Style-Based Attacks against a Topic Agnostic Fake-News Detection System

Jacob Möller Rachel Homssi
Email: {jacmo965, racho401}@student.liu.se
Supervisor: Alireza Mohammadinodooshan, {alireza.mohammadinodooshan@liu.se}
Project Report for Information Security Course
Linköpings universitet, Sweden

Abstract

Today online users are creating and sharing information on the worldwide web more than ever before. Spreading misinformation has become a common way of manipulating popular opinions and influencing political decisions. These malicious intentions have been brought up to light and automated systems have been developed to predict fake news. In this work, we will target attack a recently proposed fake-news detection system and explore what types of textual changes result in an article being labeled as real-news and types of changes not detected by the system. These changes were done both manually and automatically. The classification algorithm K-Nearest Neighbors (KNN) has been used to classify the modified articles of the news dataset. The results show that it is possible to bypass a fake-news detection system by modifying the style of the fake-news article, without modifying its meaning.

1. Introduction

Social media has grown rapidly and has become a place for people read and share news stories with each other. The rapid increase of online social media users has led to a rapid increase of fake-news being spread [1]. Cambridge Dictionary defines fake-news as “false stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke” [2]. Fake-news includes information that is misleading and or untrue which can have serious consequences. Many approaches have been introduced to identify and prevent fake news from being spread, style-based methods being one of them. It is a method that aims to classify an article purely based on its textual features. [3], describes designing a style-based fake-news detection system as a game of cat and mouse. Any successful detections will inspire fake-news writers to find counter measurements. Another challenge that comes with designing fake news detection systems is that news topics vary from year to year. A detection system that works well one year might become ineffective in the future [4]. A top agnostic approach for identifying fake news articles has been recently proposed by Castelo et al. [4]. But how well does this detection system perform against even small changes to the fake-news content? Could small changes in how the fake-news is written result in it being classified as true-news?

1.1 Purpose and Scope

The focus of this study is to design and test attacks against an existing fake-news detection system. The system that will be tested was presented in *A Topic-Agnostic Approach for Identifying Fake News Pages* [4]. The goal of the aforementioned work was to present and test the concept of a style-based topic-agnostic classification strategy for identifying fake-news.

The classifier discussed in the article is designed around analyzing morphological, psychological, readability, and web-markup features. This study will however only focus on attacking the morphological and readability features because of time limitations. Another motivation for this focus is that web-markup features often are poor targets of attacks. If an author has written an article on a certain page, changing the name of that author or the name of the page would remove the credit from the author or the page.

The following question will be the focus of this study:

- Can a relatively basic attack be designed in such a way that it bypasses a style-based fake-news detection system without making changes that alter the content’s original meaning?

2. Background

This section contains information about different kinds of textual features, the dataset that the attacks will be performed on and the libraries that are used to create the attacks.

2.1 Target of attack

PoliticalNews[1] is a dataset that was created by Castelo et al. in conjunction with their article [4]. This dataset was designed to cover a wide timespan as to be able to judge the topic-agnosticism of their method. The dataset, therefore, contains articles on mixed political topics from 2013 to 2018.

2.2 Features

Text features can be defined as building blocks for a texts' structure. The text features aim to help the reader make sense of what they are reading. Listed below are the features this project will concentrate on.

2.2.1 Topic agnostic features

Topic agnostic features are characteristics of an article that are independent from the topic the article is about. Such features are useful to study when training a fake-news detection algorithm to function on texts concerning differing topics or from different years [4].

2.2.2 Style-based features

Style based features focus on the writing style of the article. These types of features do not take into context the facts the text is about, but rather how the text is written. This exploits the fact that fake-news tends to have a distinctive, often sensationalist, style [4]. The style-based features used by *A Topic-Agnostic Approach for Identifying Fake News Pages* are web-markup, psychological, morphological and readability features.

2.2.3 Morphological features

Morphology is the study of the internal and external structure of words. The internal structure refers to features such as prefixes, suffixes, and other morphemes. A morpheme in the linguistical context is the minimal unit of a word that has meaning and cannot be split into meaningful parts. The external structure refers to how the word functions with other words. Words are split into two groups. Lexical words are words such as verbs, adjectives, nouns, and adverbs, while grammatical words are prepositions, articles, and pronouns [5].

