ITSS
International Team
For the Study of Security
Verona

Disinformation as part of Modern Warfare’s Cyber-attacks

by Joseph Moses

ITSS Verona Magazine, Vol. 1, no. 1

Spring/Summer 2022

Disinformation as part of Modern Warfare’s Cyber-attacks

Joseph Moses

To cite this article: Joseph Moses, *Disinformation as part of Modern Warfare's Cyber-attacks*, ITSS Verona Magazine, Vol. 1, no. 1, Spring/Summer 2022.

Keywords: Ukraine, Russia, Disinformation, Cyber-attacks, OSINT

ITSS Verona website: https://www.itssverona.it/itss-magazine

LinkedIn: https://www.linkedin.com/company/itss-verona/

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Twitter: https://twitter.com/itssverona

Published online: June 18th, 2022

Disinformation in the online realm is nothing new to any of us. However, the creation of narratives, false or unconfirmed urban legends and state-published propaganda all affect morale – which directly affects troops and the public on the legitimacy of one's struggle on the ground, while also subverting narratives of the raw data people across the world get from social media and the mainstream about the conflict.

The presence of the OSINT (Open-Source Intelligence) community is being felt much more because of the proliferation of smart devices with internet access, while the spontaneous creation of independent and novel journalism groups to cover crises and events help provide an alternative to the mainstream and state-owned news sites and publications. These sometimes compliment each other or are at odds over what data or narrative is being put out. The information crisis, in both driving forward a narrative and for data collection, is a challenging task, especially in the current case of the invasion of Ukraine, which at the time of writing, is over a month in. When it comes to cyber-attacks in conventional wars, they have, in most cases, preceded the guns and tanks to both create panic and a sense of distrust and confusion of online information, and also as an attempt to subvert and disrupt civilian and military infrastructure. While these attacks still persist, the increase in social media usage has proliferated one mode of cyber-attacks, and that is information (*Why Disinformation Is a Cybersecurity Threat*, 2021).

Some of the most prominent state-state incidents of cyber disruption and/or disinformation have been the 2007 cyber-attacks on Estonia, during the 2008 attacks on Georgia during the invasion of Georgia and in 2022, preceding the invasion of Ukraine and the subsequent cyber-attacks on Russian websites by Anonymous. This paper will focus on the role of disinformation and the increasing prevalence of it as an aspect of the cyber onslaught to subvert narrative in modern warfare, in an attempt to legitimize one belligerent whilst delegitimizing the narrative of the other. It attempts to emphasize that not all cyber-attacks in perception need be an infrastructural attack alone, but also purely targeted against the consumer through the cyber medium through plain (dis)information and not just manipulated code.

Estonia: Tallinn's Bronze Soldier incident

The Bronze Soldier was a controversial Soviet memorial built at the site of several war graves. The Bronze Soldier had symbolic value to Estonia's Russians, symbolizing the defeat of Nazi Germany and their influence over Estonia, while the Estonians perceive it as a symbol of Soviet occupation post-World War II. In 2006, there was a petition to demolish the monument and a subsequent bill to facilitate its destruction, a move which was vetoed by the President. In February of 2007, Estonian nationalists attempted vandalizing it, following which the government claimed that the memorial ought to be relocated somewhere else and that Tallinn's intersection was not a proper place. This led to mass protests and riots for over two nights and was the worst Estonia had seen.

Estonia was targeted during this time with large-scale cyber-attacks. Botnets were used to flood servers and spam distribution. Botnets are individual internet-connected devices which are all used to launch a Distributed Denial of Service (DDoS) attack. In a DDoS, the devices(botnets) used may be the hacker's own devices or infected devices accessed remotely by the hacker without the knowledge of the owner. Political party websites were defaced and news portals' commentaries were spammed ("Estonia Fines Man for 'Cyber War,'" 2008). There were also attempts to change the Bronze Solder's Wikipedia page. Multiple Distributed Denial of Service (DDoS) attacks were facilitated by both individuals and botnets. Sources in 2009 claimed responsibility for the attacks, coming out of the Kremlin or groups supported by the Kremlin.

