STUDIA UBB. EUROPAEA, LXII, 2, 2017, 17-29

MILITARY TROLLS, PUBLIC DISTRACTIONS AND THE CYBER

Mihai-Lucian Bârsan*

DOI:10.24193/subbeuropaea.2017.2.02
Published Online: 2017-06-30
Published Print: 2017-06-30

Abstract

Threat actors have started a disinformation process across the internet targeting the larger population, which mainly are intended to rise the mistrust of the population in the governing institutions and governmental actors. Dismantling these operations have proven to be a big challenge similar to cyberattacks which affect technological infrastructures. Even though some countries have taken a set of legal measures against disinformation and trolling many aspects have been left out and militarized trolling and the process of spreading false news is a phenomenon which can become more and more powerful.

Keywords: militpary trolls, cyber, cybersecurity, threats

1. Be a troll in 4 easy steps

"As my contact information was disclosed alongside the disinformation about me, my phone's messaging and email inboxes were filled with messages from people angry at me for 'persecuting Russians'. I received a phone call in which someone fired a gun. Later someone texted me, claiming to be my dead father, and told me he was 'observing me'"[1]

* Mihai-Lucian Bârsan is assistant researcher at The Institute of Political Sciences and International Relations "Ion I. C. Brătianu", Romanian Academy. Contact: bmihailucian@gmail.com

[1] Jessikka Aro, "The cyberspace war: propaganda and trolling as warfare tools", *European View*, June 2016, Volume 15, Issue 1, p 123

A series of unconventional wars have started to impact the world in the last 20 years. With a rising number of terrorist attacks, cyberwarfare, the controversial rise of extremism in the world are just some of the factors that have changed the landscape of understanding security and resisting threats.

Taking into consideration these elements and viewing them at a macro scale, the impact they have on individuals or groups is extremely hard to assess in a simple statistical analysis due to the high number of silenced victims. The story above belongs to a young researcher that has become victim of online trolling because she wanted to analyze the impact of this phenomenon and the inception of tainted information (or fake news) in Finland. In the last year the intensifying rise of trolling has had the primary objectives to distract the public order by exaggerating the intensity or importance of a situation, manufacturing stories or events, aggressive comments that affected normal users and in connection with cyberattacks/ hacking tainting information coming from leaked files or e-mails.

The paper intents to highlight that the methodological analysis done in the past has treated wrongly the types of threats mentioned above and will focus on the case of weaponized trolling and how this threat has been counteracted. Put in a very strong perspective, Patrick Michael Duggan pointed out: *As senior leaders have recently recognized, groups of special operators armed with asymmetric cyber tools, irregular warfare tactics, and mass disinformation can have strategic effects*[2]. Thus, I will treat the subject of online trolling and the spread of fake information as a mainstream direct threat rather than an unconventional practice.

Challenging as it may be the development of online trolling has had a long historical backtrack in communist countries. Peter N. Tanchak traces it back to the "agents of influence" in Soviet Russia that played a key point in spreading false information aimed to promote pro-communist opinions and supporting the regime[3]. The importance of this historical dating of

[2] Patrick Michael Duggan, *Strategic Development of Special Warfare in Cyberspace*, Essay Competitions / Special Warfare in Cyberspace JFQ 79, 4th Quarter 2015 p.47.

[3] Editor Olga Bertelsen, *Revolution and War in Contemporary Ukraine: The Challenge of Change, The Invisible Front: Russia, Trolls, and the Information War against Ukraine, Peter N. Tanchak,* online book [https://books.google.ro/books?hl=en&lr=&id=xCLADgAAQBAJ&oi=fnd&pg=PT232&dq=online+trolling+and+disinformation&ots=HOU6bCrFl9&sig=XU-cXZeOjmyx9364bnD65Zm-2ko&redir_esc=y#v=onepage&q=online%20trolling%20and%20disinformation&f=false], 1 July 2017

trolling implies a long standing tradition which evolved due to the rise of technological advancements and a highly decentralized network of blogs, websites and social media platforms.

For a clarification and as a statement no one wishes to institute an online police, where everyone would be closely watched. These are not constructive solutions that would be of much help, but rather impediments in development. Fighting disinformation and identifying trolls is not a new problem, but the real issue in this case is that it has never happened at this complex scale.