2.2.4 Readability features

Readability is concerned with how easy the text is to read and understand for the reader. Some of the basic readability features include number of words per sentence, how long words are, how many syllables the words contain, as well as capitalization. There are also more advanced systems of scoring readability, but these are all based on combining basic readability features in different ways to produce a single score or grade [6].

2.3 Employed Packages

To extract features of text and allow for generation of new sentences this project uses several Python packages. The most notable are listed here.

2.3.1 Natural Language Toolkit (NLTK)

NLTK is a toolkit that contains functions for building Python programs to work with human language data. It provides interfaces to several corpora and lexical resources, for example useful when extracting synonyms. It also provides text classification, tokenization and tagging [7].

2.3.2 Sentence Transformers

Sentence transformer is a Python library that contains pre-trained natural language processing models. The models are based off BERT, Bidirectional Encoder Representations from Transformers. BERT is a language model that has been trained on large datasets to understand language. The training of BERT consisted of two steps, pretraining and fine-tuning. In the pre-training phase BERT learned to understand language and context. In the second phase, fine-tuning, BERT was trained to solve specific natural language processing tasks. The model has been shown to be very effective for solving many different tasks, for example, paraphrasing, which analyzes and predicts the relationship between sentences [8]. The Sentence transformer library can use BERT to score text based on how similar they are using cosine similarity [9].

2.4 Classification

In order to determine whether news is fake or real, a classification of the news must be done. In the following subsection, the classification algorithm is described.

2.4.1 K-Nearest Neighbors (KNN)

KNN is an algorithm that is used for classification. The algorithm starts off by loading train and test data. A value of “K” is determined, which will be the “K” number of nearest neighbors the test datapoint will be compared to. When the datapoint is placed, the KNN will predict its’ classification by looking through similarities of the “K” number of neighbors with the shortest distance of the training set. Lastly the class will be set based on the class of its “K” nearest neighbors in the training set [10].

3. Solution and Analysis

This section will describe the attacks, the methodology of constructing them and their results. Further on, an analysis will be made on the results and methodology.

[1] https://osf.io/ez5q4/

3.1 Attack design

The design principle behind the attacks was to perform only minor changes to the original fake-news text as possible. The overall meaning of the text was not to be changed. Therefore, attacks had to be designed in such a way that a readable text with the same underlying message was produced in the end.

In Table 1 the attacks performed are listed. The table is split into attacks that were performed automatically and attacks that were performed manually. White-box attacks are marked with a star (*).

ID	*Description*
A1	Duplicating random letters in random words in each sentence.
A2*	Duplicating random letters in the most common fake-news words in each sentence.
A3	Substituting random adjectives with their best matching synonym.
A4*	Substituting the most common fake-news adjectives for their best matching synonym.
A5	Replacing contractions with their expansions.
M1*	Adding words to sentences that are more common in real news.
M2	Changing from active voice to passive.

Table 1: Attacks – [A/M] Automatic and Manual. Attacks marked with "*" are white-box attacks.

Attacks **A1**-**A4** were designed to make it harder for the detection system to identify fake-news by recognizing words commonly used by such articles. **A1** and **A3** functioned as baseline tests for **A2** and **A4** to be able to compare the difference between a white-box and a black-box attack.

For **A3** and **A4** words were swapped for synonyms, which might seem trivial at first. But at a second glance some problems become obvious. For example, when targeting nouns, the problem is that some nouns cannot be replaced without vastly changing the meaning of the text. Most notably names. Verbs on the other hand have the problem of tense. A synonym generated must have the same tense or the sentence will not sound right. Therefore, adjectives were selected to be the best target for the attacks.

The style of fake-news is often more emotional than true-news. This to connect to the reader on a more personal level and to make them want to propagate the news because of an emotional connection. The style of fake-news is therefore often more informal than true-news [11]. Some of the characteristics of informal writing are that it [12]:

- Uses shorter words and sentences.
- Uses personal pronouns and active voice.
- Uses contractions (won't) and abbreviations (TV).
- Uses words that express familiarity (buddy).

