INFORMATION OPERATIONS IN THE MODERN AGE

Avante Edge Research

APR 2024

Table of Contents

Setting the Stage

For over a century, the geographic nature of the United States has prevented, or deterred, a foreign nation from invading the U.S. Homeland. Its citizens have been far removed from the horrors of warfare, safely tucked away across 6000 Km of ocean to its East and West. Rarely does a power traverse the sea or venture into its realm to attack its cities, factories, and people. This safety has disappeared with the modern nature of warfare. Cyberspace and Information operations have put you and your loved ones within the reach of adversaries across the world, whether you live in America or not. It is a war that does not get publicized to the extent of other conflicts, though many more nations and groups are involved in it than conventional conflicts currently, and its weapons penetrate a nation's thickest defensive walls and into its most remote areas.

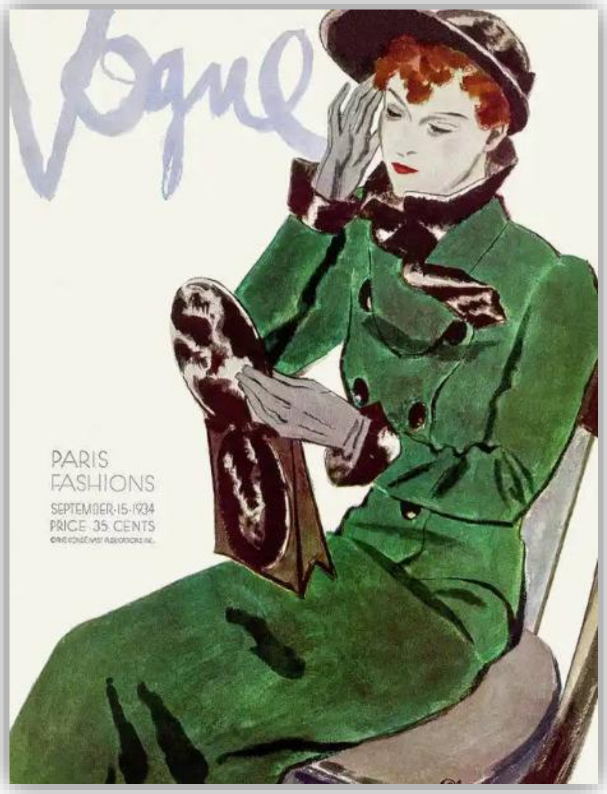
This is a war that is hard to define, it doesn't have rules of engagement, boundaries, or borders. Some nations, like the US, don't view it as "war" at all but have placed it in a category of "competition." This distinction may be detrimental in the US case as competitions grow into conflicts. The importance of information and cyberspace operations waxes and wanes in the U.S. Government, it is a hard sell to a nation that believes it can dominate any situation by physical presence or force. In China, it is known more as Political and Cyberspace warfare, these operations are generally consolidated underneath the Peoples Liberation Army (PLA) – Strategic Support Force (SSF). In Russia, it is leveraged in a concept called Hybrid Warfare. This paper will cover a breakdown of how the U.S., Russia, PRC, and other nations view these operations along with prolific events in recent history so that we may understand information operations in the modern age.

How an Influence Campaign Works

You are in the crosshairs of many individuals, well at least your thoughts, desires, interests, and usually wallet are. You the reader are the victim of information warfare on a daily basis, sometimes its from a foreign military power, and other times it's the local business. Either way, getting you to believe something is the name of their game. See – Think – Do, a simplified process of getting one to act in a way in which you want them to. A process where some entity thinks - What does my audience need to see to make them believe something in order for them to act on that belief. Let's take a look at an example from history of the power of information on the American population.

American Tobacco Company, owner of the *Lucky Strike* cigarette*,* in 1929 charged a man named Edward Bernays with the objective of opening an untapped market in America, selling cigarettes to women. How would one man change the way America views the female smoker? It was highly frowned upon and considered in severe bad taste to smoke as a woman, let alone smoke in public. Bernays studied the current politics, societal issues, news media, and more to come up with his plan. He looked at the prevailing topic of Women's suffrage and chose to use it to the company's advantage. To normalize the act, he would start by exposing the target audience to the idea by paying women to smoke. On one specific instance in 1929, he hired women to smoke in public at parades and other high-profile events during Easter weekend. Journalists were "tipped off" on the "scandalous events" taking place, within three days reports ran across the country of dozens of women smoking in public. Bernays spent tens of thousands of dollars to shape the normalcy of women smoking through actors, orators, and charity events. The tobacco industry became a powerhouse of "Feminism" almost overnight due to his actions.

