Misinfosec

Applying Information Security Paradigms to Misinformation Campaigns

Christopher R. Walker
Marvelous AI
San Francisco, CA, USA,
walker@marvelous.ai

Sara-Jayne Terp
SOFWERX
Tampa, FL, USA,
sarajterp@gmail.com

Pablo C. Breuer
U.S Special Operations Command
Tampa, FL, USA,
Pablo.Breuer.socom.mil

Courtney L. Crooks PhD
Georgia Tech Research Institute (GTRI)
Atlanta, GA, USA, courtney.crooks@gtri.gatech.edu

ABSTRACT

State actors, private influence operators and grassroots groups are all exploiting the openness and reach of the Internet to manipulate populations at a distance, extending their decades-long struggle for "hearts and minds" via propaganda, influence operations and information warfare. Computational propaganda fueled by AI makes matters worse.

The structure and propagation patterns of these attacks have many similarities to those seen in information security and computer hacking. The Credibility Coalition's MisinfosecWG working group is analyzing those similarities, including information security frameworks that could give the truth-based community better ways to describe, identify and counter misinformation-based attacks. Specifically, we place misinformation components into a framework commonly used to describe information security incidents. We anticipate that our work will give responders the ability to transfer other information security principles to the misinformation sphere, and to plan defenses and countermoves .

CCS CONCEPTS

• Security and privacy~Trust frameworks • Security and privacy~Social aspects of security and privacy • General and reference~Reliability

KEYWORDS

infosec, misinformation, disinformation, viral deception, influence campaigns

ACM Reference format:

Christopher R. Walker, Sara-Jayne Terp, Pablo C. Breuer, Courtney L, Crooks, PhD. 2019. Misinfosec: Applying Information Security Paradigms to Misinformation Campaigns. In *Proceedings of WWW '19: The Web Conference (WWW '19), May 13, 2019, San Francisco, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3308560.3316742

WWW '19, May 13, 2019, San Francisco, USA

ACM ISBN 978-1-4503-6675-5/19/05.
https://doi.org/10.1145/3308560.3316742

1 Introduction

1.1 Misinformation

There is no coherent and widely-adopted definition of *misinformation* (or of *truth*, *credibility*, *trust*, etc).

Disinformation is sometimes defined as dissemination of explicitly false or misleading information; and misinformation the communication of false information without intent to deceive, manipulate or otherwise obtain an outcome. Elsewhere, *misinformation* is used for the deliberate case, both inclusive and exclusive of the accidental case. While we think that definitions are important, we suspect that the common uses of misinformation (and disinformation) hamper their use as technical terms drawing a distinction between intentional and accidental spread. While attacks are inherently intentional, the spread of false information by individuals within an attack may not be. We will not explicitly use terminology to draw this distinction here.

We use *misinformation attack* (and *misinformation campaign*) to refer to *the deliberate promotion of false, misleading or mis-attributed information.* Whilst these attacks occur in many venues (print, radio, etc), we focus on the creation, propagation and consumption of misinformation online. We are especially interested in misinformation designed to change beliefs in a large number of people.

Actors behind misinfo attacks include nation-states, institutional actors, grassroots trolls and financially-motivated freelancers. Common motives include geopolitical aims, issue-promotion, or financial gain. In the run-up to the 2016 US election, websites churning out fabricated stories were a cottage industry. Governments worldwide are studying misinformation as a form of influence operation or information war.

1.2 Misinformation work lacks frameworks

Analysts and engineers have been creatively adapting their own techniques to a range of issues that they perceive to be essential to confronting the larger problem of online misinformation. Which sites promote false stories? How can you detect a false story? How can you detect a false statement? How can you detect a doctored photograph? How can you detect a sock-puppet or a troll? Some platforms have processes in place for detecting and mitigating nefarious user activity. And independent technical approaches have also begun to sprout up. These techniques and toolkits will have potential application in the broader domain of combating misinformation. But tools in themselves have no values and serve no inherent masters.