Making fake-news articles more formal was the purpose behind attacks **A5**, **M1** & **M2**. Attacks **A5** and **M1** also served to make the articles longer. This is based on the fact that Horne and Adalı discovered that true-news articles often are longer than their fake-news counterparts [13].

3.2 Extracting word frequencies

To determine which words were used more frequently in real-news compared to fake-news all the articles were looped through and the words extracted with the help of the NLTK library for Python. Short words (less than 4 characters) were excluded to avoid stopwords such as "a", "and", "the" etc. This was done for the real-news words and fake-news words separately. Additionally, all words which appeared less than 100 times in real- and fake-news combined were also excluded, to avoid fewer common words.

The frequency of the words in real-news were then divided by the frequency of the same words in fake-news to ascertain the ratio there between. A ratio of 1 means that the word appears equally in both, whilst 0.5 implies the word is 2 times more common in fake-news. The five words with the lowest and highest ratios respectively are shown in Table 2.

As seen in the table, most words are either names or highly specific to some topic. Therefore, they are not so useful for our attacks since they cannot with ease be inserted into or swapped in most sentences. Going through the list manually led to the discovery of some more interesting words, some examples of these are presented in Table 3.

Word	**Ratio**
Corruptly	0.0039
Maxine	0.0064
Strap	0.0071
Schooled	0.0072
F.B.I	0.0074

Word	**Ratio**
Strata	406.0
Delhi	256.0
Surrey	211.0
Generics	208.0
Edmonton	200.0

Table 2: Ratio of word frequencies in real-news compared to fake-news. A higher ratio translates to a word being more common in true news.

Word	**Ratio**
Illegals	0.013
Impeach	0.019
Implying	0.052
Furious	0.137
Shocking	0.374

Word	**Ratio**
Redistributed	53.0
Placement	19.1
Challenging	2.82
Suggestion	2.19
Introduce	2.07

Table 3: Ratio of word frequencies in real-news compared to fake-news for some interesting words.

The most common adjectives were picked in much the same way. But using NLTKs collection of synonyms, only those adjectives that had at least one synonym that was also an adjective, were selected.

Word	Ratio	Word	Ratio
Fairer	0.016	Defensive	8.16
Overzealous	0.023	Tougher	7.77
Unsubstantiated	0.028	Consecutive	7.50
Indefensible	0.061	Nonprofit	6.74
Directive	0.085	Junior	6.33

Table 4: Ratio of adjective frequencies in real-news compared to fake-news.

3.3 Performing automatic attacks

The dataset PoliticalNews was split into training and testing data. To speed up the attacks it was advantageous to make the testing set small, so that only a small number of articles needed to be changed in the attacks. Therefore, the testing set was selected to be 10% of the total dataset or i.e., 713 fake-news articles. These articles were selected by picking the first 10% of the articles from all the different years in the original dataset.

Attack **A1** looped over all sentences in the articles and then in each sentence, depending on its length 0-2 words were selected to have one letter randomly duplicated. For **A2** the same was done, but instead of selecting words at random all words with a real to fake ratio bellow or equal to 0.5 (2 times more common in fake-news) were selected. NLTK was used to split the text into sentences and then into words.

For attacks **A3** and **A4** NLTK:s part-of-speech tagger was used to determine which words in the sentences were adjectives. Then NLTK was used once again to extract the synonyms for those adjectives. For the purpose of finding the best synonym to use instead the Python library Sentence Transformers was employed. For each synonym found by NLTK, a new sentence was generated and then Sentence Transformers picked the one it considered to be the most similar to the original sentence based on their cosine similarity. In attack **A3** all adjectives were swapped for synonyms whilst in **A4** only the ones with a true to fake ratio below or equal to 0.65 were selected. A slightly higher number to include more words since adjectives are only a small portion of the total amount of words.

3.4 Performing manual attacks

The manual attacks were performed on a subset of nine selected fake-news articles from PoliticalNews. These were picked from three different years, three from each year.

Attack **M1** was performed by adding a random word to each sentence of the texts. The random word that was inserted was chosen so that it was around 4 times more common to occur in real-news (the extracted word frequencies described in 3.2 was used for this). The words were also chosen so that they fit the context of the sentence.