Fast forward a few years and though women smoking in public had become the norm, a second problem arose for Bernays, fashion. In the early 1930s fashion had changed and women found that Lucky Strike's Green packaging became unfashionable. The American Tobacco Company would accept changing the longtime and well-known signature packaging of Lucky Strike. Bernays thought about how to solve the dilemma and eventually suggested that they change fashion instead. This is an extremely bold plan as most of you could surmise, how can one person change fashion in an entire country? He decided to create a charitable ball inviting the high society and influencers from all over to join in the "Party of the Season" as it was called Invitations to the appropriately named "Green Ball" were sent out to the elite wives, singers, actresses, and put into every newspaper. Bernays organized speeches to be given in colleges on the positive effects of the color green and arranged for Vogue's September issue cover women to sport a green dress. The night of October 25th, 1934, successfully changed fashion, Green was now in. Photos and articles spread across the nation touting the message. This is the power of influence; this is the technique that's used every day for good and evil purposes across the globe.



September 1934 Vogue Cover

The story above pertains to us because, then as it is now, the people were the target. The target wasn't the color green, it wasn't the rich, and it certainly wasn't for women's rights… it was to target the people for profit. We recognize there is a difference between sales marketing to a US audience and influencing an Iranian Fisherman to report on smuggling, but the unique tactics employed to influence someone remain. In this next section, we will discuss the basic components of information operations and what is considered success.

Tactics to Influence

Let’s define some terms using the Cybersecurity and Infrastructure Security Agency (CISA) definitions. Misinformation is false information that is shared not with the direct intention to mislead or harm. This can be somewhat truthful or taken out of context, or words and actions manipulated to alter, skew, or reveal an intention or message outside of the true intention. Disinformation is false information shared that is intended to mislead, manipulate, and harm a person, group, or nation. Similar to misinformation but executed with the forethought to alter a perception or idea. Malinformation is truthful information used to harm or manipulate a group, person, or nation. An example as such could be focusing topics against a nation or person by bringing up events or information that could or is viewed by the majority as bad (I.E. Slave Trade, Colonization, Genocide, Scandals, etc.) and using those to shape a view or remind a people of past atrocities or even simply previous lies creating distrust.

Operations are conducted in the physical, cognitive, and information realms to achieve objectives, these objectives play a role in shaping the weapon that is to be used. Tactics vary by time, necessity, and resources available. In some cases revealing a capability is one tactic, concealing is another; sometimes it's a cyber-attack or the threat of an attack; it comes in the form of weapons tests; riots; news articles; and sometimes humans. Tsarist Russia in 1917 probably did not fathom how its future had shifted when on April 16th a train with just 30 passengers arrived in St. Petersburg. One passenger being Vladimir Ilyich Ulyanov (Vladimir Lenin) whose trip was orchestrated by Germany to weaken Russia by fanning the flames of political infighting, a spark that worked far better than anticipated.

The US, Russia, and China each approach information operations differently, though they fundamentally contain the same structures in it. We introduced the idea earlier of See-Think-Do as a simplified model to understand how a potential influence operation is planned. For Russia, the US and the West generally describe their tactics under a "Three *C* Concept," Covert, Coercive, and Corrupting. Russian "Hybrid Warfare" or *gibridnaya voyna* in Russian, is designed to amplify social, political, and ideological fractures in an adversary's society to weaken their enemy from within. Russia is currently assessed as the leading nation in successful executions of influence and cyber operations across the world. This may come as a surprise if you are reading this in the US or the West, but that is because you have most likely seen the thousands upon thousands of news articles or memes slandering Russia and its ability to conduct… pretty much anything. The news articles you read are an influence operation in themselves to discredit Russia and inflict a decrease in popularity or increase support to a side opposing Russia, i.e. Ukraine. Though they are struggling conventionally in the recent conflict in Ukraine at the time of this writing, Russian influence operations towards nations and peoples all over the world are successful to the point that most never realize it was their operators who helped the idea along until after the fact.