The uniqueness of these attacks was that it was not purely state-sponsored but state-encouraged. Many of these hackers are believed to have enjoyed autonomy. Most of these were DDoS attacks meant to crash servers and slow down services. It was considered more of a broad attack on Estonia and its cyber services than of a targeted military attack. Banking services, media, police and government networks were all brought down. This virtual blitzkrieg was also successful because Estonia was one of the most networked countries in Europe at the time (Davis, 2007). The attackers had initially used low intensity attacks, like ping floods, and simple DoS attacks. After three days, on the 30th of April, DDoS attacks through botnets were used to attack from 85,000 hacked computers. The online services of Estonia's largest bank, Hansabank, were down for a few hours. The reason this deserves a mention here is because it was one of the largest country-wide attacks by state-backed hackers and was similar to the attacks that followed in 2008 in Georgia.

Cyber-attacks during the Russo-Georgian war, 2008

The armed conflict took place between the Russian Federation and Georgia in the August of 2008. It was triggered by the proximate cause of a territorial dispute over South Ossetia. The cyber assault was initiated almost 10 days before the military intervention by Russia. This was the first time a cyber-attack happened in synchronization with a conventional military operation. Georgia's national bank and the ministry of foreign affairs' websites were defaced. Websites of public and private services, news media and multiple other websites were all brought down with DoS attacks. Malware and malicious scripts were distributed through online forums. Email addresses of politicians were spammed and effects of this attack were relatively small as well. Instead of massive disruption, this attack had little effect beyond making internet access difficult and the government's ability to communicate internationally. This attack was not genuinely political in nature and was widespread.

Although fingers were pointed at Russia, NATO concluded that as with Estonia, "*there is no conclusive proof of who is behind the DDoS attacks*". The Russians launched an information campaign where Russian journalists were brought along with the Russian troops to report on the progress of the troops and highlight Georgian atrocities. This was very helpful for the Russians as it was these reported atrocities that were the proximate cause for Russian intervention (*Russian Ambassador to Georgia: At Least 2,000 People Died in Tskhinvali*, 2008).

As Thomas Rid mentions, in both of these attacks, the utility of disruption was limited and it was the precedent and warlike rhetoric that surrounded them that was responsible for their high profiles, however, the subversive side of the attacks – DDoS and Disinformation and half-truths – helped invoke a sense of panic in the public and a sense of distrust in their governments. As a subversive tactic, they are more outcomes of collective passion than strategic in the military sense.

Disinformation in the Russo-Ukrainian war, 2022

While this conflict was also subjected to traditional cyber-attacks, it is also called the "first social media war", with disinformation spreading from TikTok, Telegram to Twitter and only later trickling down to the mainstream media (Suciu, 2022). Unlike what we would consider traditional cyber-attack (DDoS) this exploits a fundamental flaw in information security; the human being behind the screen, like the instance in phishing attacks.

As of the time of writing, the invasion of Ukraine is over a month in, and this article will only cover the cyber-attacks and the disinformation campaign directed towards both Ukraine and Russia only within this time period. Many of the incidents mentioned below are from secondary sources and are mostly as of yet unpublished resources.

Almost a week before the invasion took place, a high-volume cyber-attack temporarily blocked websites of Ukrainian defense agencies and banks and was deemed the largest of such an attack in the history of the country (CNN, 2022). It was a DDoS attack that was reportedly well-planned. These websites were down for a day. This was occurring as Russia had amassed around 150,000 troops on the Ukrainian border. Under Secretary of State from the US government, Victoria Nuland stated that it was "*Obviously, the Kremlin*", as this was a signature Kremlin move. The Ukrainians responded very quickly and the websites were recovered while the DDoS attacks were still underway. Ukraine concluded that it was Russia and Belarus responsible for the attack that hit them the previous month. The effect of it was mostly psychological. In an attack in January 2022, many government websites were targeted with messages stating that Ukrainians' personal information had been hacked. It displayed the message, "*Ukrainian! All your personal data has been uploaded to the public network. All data on the computer is destroyed, it is impossible to restore them. All information about you has become public, be afraid and wait for the worst. This is for you for your past, present and future. For Volhynia, for the OUN (Organization of Ukrainian Nationalists) UIA (Ukrainian Insurgent Army), for Galicia, for Polesie and for historical lands*", in Polish, Ukrainian and Russian (Newsource, 2022). While the message is interpreted to have subversive effects and point fingers away from Russia, the style of attack and the timing of it, casts doubt on Russia. Oleh Derevianko, founder of ISSP, a cybersecurity firm said, "*It's a good illustration how you can use a simple defacement attack as an informational operation tool when everyone is so nervous and agitated about potential information*" (CNN, 2022).