The same methodology was used for attack **M2**, but instead of adding a random word, the sentences that were written in active voice form were rewritten into passive voice.

3.5 Classification

To classify the articles, all the readability and morphological features of the text were extracted. This was done with the code written for *A Topic-Agnostic Approach for Identifying Fake News Pages.*

To establish the effectiveness of the attacks, the articles were then run through a KNN classifier, also provided by the mentioned above article, before and after they were attacked. The classifier looked at the features of the texts and then classified them based on that.

For the automatic attacks, the classifier labeled the articles as either true- or fake-news. The accuracy of the classifier is defined as the number of articles the classifier judged correctly. This means that the accuracy is based both on it judging fake-news and true-news. In each case the number of fake-news and true-news articles classified were the same. The true-news articles used for testing were always the same.

For the manual attacks, due to the low number of articles attacked, it was not sufficient to look at the accuracy to determine if the attack had caused a change or not. Instead, the confidence of the fake-news classification was used to determine the success of the attacks. This made it possible to see the confidence change for each individual article. With this it could be determined if an attack made an article move towards a different classification or solidify the old classification.

3.6 Attack results

This section presents the results of the attacks. See the appendix for some examples of successful attacks. The results for the automatic attacks and the manual attacks have been split into two tables, see Table 5 and Table 6 respectively. Green indicates that the attack has decreased the accuracy, i.e., the attack was successful, while red indicates that the attack as increased the accuracy. That the accuracy has changed means that the classification of one or more articles have flipped value.

ID	*Accuracy*
Before attack	0.71058
A1	0.70707
A2*	0.6517
A3	0.71198
A4*	0.71338
A5	0.71128

Table 5: Accuracy of classification on original text and after automatic attacks.

For the manual attack results in table Table 6 each column in the right-hand side corresponds to the confidence the classifier had when classifying an article.

ID	*Confidence of fake-news*									*Dif.*
Before	0.7	0.55	0.55	0.35	0.25	0.35	0.75	0.85	0.5	-
M1*	0.65	0.7	0.45	0.4	0.65	0.65	0.4	0.9	0.35	0.18
M2	0.5	0.45	0.55	0.25	0.2	0.65	0.45	0.9	0.55	0.13

Table 6: The confidence of classification after manual attacks. Confidence bellow or equal to 0.5 is considered true-news. Dif. is the average absolute difference from the baseline.

4. Discussion

Here the designing of the attacks and the result of the attacks are discussed as well as sources of error.

4.1 Evaluation of attack results

From table 5, it can be seen that all attacks changed the classification accuracy. Attack **A2** was the most successful attack out of the five and resulted in the largest positive accuracy margin. Attack **A4** was the least successful attack with the largest accuracy gain.

The two successful attacks **A1** and **A2**, included adding random letters to words and creating misspelling to make the fake-news detection system unable to recognize them. In some cases, the substitution of the random letter even changed the words meaning. Some of these changes can be overlooked by a reader, whilst others cannot. This might lead to the articles being easily identifiable as fake for a human due to the spelling errors, even though they evidentially were successful in tricking the automatic classifier.

Attacks **A3-A5** all increased the accuracy of the classifier. I.e., the attacks were unsuccessful. A possible explanation for this is that these attacks included far less changes in the texts compared to **A1** and **A2**. This might have resulted in too few changes to flip the articles from false to true. It was also observed that Sentence Transformers was not always able to produce grammatically correct results. In one of the tests performed for **A5**, the sentence *"Where's he put them and where's she?"*, was expanded to "*Where is he put them and where is she?"*. These grammatical errors could have affected the results of **A3-A5** more negatively than the word changes and expansions affected the results positively. In other words, the articles where sentences were expanded correctly included too few changes to be considered true whilst the articles with grammatically incorrect sentences were now easier to identify as fake.

This would be one possible explanation for why **A5** worsened the score even though, as mentioned in 3.1, lengthening the sentences should have increased the score according to Horne and Adalı [13].

In Table 6 it can be seen that the manual attacks affected the confidence of the classification. Attack **M2** seemed to have one more article where the accuracy value implied real news compared to attack **M1**. The overall number of fake and real articles did not differ much from both attacks, but the accuracy values for some articles were greater in attack **M2** which implies a more successful attack. The differential for M1 is however higher suggesting that it, on average had a larger effect on the results, just not always in the right way.

