Rainey Center

February 14, 2019

Post-Soviet Disinformation:
How Tinder Becomes a Weapon

Veronika Velch

MPS, PhD
Associate Fellow

While the world grapples with Russia's use of Twitter and Facebook to spread disinformation, a new trend has emerged in the post-Soviet space. Political operatives in Ukraine have weaponized Tinder for political purposes. This new case sets a conducting character assassination by constructing fake digital avatars. This inexpensive and efficient disinformation strategy not only destroys the victims' reputations, but also causes social and political disruption on a national scale.

THE NATALIIA BUREIKO CASE

On November 7th, 2018, Ukrainian university student Nataliia Bureiko published a Facebook post accusing a top police official of sexual harassment. Her post included screenshots of a Tinder conversation with Officer Oleksandr Varchenko. In the screen shots, Varchenko threatens her when she turns down his demand for a sexual relationship. Bureiko's bombshell Facebook post also claimed that Varchenko mailed her flowers with a box of raw chicken legs, and had also harassed her family and friends.

Her post became an overnight media sensation. It racked up several thousand comments and shares in just a few days. Almost all of the comment expressed outrage, not just at Varchenko, but at the police and government as a whole.

Several of Ukraine's most popular news sites, including unian.net, strana.ua, and korrespondent.net, ran the story. Bureiko also made a formal report at the Prosecutor's Office (the Ukrainian equivalent of a District Attorney). There was one problem with Bureiko's story: she and Varchenko both claim it was entirely false.

Two days later, Bureiko later posted a retraction on Facebook, saying "I feel so ashamed. I, Nataliia Bureiko, wrote a post about threats from Oleksandr Varchenko on the Facebook social network without looking into the situation or being aware

of my actions. I wanted to protect myself but harmed other people." Bureiko spent 3 weeks out of the public eye. She did not respond to countless media requests and remained silent on social media. In Bureiko's absence, social media users floated multiple theories about her whereabouts. One of those theories held that Varchenko had killed her in retaliation.

Varchenko denied the allegations, writing on Facebook that he had never corresponded with Bureiko. He continued, "I do not rule out that hackers may have created an account with my photos and used it to lead provocative correspondence with Nataliia Bureiko. I think this information attack is related to the fact that my wife, Olga Varchenko, is the first Deputy Director of the State Bureau of Investigations, and for many it was a bone in the throat."

While Bureiko was nowhere to be found, her supporters assumed that Varchenko's allies had forced her to retract her accusation and had then either killed her or intimidated her into hiding. Bureiko was alive, but when she resurfaced almost a month later, her story had changed. She reemerged in the public eye in an interview with strana.ua.[1] Bureiko claimed that someone she knew had offered to pay her roughly 50 USD in exchange for access to her Facebook account.

That same individual, Bureiko said, told her to file a complaint at the Prosecutor's Office if she ever wanted to get her normal life back. Bureiko never named the person who allegedly did this. She expressed regret at being used to facilitate a fake news campaign.

Shortly thereafter, Bureiko turned herself in to the Ukrainian police, testified to the scheme, and started living in a secret location under the protection of Ukrainian law enforcement. To this day, no one knows the real story. The damage has been done.

On December 10th, 2018, the Chief Military Prosecutor of Ukraine announced that he had identified 11 people involved in recent information attacks, including the Tinder scandal.[2] The 2 suspects most closely tied to the Tinder attack are the infamous Ukrainian "political technologist" Volodymyr Petrov, and the other is his friend, a blogger and former Advisor to the Minister of Information Policy, Olexandr Baraboshko.

The Chief Military Prosecutor announced that law enforcement authorities had seized 230,000 USD from a safe deposit box belonging to Petrov, and that the perpetrators of the sex

1 Zolotukhina, Inna. "Member of the sex scandal in the "Ukrainian FBI" Natalia Bureyko: I had to pay a half thousand hryvnia," Strana.ua, 28 November 2019. https://strana.ua/articles/interview/174024-zhertva-seks-skandala-s-chinovnikom-burejko-u-menja-nikohda-ne-bylo-akkaunta-v-tindere-.html

2 "PGO: Political consultant Petrov, Blogger Baraboshko, other 9 suspects got secret information from source in State Guard Department," Ukrainian News, 10 December 2018, accessed 11 February 2019. https://ukranews.com/en/news/601157-pgo-political-consultant-petrov-blogger-baraboshko-other-9-suspects-got-secret-information-from

scandal had received 10,000 USD as payment for their services.[3] The source of that payment has not been publicly identified.

