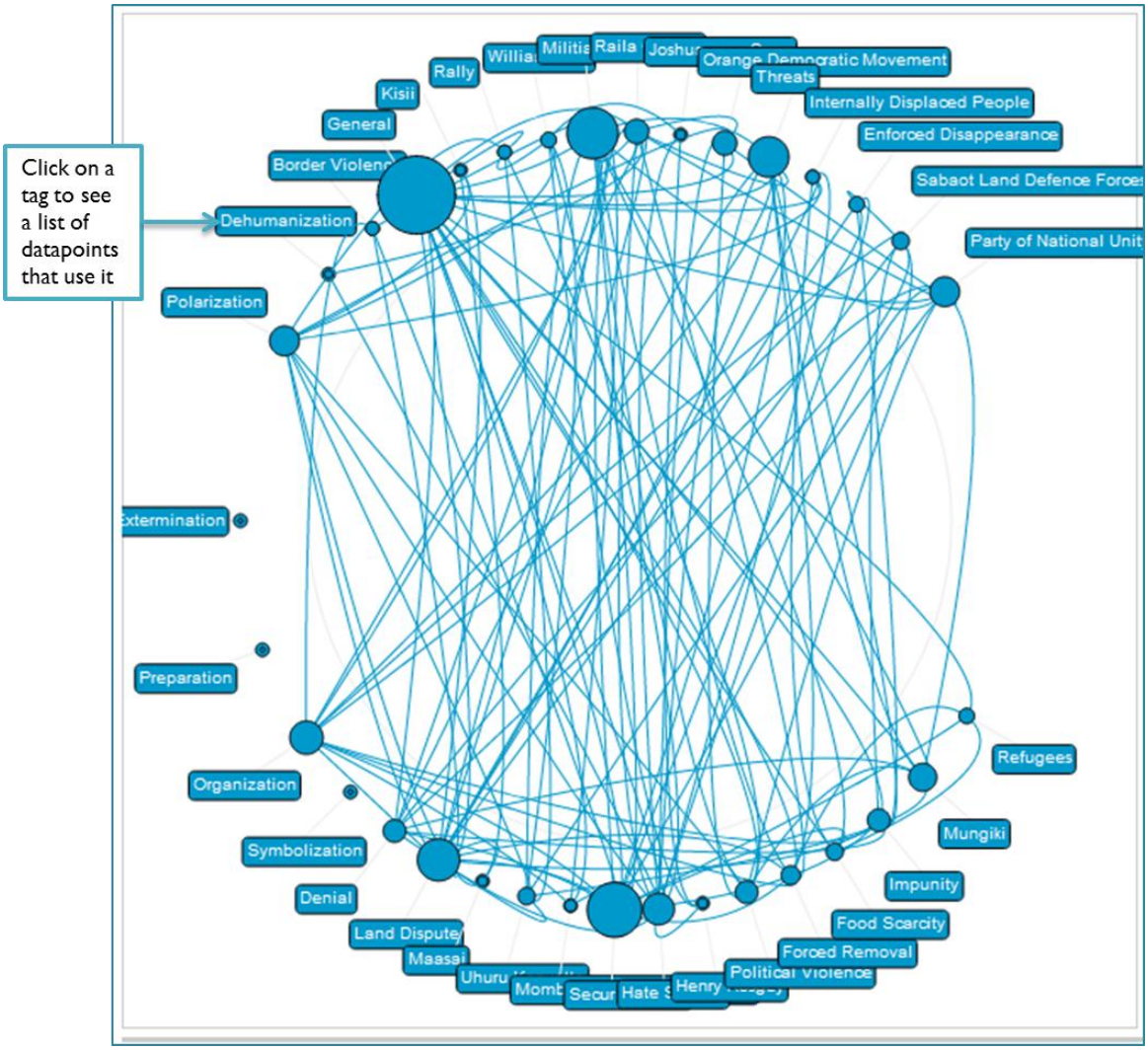


Figure 5: Correlations Tab

Second, the correlations tab shows the relationships between tags. When multiple tags are added to a datapoint, a line is drawn between the tags in the correlations tab. When tags are strongly correlated, multiple lines will be drawn between them.

1.3.4 Threatwiki Data Entry Interface

Threatwiki's data entry interface is an internal Sentinel Project tool used by analysts to manage the content for SOCs. It allows users to work with datapoints, locations, links, and data tags by adding new information or modifying the existing information. The following sections contain instructions on how to create and modify datapoints and other resources using the data entry interface.

2.0 SOURCING, TAGGING, AND WRITING DATAPOINTS

The effectiveness of the Threatwiki platform depends on its ability to show patterns of events in a clear and consistent manner. This will allow the research team to quickly analyse the data and confidently create reports that forecast the likely progression of events and suggest specific prevention or mitigation strategies.

In order to achieve this, standardized guidelines must be followed by our Operational Process Monitoring teams when locating, tagging, and creating datapoints. Threatwiki datapoints are published to the Sentinel Project website on the public Internet, so it is important that the content follows consistent standards for writing and formatting. This section covers the standards and guidelines that must be followed when creating datapoints in Threatwiki.

2.1 Sourcing Datapoints (Preferred Sources)

A datapoint may come from a variety of sources, but the main guideline is that a datapoint must refer to a specific event that has occurred within the geographical area of a Situation of Concern (SOC). If you are a volunteer who is not based in the field, you will most likely look for datapoints using free, online sources such as online newspapers, official government and Non-Governmental Organization (NGO) reports, blogs, and other social media tools. Consider the trustworthiness of the source and your information before posting; official sources such as media, NGOs, and government reports are more reliable than blog or social media posts. If you want, you may add comments that describe the trustworthiness of your datapoint.