Russia

Some of the more successful operations in recent years are the Russian influence in Africa, convincing nations to leave behind ties with the West by increasing military sales and reminding the populaces of the atrocities committed by the French. Most operations by Russia in areas such as Sahel or the Central African Republic are textbook Russian strategies that continue to work. Election interference, disinformation, campaigns, rally coups, and more. These low-cost influence operations are highly effective in Central and Southern Africa (*See Figure 1 pg. 19*), where China and now even the Islamic State are operating heavily. Other operations are in the Middle East, how they assist in shaping the narrative along with Iran in the region to their benefit taking advantage of the frustrations against the US long-term anti-terror campaigns. They were responsible for protests in Lithuania when the country wanted to remove statues of soviet soldiers, AI-generated news articles, and bot responses to posts on social media inflamed the citizenry to the point of riots. For the US, they used the strategies they honed in Africa and Europe, targeting the 2016 Elections. Many special investigators and government representatives assessed that Russia’s goal was to affect the current election. That is a near-sighted goal, as we only have a president for 4-8 years. Why waste money, time, and resources on that? What is a more substantial effect that we could produce that would have longer-lasting consequences? Not change a president for one term, but to target the US population's faith in the elections themselves, and the US fell for it hook, line, and sinker.

Russia studied the US and looked for the rifts in its society. Using the declassified Select Committee on Intelligence of the United States Senate investigation on Russian Active Measures for Campaigns and Interference, we can look at how they took these cracks in class, race, creed, and religion and exploited them through social media posts. Thousands of users controlling thousands of bots on social media to create posts all targeting different audiences. African Americans were targeted with posts and AdTech preying on the angry sentiment around inequality. Conservative voters were targeted with anti-immigration messaging and patriotic themes. Liberal voters were targeted with topics on systemic inequalities and others to incite anger toward groups against the LGBTQ community. Mexican Americans were rallied into groups inciting “Brown Power” and sharing messages to push distrust of the US political system. Muslims were shown messages denouncing terror attacks and anti-Clinton themes along with cynicism towards the US. Truly an impressive feat, once reports started flooding out after Trump was elected, the US mainstream and smaller media brands repeated how the election was fraudulent daily for four years. The media pushed it into the subconscious of everyone that elections are vulnerable, setting the stage for millions of Americans never to trust an election again if they don’t agree with the outcome.

> *This newly released data demonstrates how aggressively Russia sought to divide Americans by race, religion and ideology, and how the IRA actively worked to erode trust in our democratic institutions* - Intelligence Committee Chairman Richard Burr (R-N.C.)

Russia posts tens of millions of products a year to the US population, some estimates are reaching over 120 million individual posts and not to mention the impression and engagement rate a singular post could see. For example, during 2016, some narratives such as “Bill Clinton is a rapist” received 123.8 million impressions in under one week and another reached 177.5 million. With ~290M Social Media user in the US, that’s roughly 60% of users seeing just one of the narratives on one platform from Russia. On average it is estimated that Americans saw four organic Russian posts per day during 2016, a staggering amount of products to be created and disseminated.

Besides influence operations, Russia also has a robust hacking capability, which is most likely individuals merely paid by the Russian Federation, but they are nonetheless extremely capable. This could also be considered part of an information operation, to sow distrust in the US government's ability to successfully protect National Critical Infrastructure let alone to protect the citizens. Russia has recently infiltrated the leading agency to execute such a task, the Cybersecurity and Infrastructure Security Agency. CISA, at the time of this writing, had to take systems offline after hackers revealed themselves from inside the system for what CISA stated as an “Indeterminate amount of time.” Another wildly successful hack was the release of the entire US Intelligence Communities hacking tools to the world, some of the most powerful tools for hacking at the time. another impressive feat that was an embarrassment to many of the US agencies.

