The Role Of Disinformation, Propaganda And Active Measures In Cyber Warfare. Noname(057)16 Travels To Italy

Arturo Di Corinto[1]

[1] *Sapienza University of Rome, Piazzale Aldo Moro, 4, Roma, Italia*

Abstract

Disinformation is the hidden and intentional attempt to convey false and biased information aimed at changing the behavior of the recipient. Propaganda, on the other hand, openly addresses the public by emphasizing some information and omitting others with the aim of creating consensus around the object of communication. When we talk about the differences between disinformation and propaganda, the emphasis is therefore on intentionality, the level oftransparency and public acceptance.

Generally we distinguish disinformation from misinformation or bad information, and we attribute the latter to the biases and errors of those who convey it. However, it is the same concept of information, "putting into a shape", which makes us understand that information is always the final product of a subjective process of retrieval, selection, and communication of a piece of data or a factual event. In addition, its reception, and the effects it produces, is always the product of a negotiation process that concerns the issuer and the recipient of the same.From here it follows that "truthfulness" as an objective quality of information does not exist. Perceived truth is always the fruit of a process of convergence of perceptions and cognitions shaped by experience, culture, and the environment. This perception can be manipulated through misinformation. It is precisely here that the specialists of Active Measures come in, aimed at manipulating the behavior of an individual, a group, a nation, with the tools of cybernetic disinformation and computational propaganda. In this paper we will try to describe how cyberattacks, disinformation, propaganda and misinformation proceed together presenting a case wich illustrates the modus operandi of a group of hackers dedicated to disinformation and propaganda in the Russian-Ukrainian conflict: the NoName(057)16 collective.

Keywords

information, disinformation, misinformation, propaganda, manipulation of perceptions, cognitive warfare

1. Premise. What is disinformation, is it different from propaganda?

Disinformation is a multifaceted word. Some observers trace it back to the Russian word dezinformatzija, which the Soviets defined in the 1950s as the "spread (in the press, on the radio, etc.) of false news intended to mislead public opinion" (Jackson, 2017).

ITASEC 2024: The Italian Conference on CyberSecurity, April 8–12, 2024, Salerno (Italy)

arturo.dicorinto@gmail.com (A. Di Corinto)

According to modern vocabularies, the origin of the Russian term "dezinformatzija" (дезинформация) refers more exactly to a Russian tactical weapon dating back to 1923, when the vice president of the State Political Directorate (GPU) wanted the creation of "a special office of disinformation to conduct tactical intelligence operations".

In both cases, it is much more recent than the word "propaganda", which originated in 1600 from the name attributed to the pontifical Congregation De propaganda Fide, charged with "propagating" the Catholic faith. Since then, albeit with different nuances, it has connoted the selective use of information for political and social purposes.

In 1928 Edward Bernays in his essay Propaganda (1928) wrote:

“The conscious, intelligent manipulation of the opinions and organized habits of the masses plays an important role in democratic society. Those who manipulate this imperceptible social mechanism form an invisible government that truly runs the country."

Whether, when, and to what extent these concepts overlap is a matter of debate. Some define propaganda as the use of non-rational arguments to promote or undermine a political ideal and use disinformation as an alternative name. Others consider them entirely separate concepts. “Disinformation more precisely describes politically motivated messages, explicitly designed to generate cynicism, uncertainty, apathy, distrust, and paranoia in the public, all of which disincentivize citizen engagement and mobilization for social or political change” (Jackson, ibid).

“Misinformation”, on the other hand, generally refers to the involuntary sharing of false information. Bad information should not be confused with disinformation. Bad information, misinformation, is the work of information professionals, by mistake or to support the political-editorial line of their publishers, while disinformation is almost always the result of perception manipulation campaigns organized at a central level by specialized and occult structures.

Some would consider a third term, “malinformation”, information that is based on reality, used to inflict harm on a person, organization or country, to encompass leaks, harassment and hate speech (Council of Europe, 2017).

The role of disinformation in the recent 2016 US election has given rise to another distinct, but related term: “fake news.” Let's say straight away that satire is not fake news, criticism is not fake news, opinions are not fake news. Although there is no universal definition, fake news generally refers to misleading content on the Internet, particularly on social media. Some analyses identify five types of fake news, including intentionally misleading content, jokes and jokes taken at face value, large-scale hoaxes, distorted reporting of facts, and cover stories where the truth may be uncertain or controversial (Jackson, 2017). Fake news is often a tool for disinformation.

On January 1, 2022, Sweden launched the only independent government authority in the world to protect its citizens from disinformation (Di Corinto, 2022). Headquartered in Karlstad,

directed by Magnus Hjort, it is called the Agency for Psychological Défense, and it is an intelligence agency that has the objective of "safeguarding an open and democratic society, the free formation of public opinion, freedom and Swedish independence". And it does so using all known tools to identify, analyze and prevent disinformation aimed at unduly influencing citizens' perceptions, behaviours, and decision-making.

Organized disinformation and bad information from journalists sometimes proceed together, and it is no coincidence that Rolf Wagenbreth, under-chief of the Stasi, already in the 1960s said about newspapers: "The common man is increasingly defenceless in the face of these monstrous opinion factories. And that's where we fit in as an intelligence agency" (Rid 2021/2022).