4.2 Attack design

The main challenge of designing the automatic attacks was for the new sentence to be readable. A lot of attacks were discarded as they could not reliably be performed. For example, changing all words related to fake-news to words more common in real-news was discarded as it was too difficult to consistently generate correct synonyms for verbs and nouns. Therefore, only adjectives were considered.

However, in a real-world scenario a large-scale fake-news attack, requiring automatic changes, would probably be unlikely. Rather articles would most likely be changed on an article-to-article basis. This would mean that manual attacks likely would be more applicable than automatic.

The limitations for designing the manual attacks mainly consisted of being able to perform the attacks in a consistent manner. I.e., the attacks needed clear rules so that they were easy to document and to perform consistently between the articles. This would most likely not be considered by someone writing fake-news and thus more possibilities for attacks would be available for them.

A writer of fake-news could easily adapt their writing style to be more in line with real-news if they knew what the detection systems targeted. However, changing fake-news to look like real-news might, even though the original meaning is intact, cause them to no longer achieve their goal. As stated in 3.1 fake-news pray on peoples' emotions, changing some words to their synonyms or changing from active to passive voice, might cause this emotional connection to be lost, making the fake-news less appealing to readers.

4.3 Sources of error

In cooperation with the project's supervisor, we concluded that the code belonging to [4] that we were to use, produced different values from the ones used in the article. The code, when we and our supervisor ran it, identified far too few sentences, and could not classify difficult words correctly. After going through the code, we determined that they did no preprocessing which would result in the code assessing the features differently. This led us to rewrite some of the functions. Even after the faulty functions were replaced the new code did not produce the same values. However, the values were much closer to those of the article than before.

5. Future research

For future research, we propose that attacks should be combined. This would create more changes to the text, which will be able to affect the classification more.

Based on Horne and Adalıs research, further increasing the length of the sentences and the articles as a whole could be successful. Also, the incorperation of more technical words, more quotes and more puctuation could likely make an impact [13]. The problem, however, is that the main difficulty of designing the attacks was to automatically generate natural language. There is no clear cut why how to incorporate these things in a good way. This would likely be a field of research where machine learning could prove effective.

Further on, more complex attacks can be constructed based off the information we extracted from the articles. The frequency word list of common words in real and fake news can be used to design more attacks.

6. Related work

Fake News Detection via NLP is Vulnerable to Adversarial Attacks [3], the authors argue that that fact-based knowledge should be adopted alongside style-based methods. Pure style-based methods face a lot of vulnerabilities; for example, it is biased towards under-written articles and certain topics that can be associated with more be more fake-news. Real-news may not be written in a journalistic style and then face the potential of being misclassified. Through experiments with Fakebox, a state-of-the-art fake news detector, they draw the conclusion that only looking at linguistic aspects is not enough for fake news detection. They argue that fact checking should be used as a helpful supplement.

7. Conclusions

From this project, we can draw the following conclusions.

- It is possible to design attacks that make fake-news articles bypass a style-based detection system with modifications that do not alter the meaning of the articles.
- The most effective method tested was duplicating letters in the words most frequently common in fake-news.
- Simple rules for automatic changes to text will most likely result in some grammatical or contextual errors. Therefore, changes that fool an automatic detection system without changing the original meaning, might still be noticeable for a human reader.

References

[1] "Guides Library," [Online]. Available: https://guides.lib.umich.edu/fakenews. [Accessed 15 05 2021].

[2] Cambridge University Press, "Cambridge Dictionary," [Online]. Available: https://dictionary.cambridge.org/dictionary/english/fake-news. [Accessed 15 04 2021].

[3] Z. Zhou, H. Guan, M. M. Bhat and J. Hsu, "Fake News Detection via NLP is Vulnerable to Adversarial Attacks," in *11th International Conference on Agents and Artificial Intelligence (ICAART 2019)*, 2019.

[4] S. Castelo, T. Almeida, A. Elghafari, A. Santos, K. Pham, E. Nakamura and J. Freire, "A Topic-Agnostic Approach for Identifying Fake News Pages," in *Companion Proceedings of The 2019 World Wide Web Conference*, 2019.