Following these attacks, there were multiple reports of car bombings in the Donbass, which the Russians speculated to be the work of the Ukrainians, where, upon closer inspection of the images that came out of the aftermath of the attack, the bodies in the vehicles appear to have cuts performed during an autopsy on their skulls – implying the use of cadavers to stage a false-flag attack (Waters, 2022). Videos of these were shared to stoke tensions within the Eastern Ukrainian ranks and help justify Putin's "Special Military Operation."

Following these cyber-attacks, after the start of the invasion, the hacker group Anonymous, released confidential contact information about employees of the Russian Ministry of Defense, after which videos were released from Ukraine of people allegedly calling those numbers and confronting them. Anonymous also took down a news site, Russia Today and hacked Russian state TV channels to broadcast Ukrainian themed songs (Milmo, 2022). Many other incidents of disinformation are allegations are wholesale publications of Russian propaganda against Ukraine (WION, 2022).

There have been multiple incidents of videos through both social media and OSINT channels showing captured Russian armored vehicles which were later proven to be Ukrainian and vice versa. The story of the heroic 13 soldiers who were said to have been killed on Snake Island were later found to be alive, totaling up to 82, according to Russian state media. It is now confirmed in a Facebook post by Ukraine's Naval Forces that the soldiers survived the viral radio exchange where the soldiers based on the island said "*Russian warship, go f*** yourself.*" (BBC, 2022). Multiple photos of Ukrainian President Volodymyr Zelenskyy donning military uniform, which were shared widely on social media as a rallying call and which invoked waves of support online, were fact checked to have been pictures from an inspection of a military bunker in 2021. A tweet about this on the second day of the invasion received almost 3,000 retweets in three days alone (Vercellone, 2022). Many pictures of the injured and the wounded being shared were proven to be from different incidents and from different years. A few claims of disinformation have been fact-checked while others are still out in the wild (Reuters, 2022). Meanwhile, many of these pictures and videos become the basis of what we see of the war and of how we see it progressing. Multiple narratives of this sort have been pushed by official sources, which implies that it is intentional and pushed forward by the state. Some of the most famous incidents of online disinformation - intentional, unintentional or ambiguous - are about the narratives of the Ghost of Kyiv, the Bucha massacre and the Kramatorsk railway station bombing.

The video of the Ghost of Kyiv was about a Mig-29 pilot who allegedly shot multiple Russian jets, six of them according to a few reports. In one viral video which shows the Mig chases and shoots down another plane, it was alleged that this was the Ghost of Kyiv and the video has Ukrainian narration. The video sequence, it was exposed later, was from the video game Digital Combat Simulator World. Former Ukrainian President Poroshenko posted the photo later of a helmeted pilot in a cockpit identifying him as the Ghost. The photo was revealed to be from three years back (Welle, 2022). After revealing that this video was from a video game, multiple social media accounts, mostly Western and American, reposted the videos regardless stating that they "*want to believe*" anyway.

Regarding the Bucha massacre, soon after details of the corpses lining the streets of Bucha were released, Russian Telegram channels were in an uproar, contesting the timelines mentioned, the positions of the corpses, the lack of decoloring of the corpses and accused Ukraine of staging the incident which would result in the obvious interpretation of it being a mass execution event. While most of these Russian claims have been argued to be false by Bellingcat (Higgins, 2022), this goes to show that *if* the incident were staged by the Ukrainians, like the Russians had accused, it proves to be a very effective disinformation campaign. On the other hand, most Russian Telegram channels, which seem to be the primary source of dispersion of on-the-ground media and deduction of media, have stopped short of the counter-claims to the initial Russian claims.

The latest controversial event of significant political attention after Bucha has been the Kramatorsk railway station bombing by cluster munitions. The recent bombing of the railway station in Kramatorsk was carried out by a Tochka missile and more specifically, the Scarab-B variant of the Tochka called the Tochka-U. Ukrainian media immediately blamed and asserted that the attack was by the Russians with their Iskandr missiles (Ukrayinska Pravda, 2022). This was soon proven false after images of the remnants of the missile proved it to be a Tochka missile. The Russians immediately blamed the Ukrainians citing that Ukrainians used Tochka missiles elsewhere while the Russians have phased out the Tochka missiles in favour of the Iskandr missiles (TASS, 2022). This was soon met with Ukrainian claims that Russians were seen using Tochka missiles in the region as well, which is completely realistic (Ukrinform, 2022b). Ukrainians have previously claimed that pervious attacks in Donetsk on March 14 carried out with Tochka missileswere Russian strikes based on the the direction in which the remnants of the missile were lying in which was the same argument that the Russians are using to claim the strike on Kramatorsk was from the Ukrainian forces (Ukrinform, 2022a). While the general consensus is that the strike on Kramatorsk was Russian, given that the methodology of the analysing information from the strike on Donetsk on March 14 and the one on Kramatorsk are the same, this gives the Russian claim that the missile came from Ukrainian held territory some legitimacy. While still shrouded in mystery at the time of writing and not easily conclusive, this shows the effect of disinformation and misinformation on either belligerents' populations and if successful on winning the global trust whilst still controversial, shows how verifying information from traditional fact-checkers becomes exponentially difficult.