The debate that has developed in recent years around the theses of Valerij Gerasimov, the general of the Russian Army who in 2013 theorized the overthrow of the soft power exercised by the Americans on the global imagination through cinema and social networks, using instead Facebook, Instagram and Twitter as weapons of "mass persuasion", represents the concept in a plastic way. The internet is a perfect tool for disinformation operations: difficult to attribute, easy to deny and very cheap.

However, in the transition from an analogue society, based on hot media, to a digital and hyper-connected society, based on media convergence (Bolter & Grusin, 2000), disinformation has become a cybernetic problem. Its actors use digital artifacts to attack the certainties of their targets with an army of trolls[1], bots[2], and influencers, who make extensive use of memes[3], clickbait news[4] and narratives artfully created by digital guerrilla groups who also use software hacking to manipulate information and its protagonists, including audio and video deep fakes and computational propaganda (Wooley & Howard, 2017) that travel on instant messaging channels such as WhatsApp and Telegram or within forums such as Reddit, Discord, and 4chan.

Perception manipulation campaigns that use fake news to sow doubt and discontent among the population are widely distributed through the main Western world social networks, such as Facebook, X, Instagram, environments engineered to encourage people's involvement and the polarization of opinions so that they remain as long as possible on their platforms, increasing their value for advertisers: the more time you spend online, the greater the likelihood of being exposed to targeted information and commercial products. This is where misinformation fits into Big Tech's business model.

However, hoaxes, disinformation and propaganda are nothing new in history.

[1] Trolls are individuals who disturb the conversations we have on social media with provocative interventions. They can be automated as bots that constantly repeat the same messages.
[2] Bots are software programmed to replace human intervention and carry out collection, analysis and cataloging tasks. Bots capable of having conversations are called chatbots.
[3] Memes, minimal units of information that self-propagate because of their simplicity. These are often effective images and slogans, easy to understand and memorize. They are a tool of disinformation.
[4] Clickbait indicates web content whose main function is to attract as many internet users as possible, to generate online advertising revenue, using captivating and sensationalist titles that incite the user to click, leveraging the emotional aspect of those who access them.

2.Hoaxes in History

Pausanias, the heroic Greek leader of the Battle of Plataea, was victim of fake news. Accused of being in cahoots with the enemy, the Persian king Xerxes, based on false correspondence, was forced to flee and, walled up alive in the temple of Athena, died in there of hunger and thirst. The Donation of Constantine is an apocryphal document in which the then emperor made concessions to the Catholic Church, but it was a forgery used to legitimize the birth of the temporal power of the pontiffs. The most famous work of disinformation created by the Ochrana, the secret police of tsarist Russia, goes by the name of the "Protocols of the Elders of Zion", a text that denounces a non-existent global Jewish conspiracy. Published in instalments in a St. Petersburg newspaper in 1903, it never lost its nefarious influence (Schäfer, 2022).

The invasion of Iraq in 2003 was also the result of a hoax and makes us understand how propaganda, disinformation and bad information can proceed together.

On September 24, 2002, the British government made public a 50-page folder which testified to how Iraq had tried to purchase "significant quantities of uranium from an African country", fearing the use of the radioactive mineral for the construction of nuclear weapons. Two days later, Secretary of State Colin Powell delivered a heartfelt speech to the Senate Foreign Relations Committee, citing in turn "Iraq's attempt to obtain uranium as evidence of its persistent nuclear ambitions." On January 28, 2003, G. W. Bush addressed Congress thus: "The British government has learned that Saddam has recently attempted to acquire significant quantities of uranium from Africa..." On March the 20th, the US will decide on the invasion of the country which will end with the arrest and death by hanging of Iraqi President Saddam Hussein in 2006.

“But on which basis and on what evidence did the American president and the British prime minister push the accelerator of war: unequivocal satellite photographs? Certified reports from UN commissioners? Cross-referenced testimonies from eye-observers? No: the western front's ace in the hole was a dossier of mysterious provenance, passed into the hands of the Italian secret services and subsequently passed on to the English and American 007s. A few confusing papers, some of which were encrypted, which were supposed to prove the purchase of a large quantity of uranium by Iraq, supplied by the African state of Niger. It's a shame that the dates of the documents were compromised, the references were wrong, the data were completely unlikely" (Molino & Porro, 2003).

On March 2, 2003, before the invasion, the US Secretary of State, Colin Powell, in a speech to the United Nations had literally waved a vial of white powder, presented as anthrax, in front of those present to denounce Iraq's ability to produce weapons of mass destruction. It was later learned that the vial contained talcum powder.

Other examples reach up to the present day with the creation of fake nazi groups by the Soviets, the origins of AIDS and the infodemic related to Covid-19 (Digital Forensic Research Lab, 2021). These examples show how disinformation and propaganda are always an attempt to

manipulate consciences with false, dishonest, and deceptive information. And even today what distinguishes them is the intention to mislead those who receive them.

3. Active Measures, Disinformation and hacker interferences

Active measures is a jargon used by the intelligence community to indicate all practices of manipulating a context or behavior, and at the heart of these practices, lies disinformation. Disinformation concerns all information manipulation activities organized at a central and bureaucratic level to pollute the news by mixing truth with falsehood and producing cracks within a social body, sowing fear, uncertainty, and doubt.