Misinformation operates within a complicated socio-technical ecosystem, so the approach must be multidisciplinary. Just as cyber security professionals must keep up with constantly evolving techniques and strategies for exploiting private information available within cyberspace, misinformation professionals should expect the same. Further, policy makers must be enabled to develop and enforce data privacy policies that help protect their public from nefarious online activity and privacy breaches. The application of technical and operational techniques can only be productive in the context of thoughtfully designed tactics, grounded in well-defined strategy. Worse, absent strategic and tactical goal-setting we cannot be certain that these techniques are either necessary or sufficient to the amelioration of the threat presented by online influence operations. Without a framework, we are just stabbing in the dark.

1.3 MisinfoSec working group (MisinfosecWG)

The *MisinfoSec Working Group (MisinfosecWG)* is part of the Credibility Coalition, which is an interdisciplinary community committed to addressing the proliferation and amplification of misinformation online, through transparent and collaborative research.

Combining "misinformation" and "information security," MisinfosecWG is developing a framework for understanding organized misinformation attacks based on existing information security principles. Specifically, we promote a more formal and rigorous treatment of 1) detecting misinformation-based attacks and 2) protecting against misinformation-based attacks.

1.4 Existing work on misinfosec

This work grew out of earlier work describing red team and blue team misinformation tactics and characterizing misinformation as an information security problem that infosec frameworks and principles could be applied to .

Misinformation is slowly becoming a subject of interest to information security teams. FireEye helped characterize the Iranian IUVM disinformation network, tracked disinformation typosquats and analyzed traffic in the 2018 US midterm elections; ThreatConnect tracked online infrastructure behind Russian misinformation campaigns, and Synack described how misinformation could be used as part of an information security attack.

The extension of information security to include misinformation is also under discussion. Landau argues that the NSPD-54 definition of cybersecurity should be extended to include information operations (e.g. misinformation), and raises the issue of misinformation users adapting their tools and techniques as detection improves. Rogers frames misinformation as an information integrity problem, citing the infosec concept of maintaining CIA (*confidentiality*, *integrity*, *availability*), and suggests applying infosec practices such as threat modelling. Brockman and Grugq describe parallels between misinformation and information security. Lin and Kerr examine cyber-enabled information warfare as a conflict form where the USA is weak, examine the environment, operations and characteristics of this space, and call for new tactics and responses in it.

1.5 Methodology

Our methodology is to analyze known misinformation attacks to identify their components. What are the atomic *actions* in propaganda attacks? How do actions combine to form larger events, including more complex actions and *attacks*? How do the instances of attacks and actions combine to form *campaigns*?

We then place those components into a framework (e.g. ATT&CK) commonly used to describe information security incidents. The outputs from the group include a misinfosec threat matrix designed for use by "Blue Teams" considering options for defense and counter-attack, and by "Red Teams" anticipating future attack types.

2 MisinfosecWG Activities

2.1 Analyzing Misinformation Campaigns

MisinfosecWG is analyzing known misinformation campaigns. A *campaign* is online manipulation designed to influence the beliefs of a large number of people. It typically consists of several attacks or incidents, aligned toward a specific goal.

In 2017, at least 18 countries used misinformation tactics in elections. Most employed groups of "opinion shapers" to manipulate domestic elections; some, including Russia and Iran, used these tactics to manipulate popular beliefs in other countries. The more well-known campaigns include Russian interference and influence on Brexit, the 2017 French Presidential election, the election of Donald Trump, attacks on the Parkland teenagers, promotion of Jade Helm conspiracy theories and various influence operations around the Black Lives Matter movement. And there are countless less well-known international operations. Private influence operators manipulate beliefs; grassroots 'trolls' and marketers use misinformation campaigns to push agendas or make money, usually from online advertising.

With few exceptions, most of the response thus far has been akin to whack-a-mole. The extent of the threat and the range of

possible actions are simply not understood well enough to formulate counter-moves, whether tactical or strategic.

In our analysis, we look at the actors and their presumed goals and timeframes. We also: look in detail at the methods used in each attack; look at the counters used against them; and list related attacks, as a first pass at creating attack types that can be grouped and discussed together.

2.2 Components of Influence Campaigns

Benkler et al provide a number of useful distinctions. First, they suggest viewing categories of online information threats in terms of a few scalar dimensions, such as *centralized* versus *decentralized*, *political* versus *commercial* and *technological* versus *institutional*. These dimensions suggest we focus on factors such as the *actors*, *objectives*, and *delivery mechanisms* in describing the terrain.