China

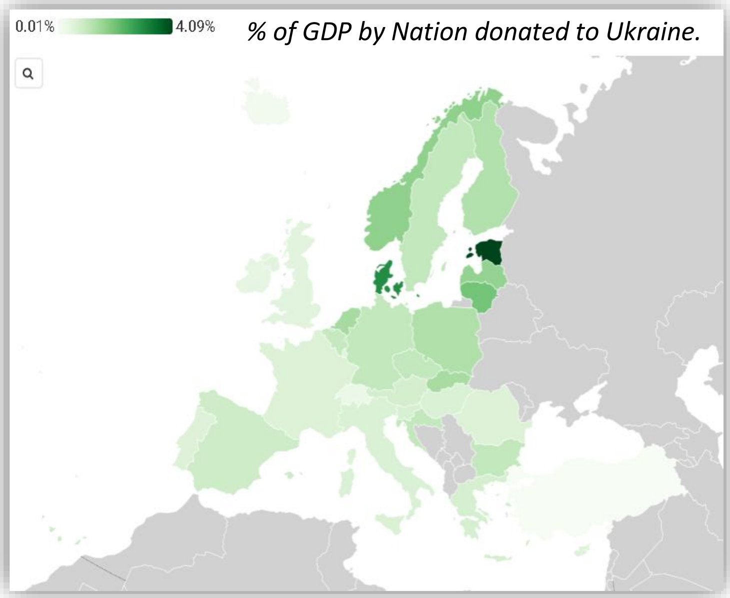
China has a bit of a different touch when it comes to its information operations and hacking. Its “Political” warfare works mainly leveraging agreements to Chinese favor once a nation has signed into a partnership. When probed or prodded by US or Western accusations, it politely denies its nefarious activity and continues firmly believing in itself. Most of China’s influence operations come from economic investments, political agreements, and its proliferation of technologies to much of the world but it has also had successful disinformation campaigns. Such as the Canadian Election interferences of 2021, one such example is of China using “Hyper-Realistic” speech software to create a fake interview between Joe Rogan and Canadian Prime Minister Justin Trudeau, the interview has the fake Trudeau stating that protesters were racists, Nazis, sexists and that he would “Nuke the Capitol” if he could have it his way. Though most of us can listen to the podcast and realize it is fake, many people have an overt trust of mainstream figures and news media brands. How many times in recent years has someone you’ve known, or yourself, fallen for a false story because it came from a source they liked? No one is immune to propaganda. Larger-scale influence operations come in the form of massive investments, such as the Belt and Road initiative, which it leverages corporate and governmental agreements to gain a political foothold and then the initiative itself, being part of the campaign, can mold a target audience for influence operations. It is a slow burn process in which it builds relationships over years through good faith without the host nation knowing their true intention. It sets up trade and industry, moves in with technology and upgrading energy grids for the nation, then starts to apply its pressure for its political and military goals like a giant economic and technological boa that can squeeze a nation as it needs. A very successful technique in many 3rd world nations around the globe. For some, the abandonment of Western alliances for China comes with known consequences, but leaders of nations need economic stimulation and investment for their people to thrive, China offers a better price point that the US or West will not match or may not even offer at all.

Though it has many long-reaching influence operations, much more of its non-tangible weaponry lies in its cyber capabilities. Like the rest of their military strategy, its cyber operations are far-sighted. There is a unique way in which China uses these tools to infiltrate and wait, gaining access and then siphoning data or information as it sits. On occasion, China will execute an attack, maybe shut down a pipeline, steal company secrets, or freeze up systems to remind the US that it is not safe just because it is on the other side of the world. Chinese cyber operations have been detected in almost every system in the US national critical infrastructure. A test was conducted in 2013 with a fake water plant, this test was set up by a researcher who simulated the operational framework of a small water purification plant, once hooked up to the internet he waited to see what would happen. Within only three days the system had been attacked numerous times and successfully hacked into by Chinese PLA Unit 61398 which is China's leading persistent threat hacking unit nicknamed "Comment Crew." This fact is deeply unsettling for the US Government and many others in the country, the PLA doesn't hide who they are in the system, rarely using applications to mask their internet protocol address which means they can be easily tracked back to China. It is a form of information operations, letting us see and know that they are there always, biding their time.

> *You can't excel at disinformation and democracy at the same time* – Dr Thomas Rid, Professor of Strategic Studies at Johns Hopkins University

United States of America

The US has a vastly different approach when it comes to information operations. The US does not view information operations or cyberspace operations as open conflict or in line with the conventional force operations that the US has consistently conducted since the 1990s. One of the main failings of the US military is its inability to accurately detail and end-state to which one can then declare victory upon and the inability to effectively message the target audiences of a conflict that the US is acting in their interest. We lost a 21-year conflict against violent extremism in the Middle East due to the failings of a whole of government messaging strategy to execute the follow-through of conventional force operations. Failing to have effective information operations when fighting an ideology ensures that one can win every battle and lose the entire war. For example, many organizations and people in and out of the US want the US to do more when it comes to foreign aid, when in fact the US provides $9.4 Billion in aid worldwide, more than the next nine countries combined adding to $8.4 Billion in total. How could it be that people across the world want the US to do more? Successful messaging of foreign nations and anti-US groups along with general misunderstanding and misinformation in the echo chambers of US society. Same with the current Ukrainian conflict where the US has provided nearly $100 Billion alone to the cause with finances and equipment. Foreign nations capitalize on the inherent and sustained division on nearly every topic in the US to continue fissuring the populace. Messages such as that the European Nations don't invest enough in defense, or donate to the Ukrainians, but they will quickly call for the US to give more. This messaging can be viewed as *malinformation,* for most nations in the EU have minimal defense budgets far less than the NATO guidelines of 2% of the GDP, and even less to donate to some other nation. Taking this truth and bringing it to the masses of the US creates frustration and anger at the fact that the US Citizen is once again "footing the bill" for another country. The Ukrainian conflict is an incredible scenario to study information operations from all sides across the globe. We suggest taking time to learn about the many campaigns executed by Russia and the US for this conflict.