The political scientist Thomas Rid in his book Active Measures. Secret history of disinformation (2021) distinguishes four historical phases of their use. A first, between the two wars coinciding with the Great Depression in which the Americans used the term political warfare, the second, during the Cold War in which the concept of dezinformatzija was established in the Soviet bloc, and subsequently that of Active Measures at the time of the fall of the Berlin Wall. The last phase is the current one in which the Active Measures are based on *hack and leak.*

Whatever they are called, Active Measures have been a central element for a hundred years in conflicts that are not fought only with missiles, drones, and tanks. They represent the continuation of war with other means, when war with military means fails to achieve the assigned objectives, and often comes alongside it and prepares for it.

Russia's annexation of Crimea, the first event of the Russian-Ukrainian war that began in 2014, is an exemplary story of how active measures helped to set the context for the invasion of the peninsula, with the creation of propagandistic media outlets (Germani et. Al, 2022; Ottaviani, 2022), the publication of false emails, leaked documents, revelation of political scandals claimed by Anonymous Ukraine but artfully created by the Russian secret services, GRU Unit 74455, and believed to be true by many activists (Rid, 2021/2022, cit.). Russian nation state hackers subsequently attacked Ukraine's railways, electricity grid, and industrial facilities with cyber weapons from 2014 to the present (CISA, 2021; Greenberg, 2019; NSC, 2017).

The logic, in short, is this: you decide to launch a military operation, you find an appropriate pretext, even a humanitarian one, and then you act militarily for a change of regime. A logic which, as Marta Federica Ottaviani explains in the book Brigate Russe. La guerra occulta del Cremlino tra troll e hacker (2022), will evolve in the infowar theorized in the so-called "Gerasimov Doctrine" to overcome the concepts of hybrid, gray and asymmetric warfare.

This thesis explains quite well the precursors of the invasion of the Ukrainian Donbass by Russia in February 2022, given that in this case the declared "special military operation" desired by Russian President Vladimir Putin would have been launched by the Russian

Federation to "denazify" the Donbass peninsula and protect the pro-Russians of those territories (Germani et al., 2022).

Whether we are talking about active measures or infowar, the central element of disinformation today is represented by the use of cyber tools to win the cognitive war online, a war affecting human cognition without inflicting prior physical force or coercion. The soldiers of this war are peculiar cyberwarriors: hackers, bots and trolls, which the Russians, and not only them, have made extensive use of in recent years.

According to Rid, the digital revolution has profoundly altered the foundations of disinformation and the very logic of active measures.

The Internet culture of *hack and leak*, *steal and publish*, has created the perfect cover for disinformation behind the defense of freedom of expression, the cult of whistleblowers, the replacement of journalism with digital activism, making active measures more dangerous. Hacking today allows you to implement active measures remotely, not to use physical violence and to deny it without problems: "Internet culture seems made specifically for mass disinformation", claims professor Rid (2021/2022). The most popular way to carry out active measures in the Western world is to manipulate the media into denying cyberwar.

“What would active measures be without journalists? Their job is made of revelations”, claimed Wagenbreth (Rid, cit., pp 196)

3.1. Attack on the mind

Rid's analysis helps us reiterate that military and intelligence agencies around the world have long been waging covert information wars in cyberspace. The memes of their psy-ops, disinformation operations, profoundly influence public perceptions of truth, power, and legitimacy (Di Corinto, 2018).

Former President Donald Trump's campaign and the role of Cambridge Analytica came under scrutiny for microtargeting (Lorenz-Spreen et. al., 2021), dark advertising and fake news, but it wasn't just the US presidential elections of 2016 to be characterized by a mix of fake news, foreign interference, cyber-attacks and social propaganda online (Wilie, 2019), but also those of 2020 and, according to Microsoft, those of 2024 will also be so, albeit with different schemes (Smith & Hutson, 2023).

A study by the University of Oxford found social media manipulation campaigns in at least 28 countries since 2010. The study also highlighted that “authoritarian regimes are neither alone nor best at organized manipulation of social media.” Already in 2014, the World Economic Forum (WEF) defined the spread of online disinformation as a significant trend to keep under observation. In the last Global Risk Report 2024 (World Economic Forum, 2024), the WEF itself ranks the disinformation as the first global threat for the years to come.

This threat is intensifying as artificial intelligence tools, such as ChatGPT, become

more widely available. AI researchers have demonstrated that they can create technologies that can produce undetectable fake audio and video, and numerous studies suggest it is easy to create high-quality digital deceptions whose authenticity cannot easily be verified. They call them Deep fake videos, and they are deeply fake videos, that is, never filmed by anyone. With technologies based on artificial intelligence it is in fact possible to put words into the mouth of a head of state that he has never uttered and trigger an international crisis once the message becomes public knowledge. In many cases, to achieve this, a skilful use of social media such as YouTube and social networks such as Facebook first, and local media later, which are not able to verify the authenticity of sources and protagonists, is sufficient.

"States, nations, activists, hacker groups and cyber criminals will use deepfakes to spread misinformation on a large scale, leaving victims unable to tell the difference reality from fiction, truth from lies" (Arruzzoli, 2022, pp21).