If you are a field volunteer, you may create datapoints based on reports from correspondents or other local contacts in an SOC. Keep in mind, however, that information gained from personal reports may be confidential. You should always ask your source for permission before posting any information publically. Contact Chris Tuckwood, the Research Coordinator, at chris@thesentinelproject.org if your source requires special accommodations before providing information to the Sentinel Project.

2.1.1 Determining if Events are In-scope

Because the goal of Operational Process Monitoring is to analyse ongoing and recent events, datapoints must represent events that have occurred no earlier than three months before the SOC monitoring effort was initiated. Events that

have occurred earlier than that are not considered valid datapoints. Check the Timelines tab of the SOC page in Threatwiki to see the date when the SOC monitoring effort started.

2.1.2 Using Editorials and Opinion Blogs

You may use editorials or online opinion blogs for datapoints only if the article reports a significant event that has not already been entered as a datapoint. When using an editorial or opinion article, make sure the datapoint summary explains that the events have been drawn from an editorial.

2.1.3 Determining the Beginning and End of Events

For online articles and blogs, use the publication date for both the start and end dates, unless you know that the event happened on a different day or days. If the event occurs on a single day, repeat the start date as the end date. If the event occurs over a span of days, use the earliest available date that is confirmed by the source material, and use today's date for the end date if the event is still ongoing. It is possible to modify the start and end dates if new information is uncovered after the datapoint has been entered.

2.2 Tagging Datapoints Using the Operational Process Model

Your goal as a Threatwiki analyst is to tag datapoints according to the Sentinel Project's Operational Process model. This model has been adapted from Gregory Stanton's 8 Stages of Genocide,[1] but has been modified to suit the needs of a continuous threat monitoring effort. Because many of these definitions overlap, the Sentinel Project has developed standards based on the need for discrete, understandable definitions that can be replicated across multiple SOC monitoring efforts.

Most, though not all, datapoints will receive one of the Operational Process tags below. This indicates that these events are either the cause or effect of one of the fundamental processes of genocide. In general, datapoints should only be tagged as one Operational Process, as they will show up in the timelines for each Operational Process tagged. Use your best judgement to determine which Operational Process applies most to your datapoint. If you strongly feel that a

[1] Stanton, Gregory. *The 8 Stages of Genocide*. http://www.genocidewatch.org/aboutgenocide/8stagesofgenocide.html

datapoint should be tagged with multiple Operational Processes, discuss it with your SOC team or team lead before posting.

2.2.1 General

Datapoints are given the general tag if they describe events that are outside the scope of the Operational Process model but provide significant context to the events occurring in an SOC.

Examples of events that would be tagged as general include:

- Political events such as elections and the appointment or dismissal of government officials.
- Security events such as bombings, terrorist attacks, or military actions.
- Human rights violations that do not fall under any other Operational Process category.
- Natural disasters.
- Significant economic disruptions.

2.2.2 Classification

Classification has been eliminated as an operational process, and it is not used to tag datapoints in Threatwiki. Stanton defines classification as the use of language in a society to identify "'us and them' by ethnicity, race, religion, or nationality." Because this is a process that happens in all societies, it is not considered a significant indicator of potential genocide.

2.2.3 Symbolization

Symbolization is a process where symbols are used to identify others, often based on their physical characteristics. This ranges from the use of derogatory language to, on the extreme end, forcing individuals to wear physical markers to identify their race or group membership. Examples of this included the gold star used by the Nazis to mark people of Jewish origin and the blue scarves used by the Khmer Rouge to mark people from the Eastern Zone.[2]

Examples of events that would be tagged as Symbolization include:

[2] Stanton, Gregory. *The 8 Stages of Genocide*. http://www.genocidewatch.org/aboutgenocide/8stagesofgenocide.html

- Authorities in a country (such as media or government) use propaganda or symbols to represent a group or individuals from that group as an "other." They may be called weak, undesirable, or dishonourable; however, in order to maintain a contrast with Dehumanization, examples of Symbolization do not portray the group as an innate threat to society or as subhuman or nonhuman.
- Authorities are imposing physical marking to identify group members.

2.2.4 Dehumanization

Dehumanization is the Denial of the humanity of a group. Individuals from a group are identified as subhuman or nonhumans. They are often referred to as "animals, vermin, insects, or diseases."[3] The process of Dehumanization portrays group members as innately threatening to society, meaning that they are threatening solely because they are members of the group (not due to their political or social associations or activities). As a result of Dehumanization, crimes and attacks against members of the group are allowed to occur with impunity; they are ignored by authorities such as the police and courts.

Examples of events that would be tagged as Dehumanization include:

- Authoritative sources, such as government officials or media personalities, deny the humanity of group members. Group members are portrayed as nonhuman or subhuman.
- Representations of the group as an innate threat to society. Individuals are, by extension, considered threats based solely on group membership.
- Crimes and attacks against members of the group are ignored or encouraged. Courts refuse to prosecute, and police refuse to arrest the perpetrators.

2.2.5 Organization

Organization refers to the process, by the perpetrators, of planning and developing resources to commit genocide. This includes the creation of militias, informal paramilitary groups, concentration camps, and mechanisms intended for the purpose of Extermination. To distinguish Organization from Preparation, the focus is on resources controlled by the perpetrator, rather than actions meant to directly affect members of the target group.