*2.2.1 Actors and Objectives.:*Influence operations are undertaken by an *attacker*, directed at a *target* and sometimes amplified by *carriers*. These actors can all be individuals, populations or institutions. But ultimately the targets are people, or aggregates of people. The objective is typically tied up in the psychology of the actors, especially the targets and carriers. The goal is to change the beliefs and behavior of individual people, often at scale, via manipulation: *directly influencing beliefs, attitudes, or preferences of a target population in ways that are not normatively appropriate in context.* The cognitive objectives of the operations often include widespread factual misunderstanding or confusion. This can vary from *gaslighting* and *disorientation* to *distraction, priming* and *agenda setting*.

*2.2.2 Message, Delivery and Propagation.:*The tactical objective of an attack is typically cognitive or social. The payload is information. Misinformation is semantically misleading, contextually misleading, misattributed, or factually incorrect. The information is transferred via communication events, which themselves can be varied and subtle; some are harder to address than others. The information can range from propaganda to bullshit. *The bullshit artist "does not care whether the things he says describe reality correctly. He just picks them out, or makes them up, to suit his purpose."*

2.3 Social Network Architecture and Message Contagion

The social factors at play involve pathways of communication and attention. For the most part, this amounts to social media. But the interaction between "mainstream" propagandists and their social media sock-puppets and supporters is highly textured. Benkler refer to this interaction as *network propaganda*, noting the familiarity effect with this approach.

Moreover, the types of informational networks that serve as a substrate for the propagation of these messages vary significantly. Some networks are *truth-corrective*: they sanction information that diverges from verified reporting. Other networks are *narrative-corrective*: they sanction information that diverges from the consensus narrative of the network.

And the role of these network-driven attention frameworks on the promotion of marginal framings into the mainstream should not be underestimated. Benkler also describes an attention backbone which promotes stories from the periphery of the network and *propaganda feedback loops* which are *pathological network dynamics in which (mostly attentional) sanctions are imposed for breaking with the received narrative preferred by the target population.*

In short, the objectives are cognitive and the vectors of delivery are social. Successful responses to attacks must be crafted in the context of these varied actors, targets, messages, goals and networks.

2.4 Why Information Security?

We considered adapting frameworks from several fields. This included advertising frameworks, lean enterprise frameworks and information security (infosec) frameworks. We chose the infosec framework because of the close fit between infosec attacks on individual and networks of machines and misinformation attacks on individuals and networks of humans.

The most frequently mentioned alternative is advertising. Tactics and techniques will inevitably draw from numerous fields, advertising prominent among them. For example, advertising test cases might be able to tell us something about the psychosocial motivators that are most effective in advertising. In other words, what techniques are effective in getting people interested or invested in the "product" of the advertisement? Understanding these motivators could be helpful in understanding what captures people's attention in misinformation campaigns.

But while advertising may have much to offer at the tactical level, we ultimately decided that it did not offer an adequate fit to our problems as a framework. Most notably, advertising uses a subset of the attack techniques that we care about, but does not typically convince an audience to do something against their own interest nor does it fabricate false facts. Furthermore, a contrarian might note that tactics from the advertising domain would more appropriately be drawn from the world of anti-corporate advocacy. Efforts to ameliorate ad placement and saturation would have quite a bit to say about which responses are most effective, whether regulatory or otherwise.

Similarly, scholars of health misinformation could be a significant source of tactical insight, given the recent Measles outbreak and its relation to misinformation regarding vaccinations. Our approach is inter-disciplinary, but our framework is information security.

2.5 Adapting Information Security Frameworks

Information security encompasses offensive and defensive computer network operations, electronic warfare, psychological operations, military deception, and operational security. Information security is a robust field with well-understood principles and best practices, covering physical, informational and cognitive dimensions of the information environment.