Research by the State University of Milan published in the journal Plos One on behalf of Marco Cremonini, Nahid Maleki-Jirsarae and Samira Maghool (2019), confirms that fake news cannot be beaten for the simple reason that people use fake news to gain an advantage. The proof comes from the use of new software for the simulation of propagation phenomena in social networks, which has demonstrated how fake news and online hatred spread with much more complex mechanisms than those that determine the contagion of real viruses because their propagation also depends on other human factors such as the desire to imitate one's peers and to spread a certain idea.

Computational propaganda exploits social media and the credulity of those who live there, exploits human psychology that does not distinguish reality from fiction, the rumors and gossip so dear to conspirators and algorithms to manipulate public opinion. This is why today we talk about cyber propaganda and cognitive warfare when we talk about disinformation.

The future of war is not on the battlefield, but on our screens and in our minds.

3.2. Disinformation, the russian school

"Some of Russia's activities that take place on or through social media are not pure disinformation efforts; rather, they are disinformation efforts functionally linked to a cyberattack of some kind. Thus, although we largely stay away from technical discussion of cyberattacks, we do touch on cyberoperations when these are closely tied to activities that use information to shape perceptions or behavior—for example, hacks that produce information that is subsequently leaked". (Treyger et. al. 2022)

In Russian terms, information confrontation (information conflict) integrates two aspects: the technical-informational one, which aims to influence "the technical systems that receive, collect, process and transmit information", and the informational-psychological one, which aims to attack "armed forces personnel and the population" (Treyger, ibidem).

As Mauro Calise (2019) points out: "But the real novelty of conflict 2.0 is its

penetration at a mass level, with propaganda or psychological campaign initiatives aimed at influencing how much citizens know about themselves and others. In this case, digital attacks are not intended for military or infrastructure targets. Instead, we are in the presence of actions aimed at influencing the political climate in another country, or at jeopardizing crucial procedures such as elections. A threat that worries Western democracies, because it goes to the very heart of their operating system: the autonomy of public opinion. And it is played on platforms that connect hundreds of millions of citizens."

There are numerous documented interference actions by Russian hackers in the democratic processes and social life of Western countries. Since the beginning of the war in Ukraine this interference has multiplied, but we have already had numerous examples of it before:

In 2008, in Georgia, a series of cyber-attack to shut down the Georgian sites was accompanied by a real military campaign. On the night of August 6, hackers attack Georgian government and news sites. SQL injection attacks to deface Georgian media occur simultaneously with DDoS conducted with botnets affiliated with pro-Russian groups. The actual military invasion begins on August 7 (Shakarian, 2011). Russian officials will claim the attacks as a reaction, with no proofs, to the hacking of sites in South Ossetia, a country with a strong Russian-speaking component.

In 2013, the Internet Research Agency, the Russian "Troll Factory", was officially born. Financed by Evgenij Viktorovič Prigožin, Russian entrepreneur, politician and mercenary commander, friend of russian President Vladimir Putin, the structure has the task of developing propaganda content in favour of the Moscow government. Its employees create web content, digital pranks, fake news, and translations of government articles to support Russia in its claim to the Crimean Peninsula, later annexed by the Russian Federation. These trolls will subsequently be used to pollute the public debate around the 2016 American elections by creating fake online supporters for Trump and spreading hoaxes and gossip to distance African-American voters from voting in swing states which could have benefited the Democratic candidate Hillary Clinton (Rid, 2021, Curioni & Giannuli, 2022, Feltri, 2023)

In 2014 the GRU, the Russian Military Secret Service, created a fake Anonymous video to support the invasion of Ukraine, having previously managed to sneak into the email address of a Ukrainian colonel to insert fake emails relating to a conspiracy between Ukraine and the United States to damage Russia (Rid, ibidem, pages 349-357).

In 2015, 2016, 2017, Russian actors attack Ukraine's electricity infrastructure.

In 2015, the attack on the website of the French TV TV5Monde and its social accounts caused the interruption of broadcasts for several hours. Initially claimed by the Cyber Caliphate, the cyber unit of ISIS, the Middle Eastern terrorist group to which it is initially attributed, according to the French ANSSI it is the work of the APT28 group connected to the Russian secret services who demonstrate with this attack that they know how to exploit moments of social crisis and to act in a way that destabilizes a social-political context.

In 2016, the Russiagate broke out, following the unauthorized intrusion of the Democratic Party's Election Committee servers by a self-styled lone hacker, Guccifer 2.0, who turned out to be a cover name for hackers from the Russian secret services. The objective of the unauthorized disclosure of the exfiltrated materials is to weaken the position of Hillary Clinton in the race for the White House against Donald Trump, but there will also be attempts at interference in the French, German and Italian elections during the government of Matteo Renzi (F. Nicodemo, Disinformatia, 2017).

In 2017, it's the time of Not Petya. An assessment by the UK National Cyber Security Center (NCSC) finds that the Russian military is almost certainly responsible for the "Not Petya" cyber-attack of June 2017 (National Cyber Security Center, 2018). Not Petya works similarly to its predecessor Petya, belonging to a family of malware that infects Windows systems and whose goal is to target Ukrainian energy companies and government institutions (Thales, 2022).