[5] J. Wagner, "IeLanguages," [Online]. Available: https://ielanguages.com/morphology.html. [Accessed 16 04 2021].

[6] "Readable," [Online]. Available: https://readable.com/. [Accessed 16 04 2021].

[7] NLTK Project, "Natural Language Toolkit," [Online]. Available: https://www.nltk.org/. [Accessed 16 04 2021].

[8] M.-W. C. K. L. K. T. Jacob Devlin, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," 2019.

[9] N. Reimers, "Sentence Transformers: Multilingual Sentence, Paragraph, and Image Embeddings using BERT & Co.," [Online]. Available: https://pypi.org/project/sentence-transformers/. [Accessed 16 05 2021].

[10] "tutorialspoint," [Online]. Available: https://www.tutorialspoint.com/machine_learning_with_python/machine_learning_with_python_knn_algorithm_finding_nearest_neighbors.htm.

[11] C. Guo, J. Cao, X. Zhang, K. Shu and M. Yu, "Exploiting Emotions for Fake News Detection on Social Media," 2019.

[12] F. Abu Sheikha and D. Inkpen, "Generation of Formal and Informal Sentences," *Proceedings of the 13th European Workshop on Natural Language Generation,* pp. 187-193, 2011.

[13] B. D. Horne and S. Adalı, "This Just In: Fake News Packs a Lot in Title, Uses Simpler,Repetitive Content in Text Body, More Similar to Satire than Real News," in *The Workshops of the Eleventh International AAAI Conference on Web and Social Media,* 2017.

[14] X. a. R. Z. Zhou, "A survey of fake news: Fundamental theories, detection methods, and opportunities.," Association for Computing Machinery, New York, Syracuse University, 2020.

Appendix

The appendix consists of some examples of attacks that worked. Changes are marked with **bold**.

A1 – Before attack

"George Carlin proves that comedy is by far the best way to relay important information to human beings, even if that information might seem 'negative' in other lights. In this case Carlin analyzes the excruciating language used in food advertising to manipulate people into buying disgusting products.

Finding the absurdity and humor in our behavior makes the madness bearable and he was a total genius in this regard.

In recent years he has become an icon on the internet, along with people likes Bill Hicks and Carl Sagan, who just have a way of delivering data to the masses in a beautiful and entertaining way that no one can resist.

You could have someone running through Times Square with Earth shattering news, but if they are forcing it down people's throats in the typical annoying activist fashion, they are screwed and no one will listen. There are deep rooted psychological reasons for the necessity of intelligent information exchange. Enjoy…

"Fresh, hearty, natural, homemade goodness, in a can.."

"Everything is natural. Dog shit is natural. It's just not real good food…"

via Minds"

A1 – After Attack

"George Carlin proves that comedy is by far the best way to relay important information to human beings, even if that **informationn** might seem 'negative' in other lights. In this case Carlin analyzes the excruciating language used in food advertising to **manipuulate peoplle** into buying disgusting products.

Finding the absurdity and humor in our behavior makes the madness bearable and he was a total genius in this regard.

In recent years he has become an icon on **thee** internet, along with people likes Bill Hicks and Carl Sagan, who just have a way of delivering data to the masses in a beautiful and entertaining way that no one can resist.

You could have someone running through Times Square with Earth shattering news, but if they are forcing it down people's throats in the typical annoying **aactivist** fashion, they are screwed and **nno** one will listen. There are deep rooted psychological reasons for the necessity of intelligent information exchange. Enjoy…

"Fresh, hearty, natural, homemade goodness, in a can.."

"Everything is natural. Dog shit is natural. It's just not real good food…"

vvia Minds"

A4 – Before Attack (all paragraphs without changes were removed, original article around 3000 words)

Instead, energies have been focused towards creating a honey pot in Syria for a generation of Islamic fanatics and fighters arriving from around the globe. To achieve this, a cult was created which appears to offer its militant entrants a new version of radical Islam.