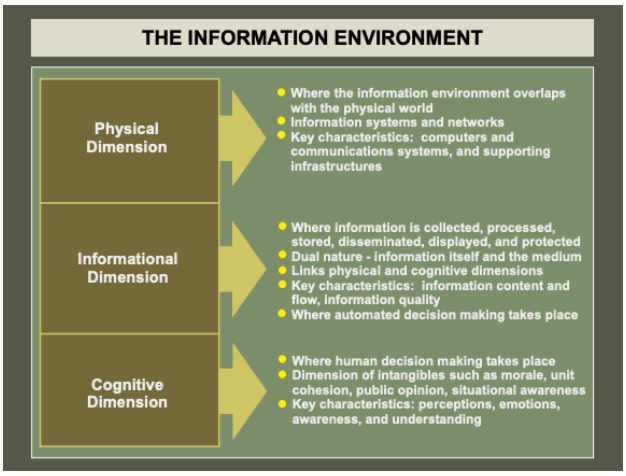

Figure 1: Dimensions of The Information Environment

Alerting systems exist on top of frameworks and standards describing information attacks like DDOS, viruses, and unwanted internet traffic like spam etc. These systems could be a good place to start with misinformation.

We explored potential fits between misinformation and several common information security frameworks: strategic-level models like the *SANS sliding scale* (architecture, passive defense, active defense, intelligence, offense), *Gartner cycle* (prevent - detect - respond - predict), *NIST framework* (detect - protect - identify - recover - respond) and *Cyber Attack Lifecycle*, and operational-level models like the *ATT&CK matrix* and *SANS top 20* .

The Cyber Attack Lifecycle basically maps to our campaign descriptions (*reconnaissance*, *weaponization*, *installation*, *exploitation*, *command-and-control*, and *actions on the objective*). We could also use this lifecycle to link goals and intent (e.g. the "four Ds" of propaganda: Dismiss, Distort, Distract, Dismay).

The MITRE ATT&CK Matrix covers the last three stages of the cyber attack lifecycle, and lists tactic phases (initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, exfiltration, command and control) with a set of techniques that an adversary could use in each phase (e.g. *Spearfishing Attachment* is a type of *Initial Access* tactic). The ATT&CK database provides examples, detection and mitigation for each technique, along with extensive references.

The ATT&CK Tactics, Techniques and Procedures (TTPs) describe *patterns of activities or methods associated with a specific threat actor or group of threat actors.* Tactics are the top-level steps that an attacker typically takes (e.g. "amplify message"); techniques are the different ways those steps can be done (e.g. "repeat message using bots"); procedures are the sequences of actions in an attack. ATT&CK TTPs were created by taxonomizing existing information security threat reports and analyses. A similar process of assembling and grouping TTPs could also work well in support of Blue Team efforts in Misinformation Security (MisinfoSec).

3 A strawman misinformation framework

3.1 Campaigns: Advanced Persistent Threats

In information security, an Advanced Persistent Threat (APT) is an attack or an attacker operating over a long period of time. APTs are usually (but not always) backed by nation-states. In misinformation, APTs usually run long-duration campaigns. The canonical nation-state misinformation campaign is the 2015-2017 Russian troll farm work on the 2016 US presidential elections. Jamieson describes these operations in detail. The objectives are numerous: *an amplifying effect; an agenda-setting effect; a normative effect; target identification; a mobilizing effect; a two-step flow effect; weighting, contagion and spiral of silence effects;* and *a familiarity effect.*

Benkler looked at the online spread of prominent political stories before and after the 2016 US presidential elections. While the authors discuss aspects of the Russian campaign, their primary focus is the online media ecosystem itself. First, the online political environment in the United States is polarized, but the "filter bubbles" are best characterized as 1) the Fox News bubble and 2) everyone else. Second, the corrective sanctions at play in the two environments are highly asymmetric. The latter bubble penalizes for straying from the truth while the former penalizes for straying from the accepted narrative. Interventions against misinfo attacks in these two environments could be very different.

3.2 Incidents: building-blocks of campaigns

Campaigns are often built from smaller building blocks. We will refer to those as *incidents.* One example is the 2014 Columbian Chemicals incident, which we've listed as:

Summary: Early Russian (IRA) "fake news" stories. Completely fabricated; very short lifespan.

Actor: probably IRA (source: recordedfuture)

Timeframe: Sept 11 2014 (1 day)

Presumed goals: test deployment

Artifacts: text messages, images, video

Method: 1. Create messages. e.g. "A powerful explosion heard from miles away happened at a chemical plant in Centerville, Louisiana #ColumbianChemicals" 2. Post messages from fake twitter accounts; include handles of local and global influencers (journalists, media, politicians, e.g. @senjeffmerkley) 3. Amplify, by repeating messages on twitter via fake twitter accounts

Result: limited traction

Counters: None seen. Fake stories were debunked very quickly.