The Petya ransomware, discovered in 2016, run on computers, encrypting certain files, locking the boot sector of the compromised system, and demanding a ransom in exchange for restoring these files. The Not Petya variant from 2017, instead, mainly concerned the commercial sector. One aspect that made it particularly notorious is the fact that often, even when the ransom was paid, the victim's files were not recovered (Germani et. al, 2022). Also, for this reason, researchers suspect that it worked to hide a cyber-attack that targeted Ukrainian institutions.

Not Petya is a different version of Wannacry, the malware used to block the English healthcare system, the Maersk company, and some Caucasian railways. Built on the basis of software vulnerabilities stolen by the mysterious Shadow Brokers from the section of the National Security Agency called Tailored Access Operation, the Wannacry malware/ransomware will infect approximately 300 thousand computers in 174 countries causing billions of dollars in damage (Thales, 2022; Rid, 2021).

In 2018 in Lithuania, Russian hackers hacked the website of one of the major national television stations by inserting an article in which the Minister of Défense declared that he was gay and was being investigated for sexual harassment.

In 2019 the infection chain of the Solarwinds supply chain started (Di Corinto, 2021). A group attributable to the Russian foreign secret services SVR (Microsoft 2021; Mandiant, 2022), penetrates the supply chain of the well-known Texan technology producer and arrives at the gates of US nuclear assets (Smith & Brown, 2019). Cybersecurity experts would later give the cyber-attack a variety of names, including Solorigate and Sunburst, referring to the Texas company SolarWinds whose software had been manipulated to organize the initial attacks by installing a small malware in the update code of a network management program called Orion. In this way, when customers installed the update on their local servers, malware connected to command-and-control servers was also installed, which allowed them to intervene on the ability to transfer files, execute commands, profile the system, reboot a machine and disable it services.

In short, the attackers had obtained a backdoor into the network of every customer who had updated the Orion program, around thirty-eight thousand clients worldwide. Russia, however, denied any involvement in the operation, stating it "does not conduct offensive operations in the cyber domain (Russian Embassy in the USA, 2020).

Finally, in 2022, the invasion of Ukrainian Donbass is accompanied by a series of cyber-attacks. These include DDoS attacks, website defacing, and distribution of wiper viruses that erase the memory registers of Windows computers. However, the first to fall is the Ka-Sat communication system, part of Via-Sat. Cyber operations that all raise intricate challenges regarding rules of engagement, attribution and response, and thus perfect to pollute the public debate, the decision making process and its possible outcomes (Baldoni, 2024).

These events follow seventy web defacements documented against Ukraine a few weeks earlier. In the meantime, the Digital Forensic Research Lab of the Atlantic Council had already reported a series of false narratives (DFRLab, 2022), distributed on social media, and propagated by pro-Kremlin newspapers and television stations: all with the same aim, to minimize the effects of the conflict on the civilian population and present Putin as a wise head of government (Di Corinto 2022). The Five Eyes, the spy alliance of the former commonwealth countries, issue an alarming alert (Di Corinto, 2022).

Subsequently, the case of the Conti ransomware gang broke out and, just three days after the invasion, on 27 February 2022, openly declared itself in support of Russia. (DI Corinto, 2022)

However, the influence and interference operations practiced are usually denied by the Russians, and, moreover, are not always attributable to orders given by Moscow, but this is precisely the essence of the hybrid war theorized by its own generals.

As Mark Galeotti states: “To fight its political war, Russia has created a machine that is undoubtedly flexible, economical, imaginative, and enterprising, but also difficult to control. The idea that all the trolls, propagandists, militias, bribers, hackers, and other soldiers of this army are always under the strict control of the government is wrong. Of course, there are operations that are managed centrally from the start and those of particular importance that clearly require the imprimatur of the Kremlin. This includes the assassination of Sergei Skripal in England in 2018 and the interference in the 2016 American presidential elections. In most cases, however, Moscow has encouraged many "political entrepreneurs" to take the initiative, often at their own pace and at their expense. If they fail, they can be disavowed; if they succeed, they can be rewarded and at that point the State can take over, expanding or developing the operation” (Galeotti, 2017).

As a demonstration of the relationship between hacking and the spread of false news, the Ukrainian secret services arrested a group of cybercriminals specialized in selling accounts to spread disinformation. The Ukrainian authorities, while not revealing the names of those arrested, provided evidence of the activity of a group of hackers operating in Lviv in possession of approximately thirty million accounts belonging to Ukrainian and European citizens sold on

the DarkWeb. The searches carried out in the homes of the suspects led to the seizure of hard drives containing personal data, mobile phones, SIM cards and flash memories used for the purpose.

According to investigators' estimates, the pro-Russian group earned around 400 thousand dollars by selling them wholesale through electronic payment systems such as Qiwi and WebMoney. In the press release, the Security Service of Ukraine (SSU) claims that the clients are pro-Kremlin propagandists: «It was they who used the identification data of Ukrainian and foreign citizens stolen by hackers to spread false news from the front and sow panic».

Authorities had previously shut down two 7,000-account bot farms for spreading disinformation and creating panic in the region. An activity linked to a phase of the Russian-Ukrainian war in which citizens of some areas, especially in occupied Donbass, receive neither food nor information. But the relationship between cybercrime, hacktivism and state hacking is even more direct (Di Corinto, 2022).