Petrov remains on house arrest, from where he has launched his presidential campaign. Baraboshko, however, spent several days in jail but was released when his friends paid bail, set at the equivalent of 110,000 USD.

MOTIVES FOR DISINFORMATION ATTACKS

This disinformation attack is notable for how it dominated a nation's news cycle for months, and also for how simple it was to carry out.

Dividing the nation proved frighteningly easy. Ukrainians picked sides and argued online. Some thought Bureiko was a victim, while others said she deserved jail time, given the seriousness of the accusations.

Creating a fake Tinder conversation does not require sophisticated technological abilities. Anyone can do this. Thanks to a lack of fact-checking, this story polarized Ukrainians and sowed distrust in the police.

This societal division was ignited by overwhelming volume of noize. While more credible media were investigating a story, the less credible one, like strana.ua, piked it up. Strana.ua is often caught spreading fake news, especially in the form of Russian propaganda.[4] Detector Media, Ukraine's premier independent news monitoring outlet, has published excellent examples of Strana's heavy biased in favor of Russia and against Ukraine. [5]

This information attack was multidimensional and needs to put in the following context:

First, it embraced the existing social disruption. A few weeks earlier, on November 4th, Ukrainian anti-corruption activist and deputy mayor of Kherson Kateryna Handzyuk was killed by an acid attack. Handzyuk was known for fighting against pro-Russian movements in Eastern Ukraine. At the beginning of December, the Prosecutor General claimed the main suspects were identified and the most likely motive was retaliation for Handzyuk's anti-corruption activities. Ukrainian civil society was fixated on this, and people protested en masse in an attempt to demand justice.

Second, this attack deepened the distrust of Ukrainian police and the State Bureau of Inves-

3 "Police take USD 230,000 of political consultant Petrov," Ukraine News, 10 December 2018, accessed 12 February 2019. https://ukranews.com/en/news/601159-police-take-usd-230000-of-political-consultant-petrov

4 Burkovskaya, Peter, "'Strana.ua' depicts Ukraine as an aggressor," Media Sapiens, 4 July 2018. https://ms.detector.media/monitoring/advocacy_and_influence/yak_stranaua_zobrazhae_ukrainu_agresorom/

5 Bakhtyev, Boris, "'Strana' a total manipulation," Detector Media, 31 March 2017. https://detector.media/kritika/article/124663/2017-03-31-strana-totalnykh-manipulyatsii/

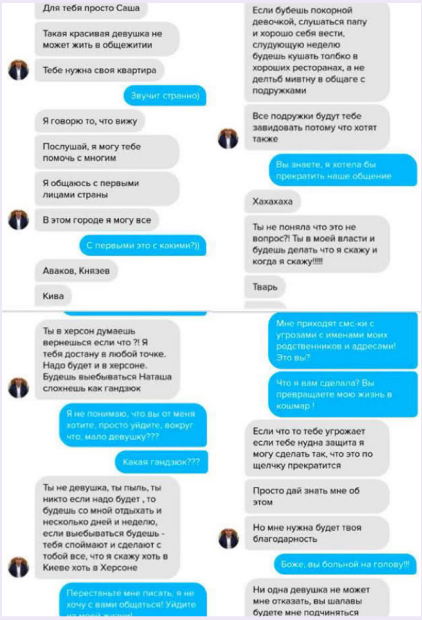
tigations. Pro-Russian outlet Strana.ua published the story as breaking news without vetting the details. This is unsurprising, as the false story fit the outlet's preferred narrative that Ukrainian government agencies are corrupt and not to be trusted. The more corrupt the Ukrainian government appears to the public, the more people tend to view Russian authorities as trustworthy in comparison.

Third, Tinder may be a testing ground for developing the technology that combines kompromat and digital platforms. The Tinder attack clearly follows the pattern of Russian kompromat, a sabotage technique favored by the KGB and its successor agency, the FSB.

Kompromat has never been easier or cheaper to manufacture. According to Katy Pearce writing at the Washington Post, "In the 1990s, an individual seeking to discredit a rival could place a compromising news article in the most popular Russian daily newspaper, paying between $8,000 and $30,000 for it…a television story to disgrace someone could cost between $20,000 and $100,000."[6] Creating a dating app account, however, is free. So is posting on social media. Anyone can invent Kompromat and then deploy it to the world.