Related attacks: These were all well-produced fake news stories, promoted on Twitter to influencers through a single dominant hashtag -- *#BPoilspilltsunami, #shockingmurderinatlanta, #PhosphorusDisaster, #EbolaInAtlanta*

3.3 Tactics and Techniques

A complete list of misinformation tactics will likely map well to the existing ATT&CK framework tactics. For example, a strawman for this could be as follows.

Table 1: Partial Tactics and Techniques Matrix

Example Tactic	Example Techniques
Initial access	Account takeover Create fake group Parody account Deep cover
Create artefacts	Steal existing artefacts Deepfake
Insert theme	Create fake emergency
Amplify message	Repeat messaging with bots Create fake argument Buy friends
Command and control	Create fake real-life events

This top-down analysis is also being augmented with bottom-up analysis of attacks, looking at the individual components of each attack, and examining and listing those as techniques to fit into the framework.

Table 2: Examples of Techniques and their Descriptions

id	Short	Desc
1	two-events-one-place	Organize two opposing physical events for the same time and place
2	widen-existing-rifts	Increase emotions and use non-false information to widen existing rifts
3	create-fake-emergency	Raise alarm about nonexistent emergency

This process is iterative and collaborative. We will refine these strawmen into more detailed TTP descriptions and recommendations as options are tested or eliminated.

Furthermore, we will define major terms of art at focal points on the scale, with an emphasis on descriptive or procedural rigor. One of the operating assumptions of MisinfosecWG is that social and cognitive factors can "scale up and down" -- facilitating some definitional and procedural crossover in both the construction of a framework for understanding these attacks and in their detection.

3.4 Procedures: New forms of attack

Once we have components, we can put them together in new ways and discover threat types that we might not have considered before. A checklist of threats and best practices creates the space necessary to think more strategically about the misinformation environment and to balance institutional needs in the context of well-tested security principles.

4 Potential Uses

This framework will give misinformation responders the ability to transfer other information security principles to the misinformation sphere, identify gaps in known attack types, plan defenses and countermoves to common components, assess tools and mechanisms, build an information security style alert structure (cf US-CERT) and plan defenses for the types of large-scale adaptive threats that machine learning and other automation makes possible.

Most offensive computer network operations are based upon misinformation, which should aid in our task: network intruders want their targets to make decisions or take actions advantageous to them based on information that's shown, hidden, altered or destroyed, e.g. STUXNET allegedly hid information about the true state of centrifuges from operators, enabling them to make an incorrect decision that no action needed to be taken.

In infosec, an organized taxonomy of attack and defense techniques allows operators to apply well-tested responses to familiar attack patterns, and learn from both successful and failed attacks. For misinformation, these interventions are likely to be drawn from various disciplines including sociology and psychology, e.g. one possible intervention to a misinformation campaign is to push inoculating information--new information that draws opinion away from the goal of the original misinformation. At the campaign scale, some of these interventions will need to be prepared in advance for deployment in specific, measurable contexts, e.g. the Macron teams' preparation in the 2017 French elections for the reuse of a 2016 US Presidential election technique (releasing and amplifying information from leaked political emails).

4.1 Red-Team, Blue-Team Exercises

To build a good defense, you need to understand your threat surface and the types of attacks that are likely on it. The best way to understand attacks is to attack; in information security this is done through simulated attacks, where a "red team" attacks the systems of a defending "blue team". These exercises typically expose previously-unseen system vulnerabilities.

Brundage et al outlines a first red team playbook for misinformation, with common examples of: actors, targets, payloads, objectives, automation, and techniques. Extending this with the misinfosec work will give us a detailed catalogue of attack types with corresponding blue team, allowing platform defenders, and autonomous blue team actors to test and stage effective counter-measures.

4.2 Alerting and Defense

Absent a comprehensive counter-influence strategy from major government and intelligence players, the responsibility for misinformation management currently falls on individual persons and institutions. This mirrors the history of the information security field, which created bodies like the US-CERT organisation: the US government body that coordinates defenses and responses to cyber attacks.