Examples of events that would be tagged as Organization include:

[3] Stanton, Gregory. *The 8 Stages of Genocide*. http://www.genocidewatch.org/aboutgenocide/8stagesofgenocide.html

- The creation and arming of militias or informal paramilitary groups, especially when membership is restricted to a specific race or ethnicity.
- Creation of concentration or detention camps.
- Creation of machines that have no purpose except for extermination.

2.2.6 Polarization

Polarization refers to political or violent acts meant to create divisions in the society. Members of different groups are discouraged from normal social interactions, and members of certain ethnic or religious groups are denied the right to participate in society, often by denying them the right to attend school or join associations such as labour unions. Group members are blamed for terrorist attacks or terrorist attacks are committed to create divisions between sectarian groups. In some contexts, moderates are removed from political positions by force or procedural methods.

Examples of events that would be tagged as Polarization include:

- Members of the group are denied the rights to participate in society normally. They are denied rights to attend school, join professional organizations or labour unions, gather in public, or participate in politics. Members of different groups are prohibited or otherwise discouraged from interacting socially.
- Terrorist attacks occur that are blamed on a specific ethnic or religious group, or a group takes credit for terrorist attacks to create divisions between different groups.
- Mixed status categories are unrecognized.
- Peaceful political rallies are attacked to create divisions in politics, or political rallies are held to further divisions in society.
- Political moderates are removed from power through force or other non-electoral means. This is not always an indicator of Polarization, but can be depending on the political context in an SOC.

2.2.7 Preparation

Preparation refers to actions taken by the perpetrators to prepare a target group for Extermination. The goal of Preparation is to identify members of the target group and reduce the target group's ability to resist through disruptions such as arrest, detainment, forced migration, or exile.

Examples of events that would be tagged as Preparation include:

- Arbitrary (without legal reason) arrest or detention of members of the target group.
- Arbitrary seizure of property of members of the target group.
- Authorities attempting to disarm members of the target group.
- Authorities creating lists of group members or performing other activities to identify or map the demographics of target group.
- Authorities dividing communities or families through forced migration or exile.
- Members of target group are forced into concentration camps or ghettos.

2.2.8 Extermination

Extermination refers to the actions which are meant to eliminate a target group through mass killings or other methods, such as forced sterilization or rape.

Examples of events that would be tagged as Extermination include:

- Mass killings of members of the target group.
- Creation of mass graves.
- Forced sterilization of group members.
- Mass rape of group members. This is often done with the purpose of eliminating the "purity" of group members in future generations.

2.2.9 Denial

Denial refers to statements or actions taken by the perpetrators to deny or dismiss the occurrence of genocide. Government or military officials deny genocide based on legal or definitional grounds. They will claim that casualties are insufficient to be called genocide or point to casualties from their own group. They will blame civil wars and other conflicts for the killings and deny that they were deliberately planned. Perpetrators of genocide may also deny the existence of discrimination or unfair treatment. When looking for instances of Denial, it is important to remember the UN Genocide Convention defines genocide as "deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part."[4] Acts of genocide may be targeted at only one class or sub-set of the group.

Examples of events that would be tagged as Denial include:

[4] UN Resolution 260 (III). *Convention on the Prevention and Punishment of the Crime of Genocide.* http://www.hrweb.org/legal/genocide.html

- Authorities deny genocide on legal or definitional grounds. They claim that casualty counts are not high enough to count as genocide, point to casualties among their supporters, or dismiss the deaths as caused by civil war.
- Authorities deny the existence of activities or policies related to the other Operational Processes. They deny taking rights away from the target group.
- Genocide crimes are covered up. Mass graves are hidden, and records are destroyed.

2.2.10 Secondary Tags

Secondary tags are used to identify the involvement of specific individuals, groups, or issues in an event and to show genocidal sub-processes, which are specific types of events (such as arrests, forced migrations, or arson) that may indicate an Operational Process. Sub-processes are separate from operational processes in the sense that the Operational Processes themselves are indicators of genocidal intent that must be explained as such, but sub-processes are self-described events that do not need further explanation.

Secondary tags are created as needed and vary between SOCs. When creating a datapoint, make sure to tag it with any applicable secondary tags. You can view the available tags for all SOCs by clicking on **Tags** from the homepage of Threatwiki's data entry interface. You can filter tags based on SOC by clicking at the top of the SOC column in the tag list.

You can also create new secondary tags if you feel there is a key individual, group, issue, or pattern of events that should be tracked. Before you do so, make sure to check the list of tags to see if your tag has already been added. If you think that the tag is a sub-process and is associated with a specific Operational Process, you should discuss this with your team before adding it.

2.3 Writing Datapoints

When creating a new datapoint, you are also required to write a short summary of the event (around 1 or 2 paragraphs) that explains the important details of the event (the who, what, where, when, and why). This summary must be drawn from your own analysis, rather than copied from the original content. After the summary, you may include comments about why you think a particular event increases or decreases the risk of genocide or provides significant context to the SOC.

2.3.1 Creating Datapoint Titles

When creating a datapoint title, you may either use the original title of a media article or blog post or you may create an original title. When creating an original title, choose something that is concise and descriptive of the events. If the event is one of the sub-process indicators for the SOC (such as arrest or rape), begin the datapoint title with the name of the sub-process (see the following example).