The rapid distribution of fake news over the internet can be done from any location and with any type of computer. Communities of online trolls are consisted of either paid people who write articles, comment and bots that automate a part of this process. Constructing the path through which these actors work is quite easy[4], due to the immediate services that one has on the internet, putting it more in simple terms, one would just sit in front of his or her computer and:

1. Buy a domain;
2. Buy hosting services;
3. Create a basic website;
4. Start writing with the community:

4.1. Articles;

4.2. Comments;

4.3. Distribute;

4.4. Discredit any comment which is unfavorable to what has been written;

[4] For further references regarding this problem, anyone can look up the simple steps taken for buying a domain or search for hosting companies. Everything is at hand and anyone can rapidly implement a simple website.

1.1. Given the problems and what to really expect

First of all, due to the rapid movement produced by these groups, an article is immediately taken over by other websites, afterwards (in some contexts) extremist groups start sharing the false news, which is rapidly picked up by mainstream media and spread to readers that become the victims of the attack. No one would expect that every person in the world start using online tools or have the sharp eye of a photographer to realize that an image was manipulated or start quickly checking that story on every possible platform.

Secondly, these communities create and generate almost alternative universes which nothing can be trusted, everything is put under a series of "attack" questions and leaves everything to wondering, never giving a clarification or solution. Readers are left with unverified facts about reality and what is happening in the world. Also, an argument that prevails among these trolls and goes beyond each border is *truth for each person* which implies a multiculturalist argument used out of context and undermines the argument of a normal user who expresses an opinion. On another side of the process, discouraging the act of expressing an opinion is attacked by trolls who start commenting about the user and use aggressive language destined to offend and not really attack the stated argument.

From Jessica Aro's analysis, the systematic troll operation in Finland has discouraged many Finns to start chats on various forums, but were not psychologically or emotionally affected by what was stated by the trolls due to their high rate of education and continuous documentation of real facts[5]. Countries that have a less independent mass media and a lower education level are more vulnerable to what trolls distribute and write. In the case of Romania and other Eastern countries which have been classified in 2017 as free[6], people are still having doubts about what is being reported by the national news agencies which leaves these countries more vulnerable to trolling operations. According to the Digital News Report from 2017 the

[5] Jessikka Aro, *op.cit.*, p. 123

[6] Freedom House, *Populists and Autocrats: The Dual Threat to Global Democracy*, [https://freedomhouse.org/report/freedom-world/freedom-world-2017], 4 July 2017.

overall trust in news is only 39%[7] which leaves the society open to fake news reports, due to their attitude of *let's start telling the truth*.

The strategy of the threat actors implies targeting the main problems of the given country and start commenting or writing fake articles that underneath feed the vulnerabilities of the society of the country, leading individuals to question their political authorities, question institutional decisions and believe in alternative facts which are just purely manufactured statements based on events or decisions never really taken into consideration.

1.2. Assessing the troll threat in security terms and dilemmas

In this contexts identifying trolls over the internet is proven to be very problematic because the term has been on the internet for a long time and was usually given to people who leave nasty comments on Reddit, 4chan and smaller forums[8]. This "new" type which can be termed as military trolls are nothing to be confused with the previous ones, due to their obvious intentions. Thus, the military trolls will try to distribute fake news through commenting on mainstream news posts and upvote through sharing and commenting the fakes ones and their purpose is to disinform the society and alter opinions.

Discovering this behavior becomes more complex when realizing how do troll factories[9] work when targeting the events that occurred. The deployment of trolls happens at a rapid rate of response timed by the mainstream media. They have the opinion and they act convincingly like they know what is really going on. Take for example the investigation made by Radu Cupcea on the troll Ioan Sbucium who specializes only on

[7] News Avoidance 2017 [http://www.digitalnewsreport.org/survey/2017/news-avoidance-2017/], 4 July 2017.

[8] Consider the definitions of trolls on the online campaigning website http://anti-troll.org/

[9] Term used across the media for groups of people that have been hired in questionable agencies in Russia that contribute mainly to the development of propaganda messages masked in articles, post, blogs etc. A journalist investigation was conducted and is related in the article written Leo Benedictus *Invasion of the troll armies: from Russian Trump supporters to Turkish state stooges*, [https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian].

commenting news that is published on *Adevarul* news website and promotes an anti-American view with powerful nationalist views.[10]

At an international scale and in developed countries, trolls are more and more aggressive. The case reported by CitizenLab from Toronto in May 2017[11] is of most importance, trolls combined cyberattack resources and carefully implanted false information within stolen e-mails from the American journalist David Satter who criticized the Russian policies and abuses. Carefully false information was planted within the leaked e-mails that would lead a reader to believe that Satter and other Russian activists were receiving money from foreign international actors for the purpose of destabilizing Putin's image.