Conclusion

Scholars like Thomas Rid have used Clausewitz to argue against the notion of a "cyber war" because of the lack of politically strategic and military tactical objective gained whereas there seems to be more anonymous protest through disruption, espionage and subversion and the lack of lethality resulting directly from a cyber-attack (Rid, 2012). The Tallinn Manual 2.0, released in 2017 however, has in its foreword in a reference to the 2007 Bronze soldier incident, "*In retrospect, these were fairly mild and simple DDoS attacks, far less damaging than what has followed. Yet it was the first time one could apply the Clausewitzian dictum: War is the continuation of policy by other means*". The more that states back cyber-attacks, or there exists a widespread counter-narrative , and attacks of a disruptive and/or subversive nature in tandem with conventional armed conflicts, these take on a political role, however anonymous or decentralized they may be as they attack/feed the legitimacy of a political narrative - thus the legitimacy of subsequent military action and vice versa. Thomas Rid argues that cyber-attacks are not acts of "war" in the Clausewitzian sense because they are never at once all three: instrumental, tactically, physically violent and politically motivated. However, given the decentralized nature, in terms of morale, even though it may lack direct physical violence, it could arguably be effective in the strategic sense and directly contributive to the war. It could be used as a decentralized tool of war, where rhetoric, narrative and propaganda are not merely in order to shape public opinion in the long term, but also tactically, used to fudge the perception of an incident for a limited period of time immediately. The only difference is that, here, instead of providing a mirage or an illusion to a particular enemy, this is done collectively and unintentionally to both boost and deteriorate morale across the board and even globally. (Dis)information here is shared intentionally or unintentionally to an extent where it is widely shared and thus taken to be a truth by consensus, thus delegitimizing even *questions about* a counter-narrative.

This, coincidentally, is complemented by the Russian Gerasimov doctrine.

Given the role cyber-attacks play in terms of disruption and digital chaos, digital disinformation is beginning to rear its head as a significant tool in the cyber realm as a tool of affecting morale – rather than mere digital blindness – and narrative. While independent reporting services and false messages can be used to spread a false narrative fast, fudged images and videos and deepfakes can lend image and video data itself, even absent of narrative, to be subversive unless subjected to reverse engineering, by which time, it would've been a conflicted topic of discussion anyway. This, with the increased reaction times of news agencies, and social media and the self-feeding panic disinformation can wreak, combating it, is crucial for both participants of a conflict and for observers outside trying to sift through fudged data, hearsay and sponsored narratives to arrive at what could be closest to the truth of the situation on the ground. And even if these attacks do not constitute "cyber war" as Rid argues, the role of the cyber realm, in disrupting state media (narrative-pushers), distributing disinformation and false or convenient narratives, directly affects morale of the troops on the ground and of the public at home. Whether they qualify within the nomenclature of cyberwar or not, the importance of reverse engineering images and videos and the intensity of OSINT work will and must increase to put these offshoots of different narratives from ambiguous information, in check. As described by Tom Sear, since the attack on Estonia in 2007, internet-based incursions have escalated but the targets have become more diffused. He stated that "*Direct attacks on a nation's defence forces, while more threatening, may in the future be less common than those that target information and* *opinion*” (Sear, 2017). Given reported Russian logistical failure in the ongoing invasion, and initial reports of low morale among the Russian ranks, disinformation further affects said morale and subsequently affects the different public perceptions of the legitimacy surrounding the conflict (INEWS, 2022). Disinformation in general, like urban legends and assertions of atrocities committed by either side as the conflict is going on is very difficult because of the fog of war and vested interests of the media outlets involved.