A similar body for sharing and alerting may be needed here. US-CERT's work includes threat monitoring and analysis, information sharing, analytics, operations, communications and international partnerships. Its outputs include a current activity list, monthly active summaries, alerts, notes and tips and security publications.

These activities and outputs map well but not exactly to misinformation (different responses and connections are needed). And US-CERT already has a sister organization, ICS-CERT, which covers security of industrial control systems. We don't yet know which organizational roles will be the end user for a new body's product. Whoever is responsible for the adoption, deployment and enforcement of these practices, will probably require help from security professionals.

4.3 Challenges involved in using frameworks from information security to misinformation

While information security attacks are firmly rooted in the quantitative field of computer science, influence campaigns are, by necessity, rooted in the qualitative fields of sociology and psychology. The linking of quantitative and qualitative fields of science has always been epistemically precarious. Additionally, any attempt to develop an overarching and generalized framework will necessarily omit details. No overarching framework will ever be completely accurate in all situations. This framework attempts to provide an ontology for influence campaigns whether or not they are executed exclusively in the cyber domain. As with any complex system, there will be an emergence of properties which is greater than the sum of its parts. Finally, this framework attempts to examine influence from the view point of tactics, techniques, and procedures (TTPs) without consideration for the intent, morality, or legality of such actions. Analysis of morality, legality, and intent are beyond the scope of this work.

4.4 Counterattack (and its limitations)

Democracies face structural disadvantages relative to the producers of misinformation. Clint Watts cites the Kremlin's strategic edge from Russia's cybercrime underworld and the plausible deniability it gives; the US and its allies don't have this advantage.

Ultimately, America's problem in counterinfluence is that we don't know what to say … During the Cold War, the United States promoted democracy and democratic values. But today the United States doesn't appear to know what it wants. Quite simply, if America doesn't have its feet on the ground, then it can't push back at those challenging us.

This seems right, but generational. In the meantime, we need a plan. One that doesn't sacrifice what we believe in. This is hard. We believe that transparency is key for democratic actors. Knowing who is ***actually*** delivering the message goes a long way. Of course, there are cases in which we want to protect the source (e.g. dissidents in an autocracy), but those are the exception rather than the rule. The framework we propose is agnostic to locality and describes components; it is up to the "local populace" to decide acceptable countermeasures. In other words, part of the remedy is democratic participation itself.

5 Conclusions and Further Work

We've started the work of adapting information security frameworks for misinformation tracking and counters, but there is much work still to do. The information security field has decades of experience that we can draw on in our work, but there have been enough differences between the fields for us to create a new framework, albeit one based on ATT&CK. Challenges we anticipate in this work include epistemology, working across multiple very different fields of research, defining and naming different levels and stages of 'attack'; persuading people that information security frameworks are already about human influence systems, and legal and ethical constraints on response.

This paper focussed on the idea of mapping misinformation to infosec frameworks. Next we complete these frameworks, to understand how we would test and implement specific defenses, before implementing and testing them. Please join us! You don't have to be an infosec person to help: we have lots of small tasks (like finding and describing classic large-scale misinformation 'attacks'). Along the way, we're hoping that more infosec people will understand misinformation better, and more misinformation people will learn about techniques we can apply from a parallel field. Join us here: https://github.com/credcoalition/community-site/wiki/How-to-Help

REFERENCES

[1] Y. Benkler, R. Farris and H. Roberts, Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics, Oxford: Oxford University Press, 2018.

[2] Smith and Banic, "Fake News: How a partying Macedonian teen earns thousands publishing lies," NBC News, 2016.

[3] R. DiResta, "THE INFORMATION WAR IS ON. ARE WE READY FOR IT?," Wired, 2018.

[4] A. Petrov, "Modeling Position Selection by Individuals during Information Warfare in Society," *Mathematical Models and Computer Simulations*, pp. 401-8, 2016.

[5] S. Oates, "When Media Worlds Collide: Using Media Model Theory to Understand How Russia Spreads Disinformation in the United States," in *American Political Science Association 2018 Annual Meeting*, Boston, MA, 2018.

[6] S. Oates, J. B. Barrow and B. Foster, "From Network to Narrative: Understanding the Nature and Trajectory of Russian Disinformation in the U.S. News.," in *International Journal of Press/Politics Conference*, Oxford, UK, 2018.