According to Google-Mandiant (Mandiant, 2023), when Russian government hackers attack, they pass the stolen data to hacktivists within 24 hours of the break-in so they can carry out new attacks and spread pro-russian propaganda. Four non-governmental groups would act in this way: XakNat Team, Infoccentr, CyberArmyofRussia_Reborn and Killnet.

However, while XakNet would coordinate with Russian intelligence, Killnet, with which it collaborates, if paid, would be ready to attack anyone. The collective, which also targeted Italy, at a certain point began to cloak its actions with patriotism, becoming a celebrity thanks to its appearances on Russian television. Mandiant believes that it was Russian hacktivists who targeted US companies such as Lockheed Martin with a series of attacks. State hackers named Sandworm, known for the Industroyer virus, then impersonated Ukrainian telecom operators Datagroup and EuroTransTelecom in their attacks.

3.3. NONAME(057)16: WHEN DISINFORMATION PRODUCES REAL EFFECTS

NoName(057)16 is a group of self-styled hacker activists who appeared on the communication scene at the dawn of the Russian-Ukrainian conflict in March 2022, claiming numerous cyber-attacks against various European and NATO countries targets.

In his manifesto he declares his intent to protect the Russian population and to respond to the attacks of "Ukropropaganda", as they define Ukrainian propaganda. To do this, the group mainly uses its same name Telegram channel with the aim of organizing DDoS campaigns, making fun of the opponents, and instructing volunteers who want to participate in the actions. They also developed an ad hoc platform, DDoSia, to launch DDoS attacks through synchronized botnets. DDosia Project is also the project's namesake group/channel created on March 18, 2022 to conduct DDoS attacks against specific targets. The tool is offered upon

registration via a bot that records the user's nickname and includes a feature that allows the user to track attacks conducted with this tool.

The group appears to collaborate with several other groups of self-declared Russian patriots such as Killnet and XakNet (YarixLab, 2022), the latter considered linked to the Russian foreign secret services (SVR).

Italy is among the numerous countries attacked by the group of activists. The DDoS attacks claimed by the group against national entities, of a volumetric, application and infrastructural nature, have slowed down and in some cases blocked the target websites of Italian ministries, public transport companies, airports, and banks. The attacks always occurred in coincidence with war events and followed the declarations in which the Italian Government expressed its support for Ukraine attacked by the Russian Federation. Their targets included the Baltic countries, Canada, Poland, Spain, France, and England, and other European nations supporting Ukraine.

NoName057(16) advertises its campaigns in a Russian-speaking channel and in a mirror channel where content is translated into English for non-Russian-speaking members. The group has also created other channels in which some of its members discuss technical aspects related to DDoS campaigns.

DDoSia users call themselves the “cyber army” and work together to support efforts and provide more resources to achieve the collective's goals. In the group's various Telegram channels you can read the alleged results of each attack by this cyber army which the channel managers use for propaganda and internal cohesion purposes, given that their effects were often limited in time and consequences, as stated by the Italian National Cybersecurity Agency, ACN, which provided the affected targets with operational indications to mitigate these attacks.

Characteristic of the individuals connected to the NoName(057)16 collective is that they are often passive spectators who do not participate in the discussions and use emojis to show appreciation of the threads generated in the channel; others appear to be technically well-versed individuals who share political motivations in attacking "Banderist Ukraine", named after the Ukrainian nationalist Stephan Bandera, and against countries they consider "Russo phobic".

Regardless of the success of the DDoS attack, a few hours after its start, the channels are populated with victory messages, and soon, from the following day, they present the journalistic coverage obtained in the various countries whose government bodies and infrastructures have been attacked.

As previously happened with the incursions of Killnet, a noisy threat actor in the galaxy of support for the Ukrainian invasion of Russia which began on February 24, 2022, NoName(057)16's Telegram channel remains the place to recruit people, aggregate consensus and communicate with the media ecosystem in a broad-spectrum work of disinformation where what matters is not just the claim of the effects of the results of the actions, which are often

limited, but the narrative that can be told to transform cyber-attacks into an instrument of proselytism, propaganda and internal cohesion.

The tactic used to achieve these objectives is always to "photograph" with a screenshot the results of the temporary interruption recorded by dedicated platforms such as check-host.net, publish the screenshot on the channel, wait for the media reaction, which - thanks to poor journalism informed and sensationalist -, will exaggerate the effects of the attack, a clamor advertised as "certification" of the effectiveness of the incursions.

The cases of attacks aimed at Italy were exemplary in this sense.

Throughout the period of the conflict, with one of the peaks reached in Italy around 5 February 2023, the disinformation tactic implemented by NoName (057)16 received unexpected help from the resignation of the Director General of Italy's National Cybersecurity Agency, professor Roberto Baldoni. The director of the Agency in fact offered his resignation to the Italian Government on which the Agency depends, on 6 March 2023, right at the turn of one of the group's now usual DDoS attacks. The resignation, according to a cause reported by some newspapers, was due precisely to the recognition of the ineffectiveness of the enforcement actions implemented by the director of the Agency against the hacktivists. Other newspapers, however, reconstructed the reason for the esteemed director's resignation in a different way, without linking it to the pro-Russian attacks (Zorloni, 2023).