	Example
Original Article Title	Another arrest in Semnan.[5]
Original Article Text	Nader Kasai, a Bahai resident of Semnan, was arrested late last week. Security agents searched his home and confiscated a computer and religious books…
Datapoint Title	Arrest of Nader Kasai in Semnan.

Figure 6: Datapoint Title Example

2.3.2 Writing Style

For instructions on writing style, including punctuation and formatting, please follow the guidelines in The Sentinel Project for Genocide Prevention Style Guide for Formal Publications, located on Dropbox at 2 – Research\Reference\SP Writing Style Guide-draft.

[5] Sen's Daily (reposted/translated from HRA News Agency). *Another Arrest in Semnan*. http://sensday.wordpress.com/2011/03/21/another-arrest-in-semnan-2/

3.0 WORKING WITH THREATWIKI

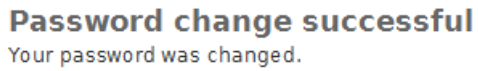
Threatwiki's data entry interface is used to add, delete or modify datapoints, locations, links, and data tags. Threatwiki's data entry interface can be reached by clicking on the following link: http://threatwiki.thesentinelproject.org/admin/ or typing it into your web browser. You then log on using the username and temporary password for Threatwiki. Your username and temporary password are emailed to you when your Threatwiki account is created.

Please change your original password after you log in. If you receive an error message when you log in, forget your password, or have any other trouble accessing Threatwiki, contact Hasan Rashid (hasan@thesentinelproject.org) for assistance.

3.1 Changing your Password

Threatwiki publishes content directly to the Sentinel Project website, so it is important that you keep your password secure. Please change your password the first time you sign into Threatwiki, and change it if you feel that your old password may have been compromised. To change your password:

1. From the top bar in any page in Threatwiki, select **Change password**.
2. Type your password into the **Old password** field.
3. Type your new password into the **New password** and **Password (again)** fields.
4. Click **Change my password**.



This message appears to confirm the change. If you forget your password, contact a Threatwiki administrator to have it reset.

3.2 Using Threatwiki's Data Entry Interface

After successfully logging on to Threatwiki, you are taken to the homepage for Threatwiki's data entry interface, shown below. There are two main sections to this page:

- **Ews:** This is the main menu you will use to work with datapoints, tags, links, and locations. These links provide access to lists of existing data objects and forms for inputting new objects.

- **Recent Actions:** Shows a list of your most recent actions with Threatwiki. The list will be empty the first time you log into Threatwiki, as it only records actions when a change has been made to a data object in Threatwiki.

Figure 7: Threatwiki Data Entry Interface

As a research analyst, you are primarily responsible for analysing recent events in a Situation of Concern (SOC), a given country or territory with an identified risk of genocide, and using the **Datapoints** link to add datapoints for events that fit one of the seven Operational Process categories. The Operational Process categories are common to all SOCs; see Tagging Datapoints Using the Operational Process Model for a definition of the Operational Processes and a breakdown on common categories where they are used.

Classifying events in this way allows Threatwiki to show how events relate to the fundamental processes of genocide and how patterns of events emerge over time. This helps our research team produce timely reports that describe the risk of genocide in a given situation and propose strategic preventive measures, based on the overall context of the SOC. Datapoints may also be added for general events, which means that they may have a significant impact on the political or social dynamics in a Situation of Concern but do not fit into an Operational Process category.

You are also responsible for tagging datapoints with secondary tags and adding locations, links, and new secondary tags into the system. Secondary tags are managed through the **Tags** link. They are specific to an SOC and allow Threatwiki highlight the relationships between different types of events and actors. Secondary tags used in current SOCs include tags for politicians, groups such as political parties or security agencies, and Operational Sub-processes, which are minor events such as arrests or instances of hate speech that will help increase our understanding of the pattern of events in an SOC.

Locations identify where events take place. They are managed through the **Locations** link and allow Threatwiki to show the locations of events on the map.

Links are simply hyperlinks to internet resources related to a particular datapoint. They allow visitors to our website to access the original article or explore additional media about the event. They are managed through the **Links** link.

3.3 Add Datapoint

Once you have located a news article, online media post, or eyewitness account that satisfies the requirements for a datapoint defined in the Tagging Datapoints Using the Operational Process Model section, the next step is to make sure that the datapoint has not been found or entered by another analyst. **Each SOC team keeps a datapoint table (an Excel spreadsheet) on Dropbox in the OP Monitoring folder for the SOC; it is your responsibility to make sure that your datapoint is not already on the list before entering it into Threatwiki.** The file naming convention for datapoint tables is:

- 2 – Research/SOCs/SOC Name/OP Monitoring/SOC Name Datapoint table.xls
- **Example (Kenya SOC):** 2 – Research/SOCs/Kenya/OP Monitoring/Kenya Datapoint table.xls

Remember to check both the OP Datapoints and General pages for your datapoint. If the datapoint is on the datapoint table, it has already been found by another analyst. If the datapoint is on the table and is bold, it has been entered into Threatwiki. You can use Find and Replace (Ctrl F or Cmd F) to quickly search the list for key terms.

If your datapoint is not in the datapoint table, you have two choices:

1. You may add a new datapoint to Threatwiki. This requires that you create a summary of its contents and select the tags and location for the datapoint. In this case, you create an entry for the datapoint in the datapoint table and bold it.
2. You may add an entry for the datapoint into the datapoint table, but not enter the datapoint into Threatwiki. You may decide to do this if you don't have time or if you are waiting for more information about an event. In this case, create an entry for the datapoint in the datapoint table, but do not bold it.