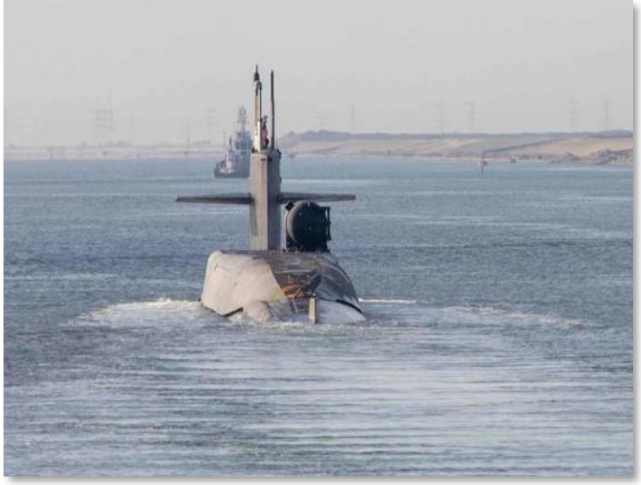


% of GDP by Nation donated to Ukraine.

The US is poor at influence messaging, the "Bureaucricide" (the excessively complicated administrative nature of US decision-making either delays a plan to the point of irrelevance or disapproves it without understanding its full intent) in its approval system hinders its ability to rapidly and effectively capitalize on an event or respond to a scenario. The many tiered levels of approvals and commands assist in the operation of conventional forces as commanders can then focus on areas of interest instead of being bombarded with copious amounts of information on a broad spectrum, but this organization hinders influence operations. Another issue is the hesitation surrounding Disinformation and Deception. The US, which is in a constant struggle for its perception across the entire globe, has increasingly become a focal point of negative sentiment across the Middle East and Africa. The successes of Russian, Chinese, and Iranian messaging operations and the poorly executed 21-year counter-insurgency operations across Iraq and Afghanistan led to a loss in credibility from regional partners. The overconfidence of the strongest military power in the world affects the decision-maker by creating an overreliance on the use of force, also its poor ability to instill it into the services along with the commanders not having a realistic understanding of what troops were going to be able to accomplish in the "Hearts and Minds" campaign of the mid-war operations during the Global War on Terror. Though the US command structure had the essential instruments of power designated DIME (Diplomatic, Information, Military, and Economic) the US DoD and Department of State (DoS) persons failed to comprehend the importance of information throughout most of the war. In its effort to retain the "high road," the US does not rely on disinformation nor deception as much as it could leverage. Both are highly effective tools if not the most effective in an influence campaign.

Massachusetts Institute of Technology (MIT) executed a study on the spread of false stories vs truth. Results showed that a "Fake news" story was 70% more likely to be shared compared to a true story, in which the true story was estimated to take six times longer to reach 1500 users as compared to a false story. Many adversaries and groups take advantage of this phenomenon to increase tensions or create an influx of information to the point where the truth is drowned out. An example is though the US spends more on defense and is militarily, for the most part, unmatched, the US has been losing ground across the globe due to the ability of China and Russia to innovate when it comes to non-traditional military tools in the influence realm of operations. These nations rely on consistent messaging from their perspective and a lack of messaging from the US.

The number one type of messaging the US is good at is security projections and presence. This may not always result in perfect end-state deterrence, but most nations and governments truly do understand the big stick that the US can take anywhere, anytime, at a moment's notice. An example of a recent force projection messaging pertains to the current conflict between the Israeli-Hamas war and the Yemeni Ansar Allah (Houthi) forces in the Middle East. The US repeatedly wanted to remind Iran to not enter the war. They see the aircraft carriers and bombers floating and flying around as usual, that is a certain level of deterrence, but Iran has the ability to see and detect these forces… There is another strategic asset that most people forget about, submarines.