Ukraine is also fertile ground for testing the likelihood of a society to fall for fake news. According to the Disinformation Resilience Index,[7] a study on the ability of post-Soviet countries to identify and resist disinformation, a major weakness in the region is the lack of media compliance with journalistic standards. Reporters and editors often fall short of the standards they set for themselves, and consequences are exceedingly rare. Consequences for the victims of disinformation campaigns, however, are painfully real.

Stories like this one form a pattern of successful disinformation projects. In 2004, Ukraine took its first decisive step away from the Kremlin.



Tinder Chat

Source: https://img.pravda.com/images/doc/8/f/8f81410-5perepyska-original.jpg)

6 Pearce, Katy, "Kompromat used to be a KGB tool in the Soviet Union. Now anyone can collect dirty data," Washington Post, 13 January 2017. https://www.washingtonpost.com/news/monkey-cage/wp/2017/01/13/kompromat-used-to-be-a-kgb-tool-in-the-soviet-union-now-anyone-can-do-it/?noredirect=on&utm_term=.082d0ef0fcd4

7 "Disinformation in Central and Eastern Europe," Prisma UA, June 2018. http://prismua.org/wp-content/uploads/2018/06/DRI_CEE_2018.pdf

In retaliation, Russian "political technologists" launched the campaign "three sorts of Ukraine" designed to ignite hostility and fuel conflict.

REAL-LIFE CONSEQUENCES OF TINDER WEAPONIZATION

First, this type of digital campaign created as an alternative digital personality, and it's almost impossible to divide where is fake and where is a truth. These days, if you would google Olexandr Varchenko in Ukrainian, his name appears with the cloud of words like "harassment," "scandal," "Tinder," and so on. Controversial headlines are followed by images of the "Varchenko" Tinder account's chat with "Natalia Bureiko" and a bowed box of chicken legs. Olexandr Varchenko's public image is forever tarnished by a digital avatar that was created and managed by someone else. A proposed "right to be forgotten" policy would erase these false news stories of sexual harassment accusations, but the same policy may also erase stories of the real crime committed here.

Second, false information attacks foster societal distrust of the media, government institutions, and other people. People are right to be skeptical of organizations that repeatedly lie. Their skepticism is not the root problem, the institutional lack of trustworthiness is. A society in which media, government, and others cannot be trusted is not a healthy one.

Third, the Varchenko-Bureiko Tinder scandal could be the beginning of a new era of post-Soviet disinformation. The social media environment makes it easy for people to represent themselves online, but also makes it easy for people to fraudulently represent others in the digital world. As digital avatars proliferate across platforms, verifying their accuracy without compromising personal privacy becomes a challenge. This case demonstrates the frightening ease of using dating apps and social media to create social disruption and political turmoil.

GLOBAL APPLICABILITY OF THE UKRAINIAN MODEL

Dating apps are everywhere, and so are the means to represent oneself - or misrepresent someone else - on those platforms. America's enemies know that our media is susceptible to spreading fake news. They also know that spreading disinformation does not require a government apparatus. A salacious story made up by an individual can end up getting nationwide attention. For instance, the "Jackie" case about an alleged gang rape at the University of Virginia was based on a single interview with one student. Even when the story was completely discredited, the accused fraternity - and college Greek systems as a whole - are still looked upon skeptically by the general public. Causing damage is easy, rehabilitating the one's reputation in digital is much harder.

Social media is the perfect vehicle to spread outrageous stories. Viral content almost always elicits a strong emotional response.. According to a study published in the Proceedings of the National Acad-

emy of Science, people are more likely to react to emotional content rather than logical content when consuming that content on social media platforms.[8] The study analyzed 563,312 tweets on the topics of gun control, same-sex marriage and climate change. Researchers found that adding one moral-emotional word to the tweet on these topics increased the expected retweet rate by an average of 20%.

HOW WE CAN PROTECT OURSELVES

The best innoculation against fake news is the knowledge that it exists and that anyone can create it for nefarious purposes. Social media, including dating apps, makes it easier than ever to both create fake conversations and disseminate them.