Both journalists Satter and Aro have been subjected to these type of attack and the disinformation campaign started against them feed the trolls' purpose in order to raise the distrust of the public in the mainstream media and governmental authorities. The analysis of these situations have unraveled the truth about them, through comparison between original e-mails and tainted ones, in the case of Satter and the attacks on Aro's reputation was covered with a false history of drug abuse, threats and insults which were proved not to be true.

The typical troll will try to confirm propaganda assumptions, using simple styled logic linking events with conspiracies, modifying photos, using shocking titles and damasking processes of the "corrupted political establishment". The leading scandals are linked to trolls influencing electoral campaigns like in the case of the US investigations of what happened during the US election last year[12]. Cybersecurity, in many Western countries were not prepared for this kind of type of attack due to the mass specialization of other kind of attacks.

[10] Radu Cupcea, *Trolli moldoveni si razboiul lor absurd impotriva Romaniei,* [http://larics.ro/trolii-moldoveni-si-razboiul-lor-absurd-impotriva-romaniei/], 20 June 2017.

[11] Adam Hulcoop, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert, *Tainted Leaks: Disinformation and Phishing with a Russian Nexus,* [https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/], 29 June 2017.

[12] Reuters.com, *U.S. government loses to Russia's disinformation campaign: advisers* http://www.reuters.com/article/us-usa-russia-disinformation-analysis-idUSKBN1492PA, Reporter Joseph Menn, 4 July 2017.

What do all aspects show in this case for any kind of analyst that tries to tackle any of these facts? The response should be given in accordance with what was stated in the beginning, we can no longer speak of a type of situation in which the impacts of troll operation have a small and insignificant result, but being a direct attack which destabilizes a society's values, then it must be treated as a mainstream attack.

Pursuing trolls and constructing a defense against them presents a major problem due to legal aspects, technological impediments that are not yet available for the larger population and dealing with large quantities of false information that is transferred at rapid speed across the internet. Each will be analyzed in detail below.

2. Fighting against trolls with some legal aspects

The legal aspects of the situation in this case is that the problem of identifying the legal definition given to what a troll is. Sanctioning trolls for their behavior has been introduced in the United Kingdom, but it targets mainly the trolls that have an aggressive behavior against other, use edited images that humiliate others, but excludes the problems of disinformation that some distribute over the internet, because it is a thin line between claiming a right to say what is right or wrong in a free speech point of view. Military trolls play by a set of rules when spreading fake news, they do not spam nor illegally upvote fake articles, but behave like normal people do and try not to get noticed as being a troll, but rather an angry citizen or just a person who expresses themselves freely.

Given the case like Aro's would be under law violations, because trolls have violated what is under the definition of law, but fake news distribution is not[13]. Disinformation is rather a subject of security and while militarized trolls have been left in the unconventional section of war[14], it seems that the authorities are not prepared to imply a mobilization of this threat among the people.

[13] For UK policy check: BBC news, *Internet trolls targeted with new legal guidelines*, [http://www.bbc.com/news/uk-37601431], 4 July 2017.

[14] I disagree with the discussions of hybrid warfare when discussing a phenomenon like militarized trolling that directly impacts a large population at an international scale.

On the online domain, companies like Google have modified their algorithm in order to promote better quality assured news, meaning that feedback sent by users of a website which distributes fake information would be downgraded from the search engine[15]. Facebook receives reports if a user has a false account and uses it to promote on social media fake articles and comments that are aggressive or make false statements[16].

3. Technological limitations of the users

This section requires a special attention and further analysis. The elements of advancement in this domain that are relevant in this context is the massive management in big data, information security which for many years has been neglected and the disproportionate high rate of gadgets used by the larger public and the verification tools of understanding and verifying the quality of data that reaches people.

Localizing the source of troll factories or websites hosted on obscure servers can be a much of a challenge similar to cyberattacks. If even discovered and urged to be closed, the hosting company would be faced with a major dilemma. One is to face a paying customer and on the other hand face a governmental figure that urges a sanction for websites used for trolling.

Trolls that used modified images that are very believable can easily convince someone that it is real. To make sure photos haven't been manipulated implies knowledge of photo editing which not all people are prepared. Online tools that show the history of editing are not quite as accurate as they say they are[17].

[15] Alex Hern, *Google acts against fake news on search engine,* [https://www.theguardian.com/technology/2017/apr/25/google-launches-major-offensive-against-fake-news], 4 July 2017.

[16] Robert Booth, *Facebook announces steps against fake news during general election,* [https://www.theguardian.com/politics/2017/may/08/facebook-help-tackle-fake-news-during-general-election], 5 July 2017.