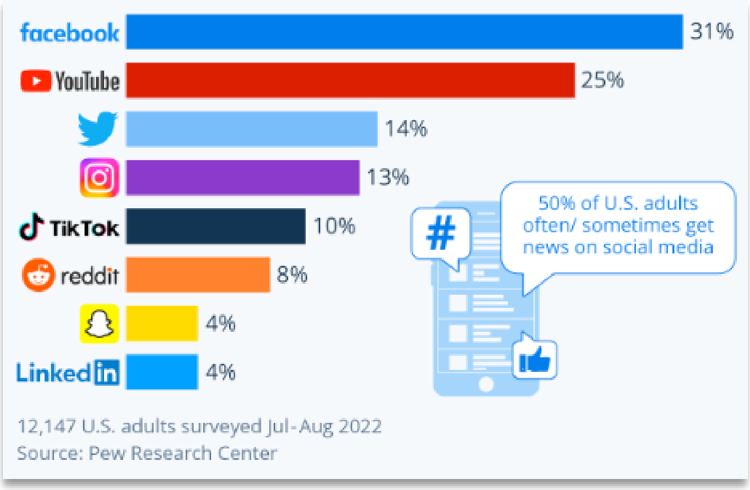


Photograph of Ohio Class Submarine Transiting the Suez Canal NOV 2023.

At times, one must remind the enemy you are present. Thus, this interesting photo was disseminated, let's break it down. In an extremely hostile area, the US surfaces and transits an incredibly important strategic asset through the Suez Canal, taking on enormous risk in exposing the Submarine to the potential for wide variety of attacks. The only reason it makes sense is if it is a message. The US has submarines across the globe, if they wanted it in a specific position near Iran, they could have ordered a sub from the Indian Ocean to silently sneak into position. But that's not what they wanted; we are assuming that it was a deliberate message. A simple and direct statement with no threatening words, just a photo that spread across the Middle East of a submarine capable of carrying 150+ tomahawk cruise missiles or multiple-warhead nuclear-capable missiles. A firm statement to those who would interfere may want to think twice about it. This is probably the only area that the US is repeatedly capable of messaging in, unfortunately, it does not always work, especially with groups that aren't a formal government nor own territory to lose.

Conclusion

Information and Cyberspace are the future of warfare, it is a gray zone in which nations operate 24/7. There are no guidelines or rules set to justify what is an act of war and many government's military and intelligence sectors do not want there to be. The freedom of operating in the grey allows for a wide range of operations from mere reconnaissance to all-out attacks. The main dangers of the information war in the US come from the new nature of American society. Belligerence, sensationalism, slandering, yellow journalism, and more all play a role in the current US



50% of U.S. adults often/ sometimes get news on social media

12,147 U.S. adults surveyed Jul-Aug 2022
Source: Pew Research Center

media consumption. The breakdown in trust of large news media bodies leads to the masses finding each other more disagreeable on what common knowledge or truth even is. The large modern news stations in the US are not to inform you, they are to sell you a product. Nothing is free, every app, channel, movie station and what not is there to influence you to buy something, it is a constant assault on those who participate in modern society. This is a weakness that has broken down the belief in news and journalism in the US. Human tendencies and the recent years of media-induced disharmony have made the citizenry of the US shun healthy debate and acceptance/neutrality of a subject and have turned them into outright antagonists. The rise of many new media sources such as social media has led to massive amounts of sensationalism and misinformation which is "extremely dangerous to our democracy" – Sinclair Owned News Station Script, but in all seriousness, social media has been a goldmine for foreign actors to influence the masses in the US. The breakthrough in artificial intelligence and Generative AI Networks will result in more frequent and harder-to-recognize mis/disinformation products to sort through in everyday life, be it photos, articles, and social media posts and comments.

> *He who dictates and formulates the words and phrases we use, he who is master of the press and radio, is master of the mind. Repeat mechanically your assumptions and suggestions, diminish the opportunity for communicating dissent and opposition. This is the formula for political conditioning of the masses* – Dr Joost Meerloo, 1956