   To add a datapoint to Threatwiki:

1. From the Threatwiki homepage, click **Add** next to **Datapoints**. You may also click **Datapoints** and then click **Add Datapoint**.

   You are taken to the Add datapoint page. This page allows you to set up a new datapoint, add it to an existing SOC, and add data tags and a location for the datapoint.

2. In the **Title** field, enter the title of the datapoint according to the guidelines in the section.

3. In the **Description** field, write[6] a short summary of the event (around 1 or 2 paragraphs) that explains the important details of the event (the who, what, where, when, and why). You may include comments or analysis below the summary, but be sure to include two line breaks before the comments and begin the comments line with "Comments:". After your summary and comments, you must add two line breaks, then the source attribution line. This line is formatted as "Source: Name of Source (web address)". Before moving on, proofread the contents of the Description field to correct any formatting, punctuation, spelling, or grammatical errors.

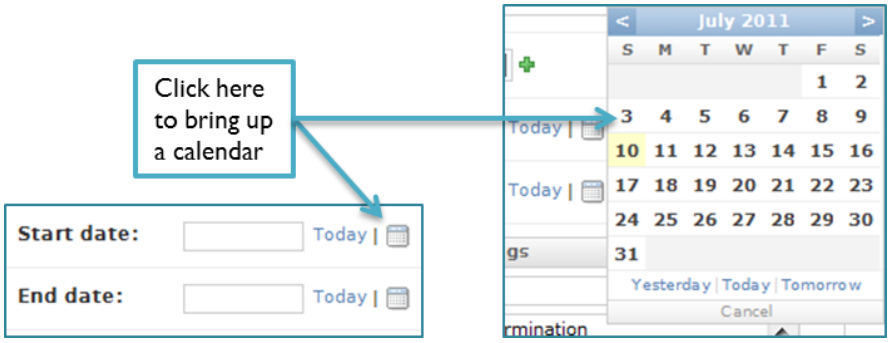
   Note: Threatwiki does not interpret the Enter or Return key as a line break. You must use the HTML tag
 to create line breaks.

4. If the event occurred in a specific location, use the **Location** drop-down to select the location. If the location does not appear in the list and you know the coordinates, you may add it by clicking the arrow next to the Location drop-down. Otherwise, leave the Location drop-down empty, complete the rest of this procedure, and save the datapoint. You can then add the location to Threatwiki using the Add Location procedure and modify the datapoint to include the location.

5. Use the **Soc** drop-down to select the SOC for this datapoint. If your SOC does not appear in this list, contact the Threatwiki administrator (hasan@thesentinelproject.org) for assistance.

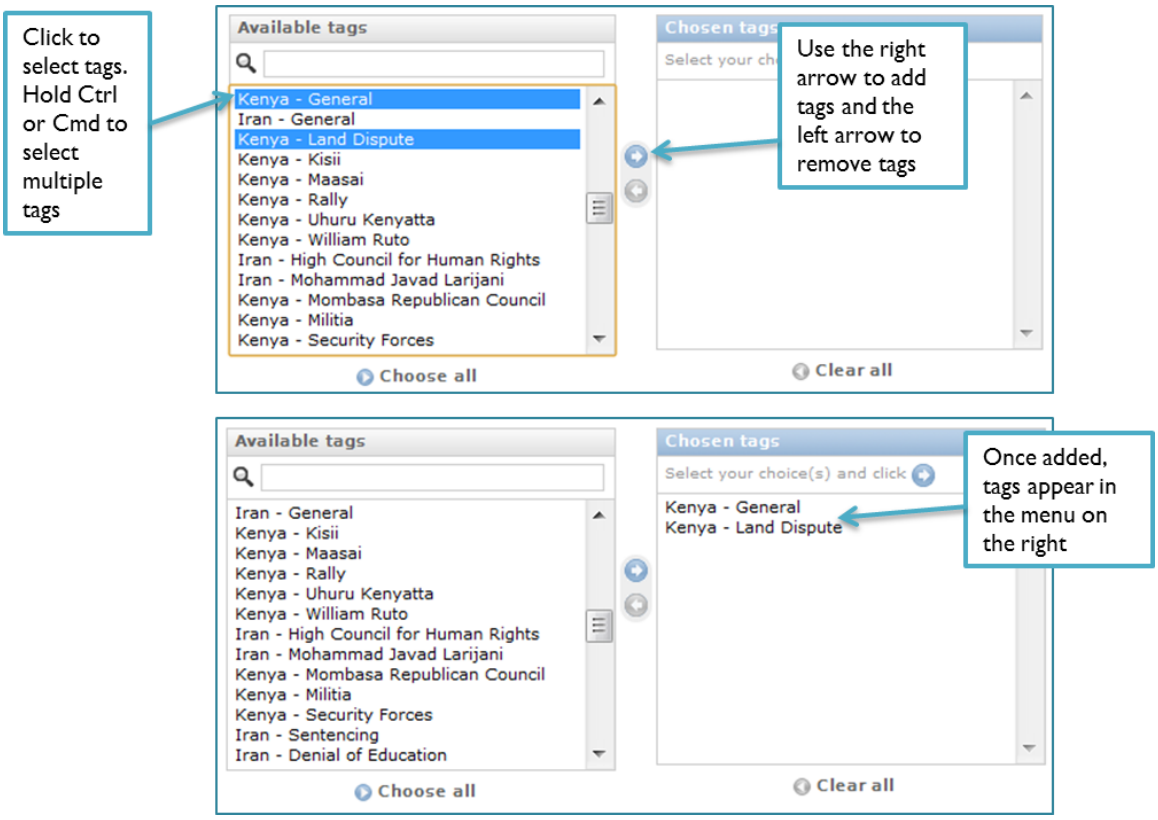
6. Enter the **Start date** and **End date** for the datapoint using the calendar buttons. For online articles and blogs, use the publication date for both the start and end dates unless you know that the event happened on a different day or days. If the event occurs on a single day, repeat the Start date as the End date. You can also quickly select today's date by clicking **Today**.