[17] See for example https://superuser.com/questions/442352/detect-if-a-photo-has-been-manipulated-or-faked, https://www.izitru.com/, https://www.tineye.com/faq. These sites claim that they can detect edited and altered images.

In a recent study on low quality viral information, that took into account the attention span of individuals, informational overload which is a main characteristic of social media news highlights that in this kind of virtual space the capacity of distinguishing from low quality to highest quality of news, memes, videos that inform people is no longer taken into account. Thus fake and true news have the same probability to go viral.

Creating images, articles, fake comments reproduce the same structural virality[18] similar to the real facts and news. Basically trolls use the recipe to promote their spread of information, only this time the fake news can be really compared to a virus, that can have a negative reaction among individuals and alter their opinion. The online diffusion, as tested by Sharad Goel, Ashton Anderson and Microsoft Researchers Jake Hofman, Duncan J. Watts highlight that what goes viral receives powerful media coverage and web contented has been distributed by broadcasting media. The analysis that they undertook has shown that the diffusion processes the make pieces of content "viral", received media attention and powerful coverage that lead the larger population of user to adopt that event and share it via Twitter, a process that for the average user that would observe it seem natural occurring. Take for example here the promotion of the next gen iPhone, which always makes a "big deal" when the key note from Apple is approaching (my personal example).

Taking into account these two significant studies, social media has a direct impact on how information is delivered to people. Thus making disinformation spread by militarized trolls a direct threat on the public opinion and the socio-political situation in every country targeted with these kind of structural attacks on real content that expresses an interconnected-false-truth.

For fake news and taking into account the number of processes that happen on social media the attention span of people and where they read the information affects *how* they read it and *where* they read it. It is quite hard to make sure that a story is true when one reads that the Anti-Missile System from Romania, can be easily armed for attack nuclear attacks[19] when in a subway and has to be in office in 10 minutes. The fact is not true and it was highlighted

[18] Sharad Goel, Ashton Anderson, Jake Hofman, Duncan J. Watts, "The Structural Virality of Online Diffusion", in *Management Science* Vol. 62, No. 1, January 2016, pp. 180-196.

[19] *Putin: Sistemul de la Deveselu nu este defensiv*, [http://news.russiatoday.ro/putin-sistemul-de-la-deveselu-nu-este-defensiv/], 6 June 2017.

by mainstream media and troll watching groups[20] who sent readers to the Agreement between Romania and USA signed in 2011, that clearly implied that the anti-missile system cannot be armed with nuclear bombs.[21]

There is a high stake on unspecialized groups of people that would not be able to understand the implications of the situation, similar to the Deveselu which implies a set of military understanding and geopolitical explanation. Thus enters the fake news that promotes false statements about the anti-missile system and, if read, seems to have an explanatory attitude regarding the situation unlike mainstream news that only reported the implementation. This is quite a smart strategy given the fact that social media news tends to be short and to the point. The premises line up very well for the context of trolling in an age where due to the informational overload and low attention (as pointed above) in reading and informing, many people received and still do, the misleading information about what truly happen in the world.

4. Conclusions and discussions

Understanding the processes of how information and news becomes viral requires more research and empirical data gathered by specialists from both private and public sectors. The structure of a viral news either fake or true cannot be taken separately in such a system because similar to the issue of sponsored content over the internet which cannot be differentiated from normal content by readers, fake news is masked in content which is carefully tailored to look like a mainstream journalistic written article.

Disinformation and trolling on online platforms treated as an asymmetric attacks companying cyberattacks has left it as a marginalized section of defense. This mistake has led authorities to believe that the impact would be of little importance if the national IT infrastructure is secure then trolling would be a mere breeze on the internet.

[20] #Checked: Scutul antirachetă de la Deveselu nu poate lansa rachete Tomahawk și nici nu e îndreptat împotriva Rusiei, http://checkmedia.ro/checked-scutul-antiracheta-de-la-deveselu-nu-poate-lansa-rachete-tomahawk-si-nici-nu-e-indreptat-impotriva-rusiei/ , 6 July 2017.

[21] *Acord intre Romania si SUA privind amplasarea sistemului de aparare impotriva rachetelor balistice ale Statelor Unite in Romania*, https://www.mae.ro/sites/default/files/file/tratate/2011.09_scut_ro.pdf, 6 July 2017.

Only in the last years', authorities from the European Union and state representatives have started discussions regarding the problem of militarized trolls and have assessed the damages that they can create. The question still remains though, how does the online communities and governmental institutions counter-attack trolls and disinformation?

In this article I have tried to highlight that militarized trolls have a higher impact on societies across the world and the false information that they spread over the internet or aggressive behavior on comment sections have the same behavior of mainstream distribution of news which leads to the same potentiality of that false information to become viral and even taken and distributed by mainstream media.