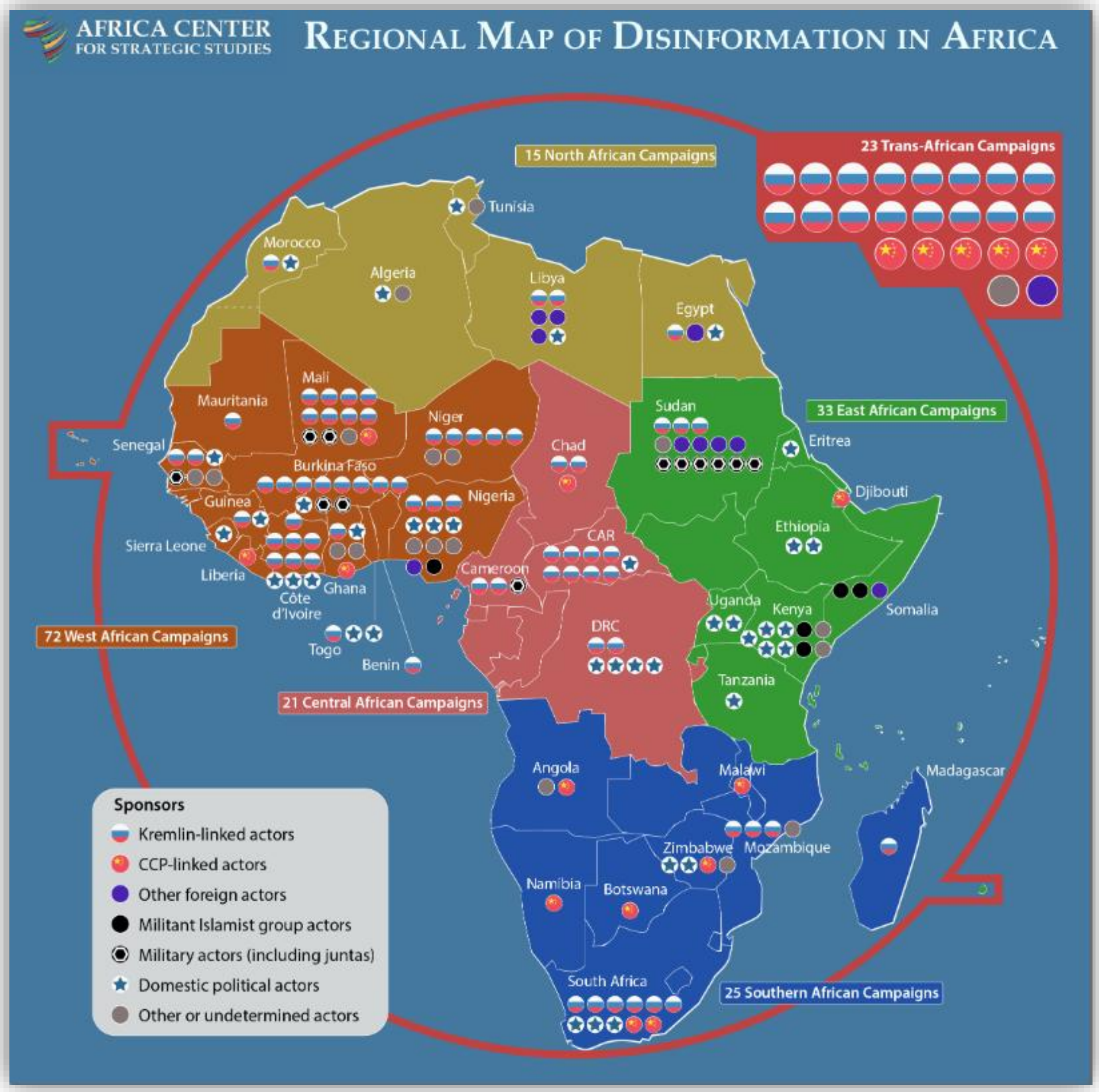

AFRICA CENTER FOR STRATEGIC STUDIES
REGIONAL MAP OF DISINFORMATION IN AFRICA
15 North African Campaigns
23 Trans-African Campaigns
33 East African Campaigns
72 West African Campaigns
21 Central African Campaigns
25 Southern African Campaigns
Tunisia
Morocco
Algeria
Libya
Egypt
Mauritania
Mali
Niger
Senegal
Burkina Faso
Guinea
Sierra Leone
Liberia
Côte d'Ivoire
Ghana
Togo
Benin
Nigeria
Chad
Sudan
Eritrea
Djibouti
Ethiopia
CAR
Cameroon
DRC
Uganda
Kenya
Somalia
Tanzania
Angola
Malawi
Mozambique
Zimbabwe
Namibia
Botswana
South Africa
Madagascar
Sponsors
Kremlin-linked actors
CCP-linked actors
Other foreign actors
Militant Islamist group actors
Military actors (including juntas)
Domestic political actors
Other or undetermined actors

Figure 1. Malign Influence Activities in Africa

References

Bernays, E. L. (n.d.). *Edward L. Bernays and selling tobacco with a grand "Green Ball"*. https://www.lkarno.com

Center for Strategic and International Studies. (n.d.). *Significant cyber incidents*. Strategic Technologies Program. https://www.csis.org

Center for Strategic and International Studies. (2020). *Russian information operations*. In C. Newlin et al., *Countering Russian and Chinese influence activities: Examining democratic vulnerabilities and building resiliency*. https://www.jstor.org/stable/resrep25322.5

