Testimony

The Weaponization of Information

The Need for Cognitive Security

Rand Waltzman

CT-473
Testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity on April 27, 2017.

RAND CORPORATION

For more information on this publication, visit www.rand.org/pubs/testimonies/CT473.html

Testimonies

RAND testimonies record testimony presented or submitted by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies.

Published by the RAND Corporation, Santa Monica, Calif.
© Copyright 2017 RAND Corporation
RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.html.

The Weaponization of Information

Testimony of Rand Waltzman[1]
The RAND Corporation[2]

Before the Committee on Armed Services
Subcommittee on Cybersecurity
United States Senate

April 27, 2017

Dimitry Kiselev, director general of Russia's state-controlled *Rossiya Segodnya* media conglomerate, has said: "Objectivity is a myth which is proposed and imposed on us."[3] Today, thanks to the Internet and social media, the manipulation of our perception of the world is taking place on previously unimaginable scales of time, space and intentionality. That, precisely, is the source of one of the greatest vulnerabilities we as individuals and as a society must learn to deal with. Today, many actors are exploiting these vulnerabilities. The situation is complicated by the increasingly rapid evolution of technology for producing and disseminating information. For example, over the past year we have seen a shift from the dominance of text and pictures in social media to recorded video, and even recorded video is being superseded by live video. As the technology evolves, so do the vulnerabilities. At the same time, the cost of the technology is steadily dropping, which allows more actors to enter the scene.

The General Threat

Traditionally, "information operations and warfare, also known as influence operations, includes the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent."[4] This definition is

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

[2] The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

[3] Joshua Yaffa, "Dmitry Kiselev Is Redefining the Art of Russian Propaganda," *New Republic*, July 14, 2014.

[4] RAND Corporation, "Information Operations," web site, undated.

applicable in military as well as civilian contexts. Traditional techniques (e.g. print media, radio, movies, and television) have been extended to the cyber domain through the creation of the Internet and social media.

These technologies have resulted in a qualitatively new landscape of influence operations, persuasion, and, more generally, mass manipulation. The ability to influence is now effectively "democratized," since any individual or group can communicate and influence large numbers of others online. Second, this landscape is now significantly more quantifiable. Data can be used to measure the response of individuals as well as crowds to influence efforts. Finally, influence is also far more concealable. Users may be influenced by information provided to them by anonymous strangers, or even by the design of an interface. In general, the Internet and social media provide new ways of constructing realities for actors, audiences, and media. It fundamentally challenges the traditional news media's function as gatekeepers and agenda-setters.[5]

Interaction within the information environment is rapidly evolving, and old models are becoming irrelevant faster than we can develop new ones. The result is uncertainty that leaves us exposed to dangerous influences without proper defenses.

The information environment can be broadly characterized along both technical and psychosocial dimensions. Information environment security today (often referred to as cybersecurity) is primarily concerned with purely technical features—defenses against denial-of-service attacks, botnets, massive Intellectual Property thefts, and other attacks that typically take advantage of security vulnerabilities. This view is too narrow, however. For example, little attention has been paid to defending against incidents like the April 2013 Associated Press Twitter[6] hack in which a group hijacked the news agency's account to put out a message reading "Two explosions in the White House and Barack Obama is injured." This message, with the weight of the Associated Press behind it, caused a drop and recovery of roughly $136 billion in equity market value over a period of about five minutes. This attack exploited both technical (hijacking the account) and psychosocial (understanding market reaction) features of the information environment.

Another attack[7], exploiting purely psychosocial features, took place in India in September 2013. The incident began when a young Hindu girl complained to her family that she had been verbally abused by a Muslim boy. Her brother and cousin reportedly went to pay the boy a visit and killed him. This spurred clashes between Hindu and Muslim communities. In an action designed to fan the flames of violence, somebody posted a gruesome video of two men being beaten to death, accompanied by a caption that identified the two men as Hindu and the mob as Muslim. Rumors spread like wildfire that the mob had murdered the girl's brother and cousin in retaliation over the telephone and social media. It took 13,000 Indian troops to put down the

---

[5] Rand Waltzman, "The Weaponization of the Information Environment," American Foreign Policy Council Defense Technology Program Brief, September 2015a.

[6] Max Fisher, "Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is It Terrorism," *Washington Post*, April 23, 2013.