The rise of disinformation and troll attacks can be treated as operations similar to cyberattacks which insert fake ideas in vulnerable minds, by creating false interpretations of events, decisions and arguing on false pretenses of a relative truth or promoting conspiracies.

Solutions for this new revived issue, even though countries have been taken by surprise, can be immediately implemented by pointing out and explaining specific news that has been falsified by mainstream news groups to the larger population. Due to the factor of negligence of quality information on social media platforms, sanctions for distributing false information can be introduced which will down vote and stop that post to be suggested to people on their walls.

Discussions regarding the messages that trolls send out need further improvement due to their chaotic behavior over the internet. Furthermore, data gathering on this subject and how they have staggering impact on people needs more profound results coming from media watchdog, online military organizations that have had connections with national and international firewalls against cyberattacks, because given the direct impact that falsified information can have on societies and also databases of people's opinions, militarized trolls can be treated as a complex structure of operation that is a branch of cyberattack.

Bibliography

Acord între Romania și SUA privind amplasarea sistemului de apărare împotriva rachetelor balistice ale Statelor Unite în România (2011), [https://www.mae.ro/sites/default/files/file/tratate/2011.09_scut_ro.pdf.], 5 July 2017

Aro, Jessikka (2016), "The cyberspace war: propaganda and trolling as warfare tools", in *European View,* June 2016, Volume 15, Issue 1, p. 121-132

Bertelsen, Olga (ed.), (2017), *Revolution and War in Contemporary Ukraine: The Challenge of Change, The Invisible Front: Russia, Trolls, and the Information War against Ukraine, Peter N. Tanchak,* online book [https://books.google.ro/books?hl=en&lr=&id=xCLADgAAQBAJ&oi=fnd&pg=PT232&dq=online+trolling+and+disinformation&ots=HOU6bCrFl9&sig=XU-cXZeOjmyx9364bnD65Zm-2ko&redir_esc=y#v=onepage&q=online%20trolling%20and%20disinformation&f=false], 4 July 2017

Booth, Robert (2017), *Facebook announces steps against fake news during general election,* [https://www.theguardian.com/politics/2017/may/08/facebook-help-tackle-fake-news-during-general-election], 8 May 2017

#Checked: Scutul antirachetă de la Deveselu nu poate lansa rachete Tomahawk și nici nu e îndreptat împotriva Rusiei (2017), [http://checkmedia.ro/checked-scutul-antiracheta-de-la-deveselu-nu-poate-lansa-rachete-tomahawk-si-nici-nu-e-indreptat-impotriva-rusiei/], 15 May 2017

Digital News Report News Avoidance 2017 (2017), [http://www.digitalnewsreport.org/survey/2017/news-avoidance-2017/], 4 July 2017

Duggan, Patrick Michael (2015), *Strategic Development of Special Warfare in Cyberspace,* Essay Competitions/Special Warfare in Cyberspace JFQ 79, 4th Quarter 2015

Freedom House (2017), *Populists and Autocrats: The Dual Threat to Global Democracy,* [https://freedomhouse.org/report/freedom-world/freedom-world-2017], 4 July 2017

Goel, Sharad; Anderson, Ashton; Hofman, Jake; Watts, Duncan J. (2016), "The Structural Virality of Online Diffusion", in *MANAGEMENT SCIENCE* Vol. 62, No. 1, January 2016, p. 180-196

Hern, Alex (2017), *Google acts against fake news on search engine,* [https://www.theguardian.com/technology/2017/apr/25/google-launches-major-offensive-against-fake-news], 25 April 2017

Hulcoop, Adam; Scott-Railton, John; Tanchak, Peter; Brooks, Matt; Deibert, Ron (2017), *Tainted Leaks: Disinformation and Phishing With a Russian Nexus,* [https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/], 29 June 2017

Kalogeropoulos, Antonis; Cupcea, Radu (2017), *Trolli moldoveni si razboiul lor absurd impotriva Romaniei,*[http://larics.ro/trolii-moldoveni-si-razboiul-lor-absurd-impotriva-romaniei/], 10 May 2017

Putin: Sistemul de la Deveselu nu este defensive (2016), [http://news.russiatoday.ro/putin-sistemul-de-la-deveselu-nu-este-defensiv/], 14 May 2016

Reuters.com, *U.S. government loses to Russia's disinformation campaign: advisers* (2016), [http://www.reuters.com/article/us-usa-russia-disinformation-analysis-idUSKBN1492PA], Reporter Joseph Menn, 21 December 2016.