As a general rule, cults are anything but transparent. This is part of the attraction – to blend your individuality into a larger pool – to become part of something larger, and more powerful. All faces covered, hiding behind a black 'al Qaeda' flag – only it's hard to know who is behind this black mask – a farmer, a Syrian defector, a jihadists, a Libyan, a Saudi, an Afghan, a

Blackwater mercenary, a Mossad operative, or an ex-SAS soldier? Ad radical female fighters into this mix and it makes it all the more potent.

Violence, death squads, bombings – romantic to some, but in reality, they are fueled by glorious posts on Twitter, Facebook – and cash. It seems each and every faction involved is willing to make a 'deal with devil' in order to realise their own objective. A dangerous game to play.

The issue of Palestine has been frozen. Israel has suffered a defeat in Syria and wants to win its positions back. If Hamas returns from Qatar and joins forces with the Resistance Front, this would make other scenarios possible. He who has the weapons sets the tune in Palestine. There is no peaceful solution here.

NH: The entire Lebanese electorate – including the Sunni, Shia, Christians – is politically divided between the March 8 and March 14 coalitions. About 55 percent vote for March 8 and 40 percent for March 14.

There are two stages of the Syrian conflict. The first one started as the people rose against the ruling regime. At that time, Hezbollah acted as a balancing power that convinced the government [in Syria] to give peaceful protesters a pass.

Instead of liberating Palestine, you can send women to Syria. It is the most dangerous way of brainwashing Muslims.

RT: How will US-Russian agreements on chemical weapons affect the region?

NH: The agreement between the US and Russia is much wider and deals not only with chemical weapons. They discussed plenty of aspects: Iran's nuclear program, Bahrain, Syria, Yemen, the Caucasus. The draft is prepared. The issue of chemical weapons in Syria is a way to enter another issue – chemical weapons of Israel. They even addressed such details as the "Death to America" slogan in Iran.

The hysteria around chemical weapons of August 21 was rooted in two things: first, there was an ambush laid for guerillas, and second, the army carried out a successful offensive.

A4 – After Attack

Instead, energies have been focused towards creating a honey pot in Syria for a generation of Islamic fanatics and fighters arriving from around the globe. To achieve this, a cult was created which appears to offer its militant entrants a new version of **extremist** Islam.

As a general rule, cults are anything but transparent. This is part of the attraction – to blend your individuality into a larger pool – to become part of something larger, and more powerful. All faces covered, hiding behind a black 'al Qaeda' flag – only it's hard to know who is behind this black mask – a farmer, a Syrian defector, a jihadists, a Libyan, a Saudi, an Afghan, a Blackwater mercenary, a Mossad operative, or an ex-SAS soldier? Ad **revolutionary** female fighters into this mix and it makes it all the more potent.

Violence, death squads, bombings – romantic to some, but in reality, they are fueled by glorious posts on Twitter, Facebook – and cash. It seems each and every faction involved is willing to make a 'deal with devil' in order to realise their own objective. A **unsafe** game to play.

The issue of Palestine has been frozen. Israel has suffered a defeat in Syria and wants to win its positions back. If Hamas returns from Qatar and joins forces with the Resistance Front, this would make other scenarios possible. He who has the weapons sets the tune in Palestine. There is no **peaceable** solution here.

NH: The **full** Lebanese electorate – including the Sunni, Shia, Christians – is politically divided between the March 8 and March 14 coalitions. About 55 percent vote for March 8 and 40 percent for March 14.

There are two stages of the Syrian conflict. The first one started as the people rose against the ruling regime. At that time, Hezbollah acted as a balancing power that convinced the government [in Syria] to give **peaceable** protesters a pass.

Instead of liberating Palestine, you can send women to Syria. It is the most **life-threatening** way of brainwashing Muslims.

RT: How will US-Russian agreements on **chemic** weapons affect the region?

NH: The agreement between the US and Russia is much wider and deals not only with chemical weapons. They discussed plenty of aspects: Iran's nuclear program, Bahrain, Syria, Yemen, the Caucasus. The draft is **fain**. The issue of **chemic** weapons in Syria is a way to enter another issue – chemical weapons of Israel. They even addressed such details as the "Death to America" slogan in Iran.

The hysteria around **chemic** weapons of August 21 was rooted in two things: first, there was an ambush laid for guerillas, and second, the army carried out a successful offensive.