[7] Mark Magnier, "Hindu Girl's Complaint Mushrooms into Deadly Indian Riots," *Los Angeles Times*, September 9, 2013.

resulting violence. It turned out that while the video did show two men being beaten to death, it was not the men claimed in the caption; in fact, the incident had not even taken place in India. This attack required no technical skill whatsoever; it simply required a psychosocial understanding of the place and time to post to achieve the desired effect.

These last two actions are examples of cognitive hacking. Key to the successes of these cognitive hacks were the *unprecedented speed and extent* of disinformation distribution. Another core element of the success of these two efforts was their authors' correct assessment of their intended audiences' *cognitive vulnerability*—a premise that the audience is already predisposed to accept because it appeals to existing fears or anxieties.[8]

Another particularly instructive incident took place during Operation Valhalla in Iraq in March 2006. A battalion of U.S. Special Forces Soldiers engaged a Jaish al-Mahdi death squad, killing16 or 17, capturing 17, destroying a weapons cache, and rescuing a badly beaten hostage. In the time it took for the soldiers to get back to their base—less than one hour—Jaish al-Mahdi soldiers had returned to the scene and rearranged the bodies of their fallen comrades to make it look as if they had been murdered while in the middle of prayer. They then put out pictures and press releases in Arabic and English showing the alleged atrocity.

The U.S. unit had filmed its entire action and could prove this is not what happened. And yet it took almost three days before the U.S. military attempted to tell its side of the story in the media. The Army was forced to launch an investigation that lasted 30 days, during which time the battalion was out of commission.[9]

The Jaish al-Mahdi operation is an excellent example of how social media and the Internet can inflict a defeat without using physical force. This incident was one of the first clear demonstrations of how adversaries can now openly monitor American audience reactions to their messaging, in real time, from thousands of miles away and fine tune their actions accordingly. Social media and the Internet provide our adversaries with unlimited global access to their intended audience, while the U.S. government is paralyzed by legal and policy issues.

The Russian Threat

In February 2017, Russian Defense Minister Sergey Shoigu openly acknowledged the formation of an Information Army within the Russian military: "Information operations forces have been established that are expected to be a far more effective tool than all we used before for counter-propaganda purposes."[10] The current chief of the Russian General Staff, General Valery Gerasimov, observed that war is now conducted by a roughly 4:1 ratio of nonmilitary and military measures. [11] In the Russian view, these nonmilitary measures of warfare include

---

[8] Waltzman, 2015a.

[9] Rand Waltzman, "The U.S. Is Losing the Social Media War," *Time*, October 12, 2015b. For a detailed account, see Cori E. Dauber, "The TRUTH Is Out There: Responding to Insurgent Disinformation and Deception Operations, Military Review, January–February 2009.

[10] Ed Adamcyzk, "Russia Has a Cyber Army, Defense Ministry Acknowledges," UPI, February 23, 2017.

[11] Valery Gersimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," Military Review, January–February 2016.

economic sanctions, disruption of diplomatic ties, and political and diplomatic pressure. The Russians see information operations (IO) as a critical part of nonmilitary measures. They have adapted from well-established Soviet techniques of subversion and destabilization for the age of the Internet and social media.

Russia has a very different view of IO than the United States (or the West in general). For example, a glossary[12] of key information security terms produced by the Russian Military Academy of the General Staff contrasts the fundamental Russian and Western concepts of IO by explaining that for the Russians IO are a continuous activity, regardless of the state of relations with any government, while the Westerners see IO as limited, tactical activity only appropriate during hostilities.[13] In other words, Russia considers itself in a perpetual state of information warfare, while the West does not.

State-sponsored propaganda and disinformation have been in existence for as long as there have been states. The major difference in the 21st century is the ease, efficiency, and low cost of such efforts. Because audiences worldwide rely on the Internet and social media as primary sources of news and information, they have emerged as an ideal vector of information attack. Most important from the U.S. perspective, Russian IO techniques, tactics and procedures are developing constantly and rapidly, as continually measuring effectiveness and rapidly evolving techniques are very cheap compared to the costs of any kinetic weapon system—and they could potentially be a lot more effective.