[6] For guidance on writing style, see the Sentinel Project Style Guide for Formal Publications, available on Dropbox at: 2 – Research\Reference\SP Writing Style Guide-draft.docx.



Note: You must enter an end date or Threatwiki defaults to today's date.

7. Use the **Available Tags** menu to add any applicable data tags to the datapoint. Make sure to add only tags specific to this SOC, as the Available Tags menu shows the tags for all SOCs. See the Tagging Datapoints Using the Operational Process Model section for guidance on how to tag datapoints with Operational Process and secondary tags. Add tags by clicking on them in the **Available Tags** menu to highlight them. Then, click the right arrow next to the box to add them to the datapoint. You may search through available tags using the search bar at the top, and you can select multiple tags at once by holding Ctrl (or Cmd on Mac). To remove tags from the datapoint, highlight them in the **Chosen tags** menu and click the left arrow.



8. Review the contents of your datapoint to ensure that everything is correct, and click **Save**. You may also use the **Save and add another** to create another datapoint or the **Save and continue editing** button to save any current changes and continue making changes to the datapoint.

   This publishes your datapoint on Threatwiki, adjusting the Timelines and Correlations tabs accordingly. You can verify that your datapoint has been successfully saved by visiting the SOC page on the Sentinel Project website.

3.4 Modify Datapoint

You can change the contents and tags for a datapoint if it has been entered incorrectly or if details known about it change.

1. From the Threatwiki homepage, select **Datapoints**.

   The Select a Datapoint page appears, with a list of datapoints. You may click at the top of the Soc column to sort datapoints by their SOC, or click the top of the other columns to sort by the Title, Start Date, or End Date.

2. Click the title of the datapoint you would like to modify from the list.

3. Modify the **Title**, **Description**, **Location**, **Soc**, **Start Date**, and **End Date** as needed.
4. Use the **Tags** section to change the tags for the datapoint. Tags already added to the datapoint are located under the Chosen tags menu. Tags that have not been added are located under the Available tags menu. To move tags between these menus, click on their name to select them (select multiple tags by holding Ctrl or Cmd on Mac) and click the left or right arrows.
5. Click **Save** to save your changes.

3.5 Delete Datapoint

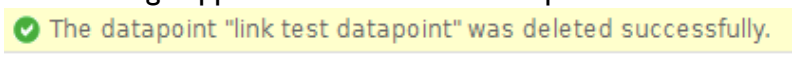
Check with your SOC team before deleting any datapoints that you have not added.

1. From the Threatwiki homepage, select **Datapoints**.

   The Select a Datapoint page appears, with a list of datapoints. You may click at the top of the Soc column to sort datapoints by their SOC, or click the top of the other columns to sort by the Title, Start Date, or End Date.

2. Click the title of the datapoint you would like to delete.
3. Click **Delete** in the bottom-left corner of the Change datapoint page.
4. Click **Yes, I'm sure** to confirm.

   This message appears to confirm the datapoint has been deleted.

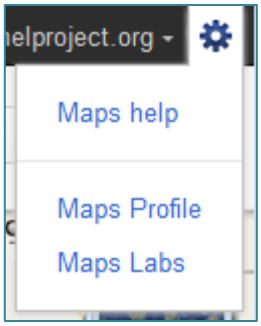


3.6 Add Location

When an event occurs in a location that has not been entered into Threatwiki, you must add it. Locations are added according to their coordinates, which are obtained using Google Maps. The following example is using the location Khartoum, Sudan.

First, locate the coordinates:

1. Go to maps.google.com.
2. Click the gear icon in the top-right corner, and select **Maps Labs**.

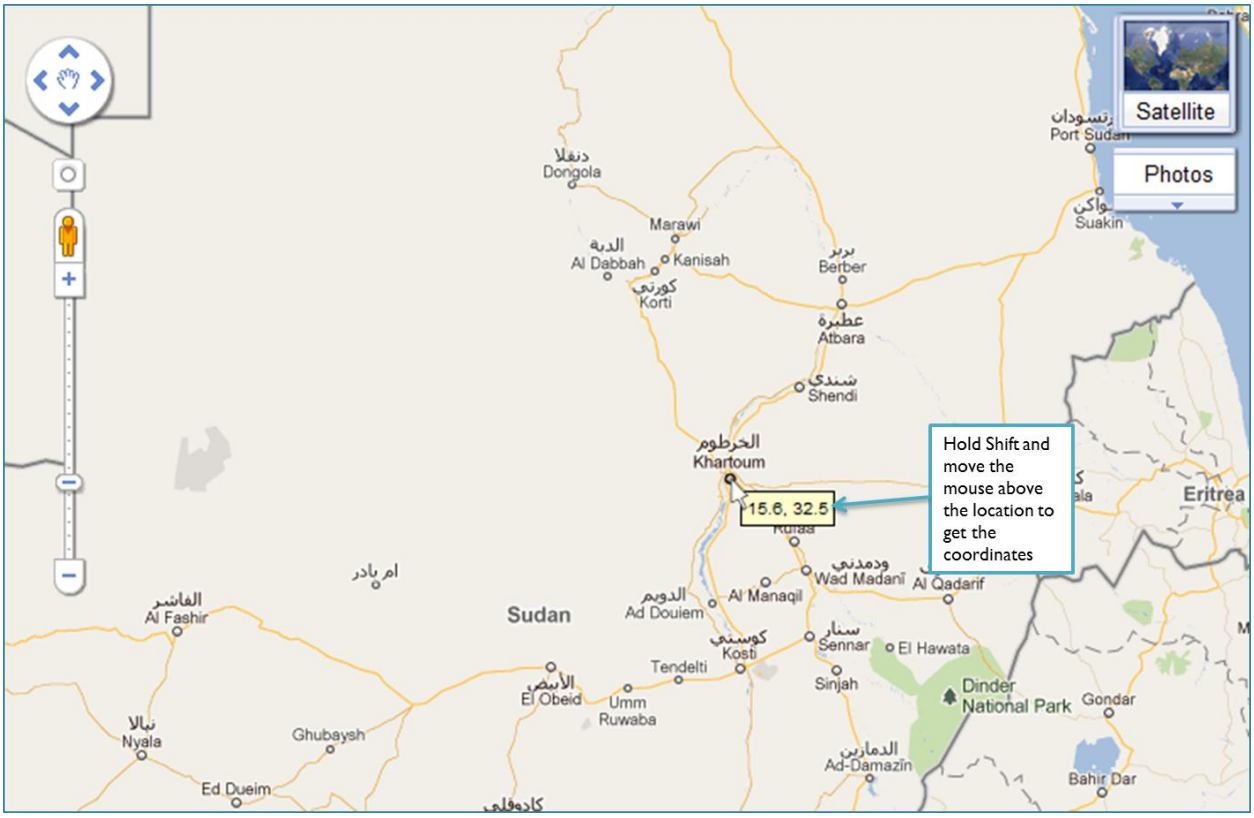


3. Find the **LatLng Tooltip** and check **Enable** to turn it on.

4. Click **Save changes**.

   Now that the LatLng tooltip has been enabled, you may locate the coordinates of any location on the map by holding the Shift key and moving the mouse over it.

5. Find the location on the map, move your mouse over it, and hold Shift to show the coordinates. Write down the exact coordinates shown.



Then, add the location to Threatwiki:

1. From the Threatwiki homepage, click **Add** next to **Locations**.
2. In the **Title** field, type the name of the location as "City Name, Country." Our example location would be written as Khartoum, Sudan.
3. In the **Coordinates** field, type the coordinates obtained from Google Maps exactly as they appear. Make sure to separate the numbers by a comma and space. The coordinates for Khartoum would be entered as 15.6, 32.5.
4. Click **Save** to add the location to Threatwiki.

   This message appears to confirm the location has been added.

   The location "Khartoum, Sudan" was added successfully.

   The location now shows up in the list of locations that appears when you click Locations from the Threatwiki homepage or when you add a location to a datapoint.

3.7 Modify Location

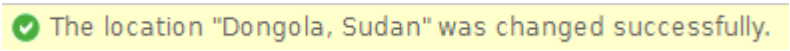
If the name or coordinates of a location have been added incorrectly, you may change them. Doing this automatically updates any datapoints that use this location.

1. From the Threatwiki homepage, click **Locations**.

   The Select location to change page appears, with a list of locations.

2. Click the name of the location you would like to change from the list.
3. Modify the location's **Title** and **Coordinates**, as needed. Remember that coordinate values must be separated by a comma and space (for example: 15.6, 32.5).
4. Click **Save**.

   This message appears to confirm your changes.

3.8 Delete Location

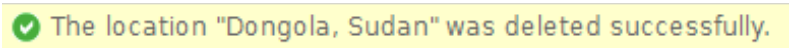
Deleting a location also deletes any datapoints that use it. **You should only delete a location if it has been entered incorrectly and does not have any datapoints associated with it.** Otherwise, use the previous procedure to change the name or coordinates for the location.

1. From the Threatwiki homepage, click **Locations**.

   The Select location to change page appears, with a list of locations.

2. Click the name of the location you would like to delete from the list.
3. Click **Delete**.
4. Click **Yes, I'm sure** to confirm. The confirmation screen shows if any datapoints are associated with the location. **Do not delete the location if any datapoints are shown.**

   This message appears to confirm.

3.9 Add Secondary Tag

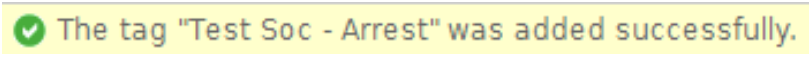
Secondary tags[7] are added to an SOC to enable analysts to connect datapoints to genocidal sub-processes and key actors, groups, and other issues specific to that SOC.

1. From the Threatwiki homepage, click **Add** next to **Tags**.
2. In the **Title** field, enter the title of the secondary tag.
3. Use the **Soc** drop-down to select the SOC this secondary tag is for.

   Note: The Alwaysoccurswith section does not work. It is a non-functional demonstration of a feature may be implemented in a future version of Threatwiki.

4. Click **Save** to add your tag to the SOC.

   This message appears to confirm.