Reference list

BBC. (2022, February 28). Snake Island: Ukraine says troops who swore at Russian warship are alive. *BBC News*. https://www.bbc.com/news/world-europe-60554959

CNN, S. L., Anastasia Graham-Yooll, Tim Lister and Matthew Chance. (2022, February 16). *Ukraine cyberattack is largest of its kind in country's history, says official*. CNN. https://edition.cnn.com/2022/02/16/europe/ukraine-cyber-attack-denial-service-intl/index.html

Davis, J. (2007, August 21). *Hackers Take Down the Most Wired Country in Europe*. Wired. https://www.wired.com/2007/08/ff-estonia/

Estonia fines man for "cyber war." (2008, January 25). *News.bbc.co.uk*. http://news.bbc.co.uk/2/hi/technology/7208511.stm

Higgins, E. (2022, April 4). *Russia's Bucha "Facts" Versus the Evidence*. Bellingcat. https://www.bellingcat.com/news/2022/04/04/russias-bucha-facts-versus-the-evidence/

INEWS. (2022, March 6). *Morale of Russian troops is being hit due to "mess" of Ukrainian invasion, military chief says*. Inews.co.uk. https://inews.co.uk/news/morale-of-russian-troops-is-being-hit-due-to-mess-of-ukrainian-invasion-military-chief-says-1500783

Milmo, D. (2022, February 27). *Anonymous: the hacker collective that has declared cyberwar on Russia*. The Guardian. https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

Newsource, C. N. N. (2022, January 14). *Cyberattack hits Ukraine government websites*. KESQ.https://kesq.com/news/2022/01/14/massive-cyber-attack-hits-ukraine-government-websites/

Reuters. (2022, March 4). Fact Check-Photo of Ukrainian woman injured in shelling attack was captured on Feb. 24. *Reuters*. https://www.reuters.com/article/factcheck-ukraine-chuhuiv-idUSL2N2V70MK

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Russian Ambassador to Georgia: at least 2,000 people died in Tskhinvali. (2008, August 9). Interfax.ru. https://www.interfax.ru/russia/26124

Sear, T. (2017). *Cyber attacks ten years on: from disruption to disinformation*. The Conversation.https://theconversation.com/cyber-attacks-ten-years-on-from-disruption-to-disinformation-75773

Suciu, P. (2022, March 1). *Is Russia's Invasion Of Ukraine The First Social Media War?* Forbes.https://www.forbes.com/sites/petersuciu/2022/03/01/is-russias-invasion-of-ukraine-the-first-social-media-war/

TASS. (2022). *Tochka-U missiles not in service in Russian Armed Forces — mission to UN*. Tass.com. https://tass.com/politics/1423317

Ukrayinska Pravda. (2022). *Russians hit train station in Kramatorsk with Iskander ballistic missiles: dozens dead, more then hunred injured*. Ukrayinska Pravda. https://www.pravda.com.ua/eng/news/2022/04/8/7338073/

Ukrinform. (2022a). *CIT: Tochka-U strike on Donetsk was Russia's provocation*. Www.ukrinform.net. https://www.ukrinform.net/rubric-ato/3430801-cit-tochkau-strike-on-donetsk-was-russias-provocation.html

Ukrinform. (2022b). *Ukraine at OSCE exposes Russian lies about Tochka-U missile attack on Kramatorsk*. Www.ukrinform.net. https://www.ukrinform.net/rubric-ato/3455256-ukraine-at-osce-exposes-russian-lies-about-tochkau-missile-attack-on-kramatorsk.html

Vercellone, C. (2022, February 28). *Fact check: Viral image of Volodymyr Zelenskyy in uniform is from 2021*. USA TODAY. https://www.usatoday.com/story/news/factcheck/2022/02/28/fact-check-volodymyr-zelenskyy-pictured-uniform-donbas-2021/6971781001/

Waters, N. (2022, February 28). *"Exploiting Cadavers "and "Faked IEDs": Experts Debunk Staged Pre-War "Provocation" in the Donbas*. Bellingcat. https://www.bellingcat.com/news/2022/02/28/exploiting-cadavers-and-faked-ieds-experts-debunk-staged-pre-war-provocation-in-the-donbas/

Welle (www.dw.com), D. (2022, March 1). *Fact check: Ukraine's "Ghost of Kyiv" fighter pilot | DW | 01.03.2022*. DW.COM. https://www.dw.com/en/fact-check-ukraines-ghost-of-kyiv-fighter-pilot/a-60951825

Why Disinformation is a Cybersecurity Threat. (2021). EU DisinfoLab. https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat/

WION. (2022, March 4). *Digital weaponry: Russia using deepfakes to spread misinformation against Ukraine, claims report*. WION. https://www.wionews.com/world/digital-weaponry-russia-using-deepfakes-to-spread-misinformation-against-ukraine-claims-report-458746