Center for Strategic and International Studies. (2020). *Chinese influence operations*. In C. Newlin et al., *Countering Russian and Chinese influence activities: Examining democratic vulnerabilities and building resiliency*. https://www.jstor.org/stable/resrep25322.6

Cordesman, A. H., & Hwang, G. (2020). *Chronology of possible Chinese gray area and hybrid warfare operations*. Center for Strategic and International Studies. https://www.jstor.org/stable/resrep24778

Council on Foreign Relations. (n.d.). *Our biggest errors in Afghanistan and what we should learn from them*. https://www.cfr.org

Cultural Currents Institute. (n.d.). *How Lucky Strike became an icon of the feminist movement*. https://culturalcurrents.institute

Cybersecurity and Infrastructure Security Agency. (n.d.). *Tactics of disinformation*. https://www.cisa.gov

Daniel, T. K. (n.d.). *Information operations, information warfare, and computer network attack: Their relationship to national security in the information age* [PDF]. https://www.menlosecurity.com

Defense Technical Information Center. (2014). *JP 3-13: Information operations*. https://www.dtic.mil

Digital History – Histoire Numérique. (n.d.). *Fashion and elitism advertisements: American women in tobacco advertisements, 1929–1939*. University of Ottawa. https://www.uottawa.ca

DivA Portal. (n.d.). *Russian hybrid warfare* [PDF]. https://www.diva-portal.org

Foreign Affairs. (2023). Power, S. *How democracy can win against autocracy*. https://www.foreignaffairs.com

Kuehl, D. T. (2009). *Information warfare and information operations*. National Defense University Press. https://ndupress.ndu.edu

Military.com. (2023, November 6). *Navy sub with Tomahawk cruise missiles joins Middle East buildup*. https://www.military.com

Morin, D. (2021). Information influence operations: The future of information dominance. *The Cyber Defense Review, 6*(1), 133–140. https://www.jstor.org/stable/26994117

Modern War Institute at West Point. (n.d.). *Information operations for the information age: IO in irregular warfare*. https://mwi.westpoint.edu

National Defense University Press. (n.d.). *Information warfare in an information age*. https://ndupress.ndu.edu

Newlin, C., Conley, H. A., Searight, A., Kostelancik, T., Ellehuus, R., Mankoff, J., & Stewart, D. (2020). *Countering Russian and Chinese influence activities: Examining democratic vulnerabilities and building resiliency*. Center for Strategic and International Studies.

New York University. (n.d.). *Exposure to Russian Twitter campaigns in the 2016 presidential race highly concentrated*. https://www.nyu.edu

Oxford Internet Institute. (n.d.). *IRA political polarization*. https://comprop.oii.ox.ac.uk

Pew Research Center. (2017). *The future of truth and misinformation online*. https://www.pewresearch.org

Porche, I. R., Paul, C., York, M., Serena, C. C., Sollinger, J. M., Axelband, E., Min, E. Y., & Held, B. J. (2013). The problem with information operations. In *Redefining information warfare boundaries for an Army in a wireless world* (pp. 19–30). RAND Corporation. https://www.jstor.org/stable/10.7249/j.ctt3fh1qp.11

Senate Select Committee on Intelligence. (2019). *Report on Russian active measures campaigns and interference in the 2016 U.S. election* (Vol. 5). https://www.intelligence.senate.gov

Shallcross, N. J. (2017). Social media and information operations in the 21st century. *Journal of Information Warfare, 16*(1), 1–12. https://www.jstor.org/stable/26502873

Stanford University. (n.d.). *Targeting women: High fashion*. https://tobacco.stanford.edu

Statista. (n.d.). *U.S. social media users, 2020–2029*. https://www.statista.com

Statista. (n.d.). *Largest donor countries of aid worldwide*. https://www.statista.com

Strategy Bridge. (2018, November 14). *Information warfare: Past, present, and future*. https://thestrategybridge.org

United States Agency for International Development. (2023, March 30). *Remarks by Administrator Samantha Power at the advancing technology for democracy event*. https://www.usaid.gov

United States Air Force. (2023). *Modernizing information operations doctrine to meet new national security needs*. Air University. https://www.airuniversity.af.edu

United States Navy. (n.d.). *Ballistic missile submarines*. https://www.csp.navy.mil

YouTube. (n.d.). *[Video]* https://www.youtube.com/watch?v=ZggCipbiHwE

YouTube. (n.d.). *[Video]* https://youtu.be/K0YRNS0FYTQ