3.10 Modify Secondary Tag

If necessary, you can change the names or SOC settings of tags. Doing this updates all datapoints that use the tag.

1. From the Threatwiki homepage, click **Tags**.

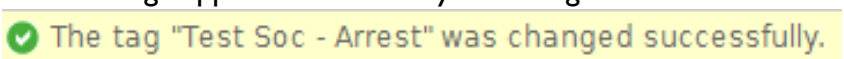
   The Select a tag to change page appears, with a list of tags.

2. Click the name of the tag you would like to change from the list. Keep in mind that tags are specific to each SOC, and make sure that you select the tag from the correct SOC.
3. Modify the tag's **Title** and **Soc**, as necessary.

   Note: The Alwaysoccurswith section does not work. It is a non-functional demonstration of a feature may be implemented in a future version of Threatwiki.

4. Click **Save**.

   This message appears to confirm your changes.

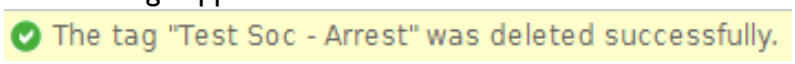
[7] See Secondary Tags for more information on how to use secondary tags, including instructions on when to add new secondary tags.

3.11 Delete Secondary Tag

Deleting a tag removes that tag from any datapoints that use it. If you want to change the name of the tag or the always occurs with settings, use the previous procedure instead.

1. From the Threatwiki homepage, click **Tags**.
2. The Select a tag to change page appears, with a list of tags.
3. Click the name of the tag you would like to delete from the list. Keep in mind that tags are specific to each SOC, and make sure that you select the tag from the correct SOC.
4. Click **Delete**.
5. Click **Yes, I'm sure**.

   This message appears to confirm deletion.

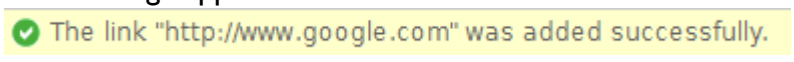
   

3.12 Add Link

Links are added to datapoints to direct the reader to the source or other resources related to the datapoint.

1. From the Threatwiki homepage, click **Add** next to **Links**.
2. In the **Url** field, type the link address. Be sure to include the http:// prefix, as Threatwiki assumes that addresses without it are for pages at thesentinelproject.org.
3. Use the **Datapoint** drop-down to select the datapoint you would like this link to appear under.
4. Click **Save**.

   This message appears to confirm.

   The link appears at the bottom of the datapoint on the SOC page on the Sentinel Project website.

3.13 Modify Link

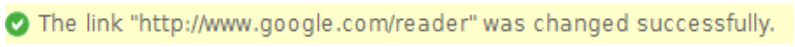
You can change the addresses for links or the datapoints they appear with. Changing the address for a link automatically updates the datapoint it appears under.

1. From the Threatwiki homepage, click **Links**.

   The Select a link to change page appears, with a list of links.

2. Click the name of the link you would like to change from the list.
3. Change the address using the **Url** field, if necessary.
4. Use the **Datapoint** drop-down to change the datapoint the link appears with, if necessary.
5. Click **Save**.

   This message appears to confirm.



3.14 Delete Link

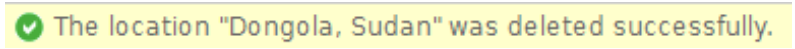
Deleting a link removes it from the datapoint it was added to.

1. From the Threatwiki homepage, click **Links**.

   The Select a link to change page appears, with a list of links.

2. Click the name of the link you would like to delete from the list.
3. Click **Delete**.
4. Click **Yes, I'm sure**.

   This message appears to confirm.



4.0 APPENDIX A: SENTINEL PROJECT DOCUMENTATION REFERENCE

File paths are for our Dropbox folder.

SOC Files (Datapoint tables, etc.):

2 – Research\SOCs

Sentinel Project Glossary:

2 – Research\Reference\SP Glossary-draft.doc

Sentinel Project Style Guide for Formal Publications:

2 – Research\Reference\SP Writing Style Guide-draft.docx

"The 8 Stages of Genocide" by Gregory Stanton:

http://www.genocidewatch.org/aboutgenocide/8stagesofgenocide.html

UN Convention on the Prevention and Punishment of the Crime of Genocide:

http://www.hrweb.org/legal/genocide.html

Threatwiki Github page (including code and issue trackers):

https://github.com/thesentinelproject/threatwiki/

Source File for this Document:

3 – Technology/Threatwiki/User Guide/User Guide-draft.docx

5.0 APPENDIX B: CONTACT LIST

If you…	Contact	Name
Lose your Threatwiki password	hasan@thesentinelproject.org	Hasan Rashid
Need special accommodations for a correspondent	chris@thesentinelproject.org	Chris Tuckwood
Have any comments or suggestions for this document	daniel@thesentinelproject.org	Daniel Friedman
Have any general inquiries or would like to volunteer for the Sentinel Project	contact@thesentinelproject.org	N/A

6.0 INDEX

THE SENTINEL PROJECT FOR GENOCIDE PREVENTION IS A NON-PROFIT ORGANIZATION DEVOTED TO EFFECTIVE EARLY WARNING OF GENOCIDE AND THE IMPLEMENTATION OF PREVENTIVE MEASURES BEFORE LIVES ARE LOST.

OUR GOAL IS TO ACHIEVE THIS THROUGH THE CREATIVE USE OF TECHNOLOGY AND COOPERATION OF THREATENED GROUPS.