Since social networks are simplifying the process of sharing viral content, the biggest responsibility of traditional media is to sort, check, and analyze the information before helping it spread even further.

At the institutional level, media organizations are incentivized to attract viewers to a story. News organizations get paid by how many people visit their sites (and view and/or click the advertisements there). They do not get paid more for stating truth or pay penalties for spreading falsehoods. Market forces drive the success or failure of any private sector media enterprise. We are fortunate here in the United States that consumer demand can cause change, as opposed to societies in which the government funds major media outlets; those outlets have little, if any, incentive to respond to consumer demand.

At the individual level, people need to be responsible consumers of media. By sticking to trusted media outlets, and even using social media to press reporters, witnesses, and participants to verify their claims, consumers can lead a media revolution that rewards veracity over shock value. When the market demands evidence, media businesses will look for it.

The rise of viral content allows anyone to make news, but not all viral content is truthful. Media organizations need to earn the trust of the people by verifying stories before publishing. Consumers need to reward ethical media organizations by frequently turning to them, rather than reading and watching uncorroborated stories that contain no evidence of their splashy claims. Otherwise, significant damage to political stability can be inflicted with something as simple as a fake Tinder profile.

8 Brady, William J.; Wills, Julian A.; Jost, John T.; Tucker, Joshua A.; Van Bevel, Jay J.; "Emotion shapes the diffusion of moralized content in social networks," Proceedings of the National Academy of Sciences of the United States, 11 July 2017, 114 (28) 7313-7318. https://doi.org/10.1073/pnas.1618923114

WORKS CITED

Bakhtyev, Boris, "'Strana' a total manipulation," Detector Media, 31 March 2017. https://detector.media/kritika/article/124663/2017-03-31-strana-totalnykh-manipulyatsii/

Brady, William J.; Wills, Julian A.; Jost, John T.; Tucker, Joshua A.; Van Bevel, Jay J.; "Emotion shapes the diffusion of moralized content in social networks," Proceedings of the National Academy of Sciences of the United States, 11 July 2017, 114 (28) 7313-7318. https://doi.org/10.1073/pnas.1618923114

Burkovskaya, Peter, "'Strana.ua' depicts Ukraine as an aggressor," Media Sapiens, 4 July 2018. https://ms.detector.media/monitoring/advocacy_and_influence/yak_stranaua_zobrazhae_ukrainu_agresorom/

"Disinformation in Central and Eastern Europe," Prisma UA, June 2018. http://prismua.org/wp-content/uploads/2018/06/DRI_CEE_2018.pdf

Pearce, Katy, "Kompromat used to be a KGB tool in the Soviet Union. Now anyone can collect dirty data," Washington Post, 13 January 2017. https://www.washingtonpost.com/news/monkey-cage/wp/2017/01/13/kompromat-used-to-be-a-kgb-tool-in-the-soviet-union-now-anyone-can-do-it/?noredirect=on&utm_term=.082d0ef0fcd4

"PGO: Political consultant Petrov, Blogger Baraboshko, other 9 suspects got secret information from source in State Guard Department," Ukrainian News, 10 December 2018, accessed 11 February 2019. https://ukranews.com/en/news/601157-pgo-political-consultant-petrov-blogger-baraboshko-other-9-suspects-got-secret-information-from

"Police take USD 230,000 of political consultant Petrov," Ukraine News, 10 December 2018, accessed 12 February 2019. https://ukranews.com/en/news/601159-police-take-usd-230000-of-political-consultant-petrov

"'The Wroclaw sex scandal is like an information attack' - an expert," Radio Ukraine International, 10 November 2018. http://www.nrcu.gov.ua/news.html?newsID=82319

Zolotukhina, Inna. "Member of the sex scandal in the "Ukrainian FBI" Natalia Bureyko: I had to pay a half thousand hryvnia," Strana.ua, 28 November 2019. https://strana.ua/articles/interview/174024-zhertva-seks-skandala-s-chinovnikom-burejko-u-menja-nikohda-ne-bylo-akkaunta-v-tindere-.html

RAINEY CENTER

The Rainey Center is a post-partisan, 501(c)3 think tank and leadership community by and for women, minorities, and political mavericks, named after Rep. Joseph Rainey, a former slave who was the first African-American to serve in the United States House of Representatives.

80 M Street SE
Washington, DC 20003

Website
raineycenter.org

Email
info@raineycenter.org