[7] A. Field, D. Kliger, S. Wintner, J. Pan, D. Jurafsky and Y. Tsvetkov, "Framing and Agenda-setting in Russian News: a Computational Analysis of Intricate Political Strategies.," EMNLP, 2018.

[8] T. Boucher, "Adversarial social media tactics," Medium, 2018.

[9] S.-J. Terp, "Security frameworks for misinformation," 2018.

[10] S.-J. Terp, "Practical influence operations," 2018.

[11] S.-J. Terp, "Social engineering at scale," 2018.
[12] Stubbs, "Exclusive Iran based political influence operation - bigger, persistent, global," Reuters, 2018.
[13] F. Mortola, "Disinformation through fabricated news site," 2018.
[14] Foster, "Influence Operations Targeting the 2018 U.S. Midterms: What are we seeing? What are we not?," 2018.
[15] Ehmke, "Influencer Vaccine: Identifying Information Operations Infrastructure," 2018.
[16] Kuhr, "Leveraging threat intel disinformation campaigns to defeat attribution," 27 February 2017. [Online]. Available: https://www.synack.com/2017/02/27/shmoocon-2017-recap-election-hackers-vs-threat-intel-attribution/.
[17] Landau, "Cybersecurity: time for a new definition," 2018.
[18] Rogers, "Fake news as an information security problem," May.
[19] Rogers, Director, *Fake news as an information security problem.* [Film]. 2018.
[20] D. Gordon, "DEFENDING THE INDEFENSIBLE: A NEW STRATEGY FOR STOPPING INFORMATION OPERATIONS," 2018.
[21] Grugq., "Lessons in Cyber: Influence Operations," 2018.
[22] A. Zegart, H. Lin, T. Fingar, N. Persily and L. Ross, "Cyber-Enabled Information and Influence Warfare and Manipulation: Understanding Problems, Developing Solutions," 2017.
[23] H. Lin and J. Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation," 2017.
[24] H. Lin, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations," 2018.
[25] FreedomHouse., "Manipulating Social Media to Undermine Democracy," 2018.
[26] S. Zannettou, T. Caulfield, W. Setzer, M. Sirivianos, G. Stringhini and J. Blackburn, "Who Let The Trolls Out? Towards Understanding State-Sponsored Trolls," 2018.
[27] D. D. Kirkpatrick, "Signs of Russian Meddling in Brexit Referendum," 2017.
[28] D. O'Sullivan and D. Byers, "Exclusive: Fake black activist accounts linked to Russian government," 2017.
[29] V. Joler, M. Jovanović and A. Petrovski, "Mapping and quantifying political information warfare Part 1 : Propaganda, domination & attacks on online media," 2016.
[30] M. Rosenberg, N. Confessore and C. Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," 2018.
[31] A. Nossiter, D. E. Sanger and N. Perlroth, "Hackers Came, but the French Were Prepared," 2017.
[32] H. G. Frankfurt, On Bullshit, Princeton, NJ: Princeton Univerity Press, 2005.
[33] DoD, "Joint Publication 3-13: Information Operations, February 13, 2006," 2006.
[34] Cyberpedia, "HOW TO BREAK THE CYBER ATTACK LIFECYCLE," 2019.
[35] B. Ninmo, "The 4 Ds of Propaganda: Dismiss, Distort, Distract, Dismay," 2017.
[36] MITRE, "Att&ck matrix for enterprise," 2019. [Online]. Available: https://attack.mitre.org/.
[37] "Post-Exploit Threat Modeling with ATT&CK," 2016.
[38] K. H. Jamieson, Cyberwar: How Russian Hackers and Trolls Helped Elect a President - What We Don't, Can't, and Do Know, Oxford. UK: Oxford University Press, 2018.
[39] M. Brundage, A. Shahar, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, A. Dafoe, P. Scharre, T. Zeitzoff, B. Filar, H. Anderson, H. Roff, G. C. Allen, J. Steinhardt and C. Flynn, "The Malicious Use of Artificial Intelligence:," Archiv, 2018.
[40] M. Brockman, "Data-Driven Propaganda as a Subset of Adversarial Examples," 2018.
[41] C. Watts, Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News, New York, NY: Harper Collins, 2018.