However, the group used this opportunity to claim, through all the means at its disposal, the merit of Baldoni's "expulsion" as a specific result and as the demonstration of the "unstoppable" nature of its disruptive action, writing on Telegram: «Our series of attacks on the Italian internet infrastructure can rightly be considered successful: following this, the head of the Italian National Agency for IT Security was removed from his position. Let's see - continued the ironic message - how the new head of this Italian office will deal with the cyber threats coming from the NoName057(16) team" (Fiammeri, 2023). After that NoName(057)16 continued DDoS attacking Italy, but the new head of the Italian Agency is still in office (Fig.1)

Figure 1: Noname057(16) meme represents their supposed role in Baldoni's resignation for the unsuccessful attempts of ACN to stop the DDoS attacks, via Noname057(16) main Telegram channel.

Whatever the actual reason for the resignation of the director of the Italian cybersecurity agency, the affair represents a textbook example of how Active Measures can be exploited: it is not the result that counts, but the ability to create doubt and bewilderment in the recipients of

the disinformation operation coupled with the use of cyber-attack techniques. As Thomas Rid states, when talking of Active measures, it is counterproductive to distinguish facts from non-facts: "What made the active measures active was not the correlation with reality, but with emotions, with the values shared by a community, and the ability to exacerbate existing tensions: in the jargon of Cold War actors, to reinforce contradictions."

4.CONCLUSIONS

Every war is a hybrid war. The actors of a war have always used all the tools at their disposal to prevail over the adversary, from conventional weapons to terrorism, from economic interference to hacker warfare up to cognitive warfare, i.e. techniques for manipulating perceptions, based on propaganda and disinformation (Borgia, 2022).

With the advent of the Internet, all subjects, civil and military, individual and organized, can participate in an open, conscious and mercenary manner in conflicts using both non-military means and military techniques and tools. War is no longer just the business of military commands and the Russian-Ukrainian conflict – in which both citizens, telecommunications companies and digital platforms take part – makes this clear. However, it remains to be assessed what contribution disinformation offers to hybrid warfare. The core challenge being the description of hybrid warfare social effects which lie in synchronising capabilities and operations, including perception manipulation campaigns. To understand this, it appears important to evaluate the effects of disinformation on a case-by-case approach, trying to reconstruct the purposes of its own actors each time, although recurring patterns may appear.

References

[1] F. Arruzzoli, Deepfake & Cyber Intelligence. Tecniche di creazione, rilevamento e prevenzione, 2022, URL: https://www.ictsecuritymagazine.com/pubblicazioni/deepfake-cyber-intelligence/

[2] R. Baldoni, Charting digital sovereignity. A survival playbook, Amazon, 2024

[3] E. L., Bernays, Propaganda. L'arte di manipolare l'opinione pubblica, a cura di Raffaele Scelsi, Milano, Shake Edizioni 2020; or. ed. *Propaganda,* Horace Liveright, New York, *1928.*

[4] F. Bigazzi, D. Fertilio, S. Germani, Bugie di guerra. La disinformazione russa dall'Unione sovietica all'Ucraina, Roma, Paesi Edizioni, 2022.

[5] J. D. Bolter, R. Grusin, Remediation: Understanding New Media, Mit Press, 2000.

[6] F. Borgia, in M. Bressan, G. Cuzzelli, a cura di: Da Clausewitz a Putin: la guerra nel XXI secolo. Riflessioni sui conflitti nel mondo contemporaneo, Ledizioni, 2022.

[7] R. R. Brooks, I. Oxcelik, J. Oakley, & N. Tusing, . Distributed Denial of Service (DDoS): A History, IEEE, 2021
[8] Digital Forensic Research Lab, Weaponized: How rumors about COVID-19's origins led to a narrative arms race, 2021. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/weaponized-covid-19
[9] M. Calise, F. Musella. Il Principe digitale, Bari, Laterza, 2019
[10] A. Curioni, A. Giannuli, Cyberwar. La guerra prossima ventura, Milano – Udine, Mimesis edizioni, 2019.
[11] A. Di Corinto, In Svezia la prima agenzia per la difesa psicologica contro la disinformazione, 2022. URL https://www.repubblica.it/tecnologia/2022/01/24/news/in_svezia_la_prima_agenzia_per_la_difesa_psicologica_contro_la_disinformazione-333428197/
[12] A. Di Corinto, Le guerre del futuro si combatteranno nei nostri cuori, 2018. URL: https://ilmanifesto.it/le-guerre-del-futuro-si-combatteranno-nei-nostri-cuori
[13] A. Di Corinto, Perché l'attacco a SolarWinds è stato così devastante, 2021. URL: https://www.italian.tech/2021/09/18/news/perche_l_attacco_a_solarwinds_e_stato_cosi_devastante_-318027621/
[14] A. Di Corinto, La guerra in Ucraina è anche sul web: allarme per un virus che cancella la memoria dei computer, 2022. URL: https://www.repubblica.it/tecnologia/2022/02/24/news/ucraina_sotto_attacco_cibernetico_allarme_per_un_virus_che_cancella_la_memoria_dei_computer_killdisk-339103442/
[15] A. Di Corinto, Gli alleati dell'Ucraina sono a rischio cyberwar, avvertono i Five Eyes, 2022. URL: https://www.repubblica.it/tecnologia/2022/04/22/news/i_five_eyes_avvertono_rischio_cyberwar_per_gli_alleati_dellucraina-346435822/
[16] A. Di Corinto, Hacking e disinformazione, la scuola russa, 2022. URL:, https://ilmanifesto.it/hacking-e-disinformazione-la-scuola-russa
[17] Digital Forensic Research Lab, How ten false flag narratives were promoted by pro-Kremlin media, 2022. URL: https://medium.com/dfrlab/how-ten-false-flag-narratives-were-promoted-by-pro-kremlin-media-c67e786c6085
[18] B. Fiammeri, (2023). Cybersecurity, cosa succede dopo le dimissioni di Baldoni? Oggi Mantovano al Copasir, 2023. URL: https://www.ilsole24ore.com/art/cybersecurity-cosa-succede-le-dimissioni-baldoni-pole-prefetto-frattasi-AEFIggzC
[19] S. Feltri, Il Partito degli influencer. Perché il potere dei social network è una sfida alla democrazia, Torino, Giulio Einaudi Editore, 2022.
[20] A. Greenberg, Sandworm. A new era of cyberwar and the hunt for Kremlin's most dangerous hackers, New York, DoubleDay, 2019.
[21] D. Jackson, Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and "Fake News", 2017. URL: https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/
[22] Lorenz-Spreen, Philipp; Geers, Michael; Pachur, Thorsten; Hertwig, Ralph; Lewandowsky, Stephan; Herzog, Stefan M. (30 July 2021). "Boosting people's ability to detect microtargeted advertising". Scientific Reports. 11 (1): 15541. doi:10.1038/s41598-021-94796-z. PMC 8324838. PMID 34330948.

[23] Mandiant, Hacktivists Collaborate with GRU-sponsored APT28, 2022, updated aug. 2023. URL: https://www.mandiant.com/resources/blog/gru-rise-telegram-minions
[24] S. Maghool, Maleki-Jirsaraei, Nahid, Cremonini, M. (2019). The coevolution of contagion and behavior with increasing and decreasing awareness, PlosOne, 2019, https://pubmed.ncbi.nlm.nih.gov/31794564/
[25] W. Molino, S. Porro,. Disinformation Technology. Come si manipola l'informazione per divertirsi, fare soldi e magari provocare una guerra, Milano, Apogeo Editore, 2003.
[26] National Cyber Security Center. Russian military 'almost certainly' responsible for destructive 2017 cyber-attack, 2018. URL: https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack
[27] M. F. Ottaviani, Brigate Russe. La guerra occulta del Cremlino tra troll e hacker, Milano, Ledizioni LediPublishing, 2022
[28] T. Rid, Misure Attive. Storia segreta della disinformazione, Roma, Luiss University Press, 2022; or. ed. Active Measures: The Secret History of Disinformation and Political Warfare, Ferrar Straus & Giroux, 2021.
[29] Russian Embassy in the USA, 2020. URL: https://www.facebook.com/RusEmbUSA/posts/1488755328001519
[30] P. Schäfer,. Storia dell'Antisemitismo. Dall'antichità fino a oggi, Roma. Donzelli, 2022
[31] P. Shakarian, The 2008 Russian Cybercampaign against Georgia, Mil, Rev, vol 91, no.6, p 63, 2011
[32] B. Smith, A. C. Brown,. Tools and Weapons: The Promise and the Peril of the Digital Age, New York, Penguin Book, 2019
[33] N. Smith, T. Hutson, Microsoft announces new steps to help protect elections, 2023. URL: https://blogs.microsoft.com/on-the-issues/2023/11/07/microsoft-elections-2024-ai-voting-mtac/
[34] Thales, (2022). Cyber Threat Handbook 2022, 2022. URL: https://bo-cyberthreat.thalesgroup.com/sites/default/files/2022-11/THALES%20THREAT%20HANDBOOK%202022.pdf
[35] E. Treyger, J. Cheravitch, R. S. Cohen, Russian disinformation Effort on social media, 2022. URL: https://www.rand.org/pubs/research_reports/RR4373z2.html
[36] YarixLab, Analysis of the Russian-Speaking Threat Actor NoName 057(16), 2022. URL: https://labs.yarix.com/2022/10/analysis-of-the-russian-speaking-threat-actor-noname-05716/
[37] World Economic Forum, Global Risk Report 2024. URL: https://www.weforum.org/publications/global-risks-report-2024/ [10-01-2024]
[38] C. Wilye, Il Mercato del consenso: come ho creato e poi distrutto Cambridge Analytica, Milano, Longanesi, 2019; ed.or. *Mindf*ck: Inside Cambridge Analytica's Plot to Break the World*, London, Profile Books, 2019.
[39] S. C. Woolley, P. N. Howard, "Computational Propaganda Worldwide: Executive Summary." Samuel Woolley and Philip N. Howard, Eds. Working Paper 2017.11. Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk. 14 pp.
[40] L. Zorloni, (2023). Cosa sappiamo sulle dimissioni del direttore dell'Agenzia per la cybersicurezza nazionale, 2023. URL: https://www.wired.it/article/baldoni-agenzia-cybersicurezza-dimissioni-soldi-pnrr/