At this point, Russian IO operators use relatively unsophisticated techniques systematically and on a large scale. This relative lack of sophistication leaves them open to detection. For example, existing technology can identify paid troll operations, bots, etc. Another key element of Russian IO strategy is to target audiences with multiple, conflicting narratives to sow seeds of distrust of and doubt about the European Union (EU) as well as national governments. These can also be detected. The current apparent lack of technical sophistication of Russian IO techniques could derive from the fact that, so far, Russian IO has met with minimal resistance. However, if and when target forces start to counter these efforts and/or expose them on a large scale, the Russians are likely to accelerate the improvement of their techniques, leading to a cycle of counter-responses. In other words, an information warfare arms race is likely to ensue.

A Strategy to Counter the Russian Threat

Because the culture and history of each country is unique and because the success of any IO defense strategy must be tailored to local institutions and populations, the most effective strategies are likely to be those that are developed and managed on a country-by-country basis. An information defense strategy framework for countering Russian IO offensives should be "whole-of-nation" in character. A whole-of-nation approach is a coordinated effort between

---

[12] Voyennaya Akademiya General'nogo Shtaba, *Словарь терминов и определений в области информационной безопасности* (*Dictionary of Terms and Definitions in the Field of Information Security*), 2nd ed., Moscow Voyeninform, 2008.

[13] Office of the Under Secretary of Defense for Acquisition and Technology, "Report of the Defense Science Board Task Force on Information Warfare," Washington, D.C., November 1996.

national government organizations, military, intelligence community, industry, media, research organizations, academia and citizen organized groups. A discreet US Special Operations Force could provide individual country support as well as cross country coordination.

Just as in the physical world, good maps are critical to any IO strategy. In the case of IO, maps show information flows. Information maps must show connectivity in the information environment and help navigate that environment. They exist as computer software and databases. Information cartography for IO is the art of creating, maintaining, and using such maps. An important feature of information maps is that they are constantly changing to reflect the dynamic nature of the information environment. Because they are artificially intelligent computer programs, they can answer questions; provide situation awareness dynamically; and help to plan, monitor, and appropriately modify operations. Information maps are technically possible today and already exist in forms that can be adapted to support the design and execution IO strategy.

As an example, most of the North Atlantic Treaty Organization (NATO) states, as well as several non-NATO partners, are already subject to concentrated Russian IO and they illustrate ongoing Russian IO techniques. Using information cartography, it is possible to map key Russian sources as part of Russian IO operations against a target state. These sources might include:

- Russian and target country think tanks
- foundations (e.g., Russkiy Mir)
- authorities (e.g., Rossotrudnichestvo)
- television stations (e.g. RT)
- pseudo-news agencies and multimedia services (e.g., Sputnik)
- cross-border social and religious groups
- social media and Internet trolls to challenge democratic values, divide Europe, gather domestic support, and create the perception of failed states in the EU's eastern neighborhood
- Russian regime–controlled companies and organizations
- Russian regime–funded political parties and other organizations in target country in particular and within the EU in general intended to undermine political cohesion
- Russian propaganda directly targeting journalists, politicians, and individuals in target countries in particular and the EU in general.

Similarly, the mapping of target state receivers as part of Russian IO against the target state might include:

- national government organizations
- military
- intelligence community
- industry
- media
- independent think tanks
- academia
- citizen-organized groups.

An effective information defensive strategy would be based on coordinated countering of information flows revealed by information maps. An effective strategy would include methods for establishing trust between elements of the defense force and the public. The strategy also will include mechanisms to detect the continuously evolving nature of the Russian IO threat and rapidly adapt in a coordinated fashion across all defense elements.

Christopher Paul and Miriam Matthews of the RAND Corporation observe: "Experimental research in psychology suggests that the features of the contemporary Russian propaganda model have the potential to be highly effective."[14] They present a careful and concise analysis of relevant psychological research results that should inform any information defensive strategy. For example, they describe how propaganda can be used to distort perceptions of reality:

- People are poor judges of true versus false information—and they do not necessarily remember that particular information was false.
- Information overload leads people to take shortcuts in determining the trustworthiness of messages.
- Familiar themes or messages can be appealing even if they are false.
- Statements are more likely to be accepted if backed by evidence, even if that evidence is false.
- Peripheral cues—such as an appearance of objectivity—can increase the credibility of propaganda.[15]

Here is what a typical offensive strategy against a target population might look like. It consists of several steps:

1. Take the population and break it down into communities, based on any number of criteria (e.g. hobbies, interests, politics, needs, concerns, etc.).
2. Determine who in each community is most susceptible to given types of messages.
3. Determine the social dynamics of communication and flow of ideas within each community.
4. Determine what narratives of different types dominate the conversation in each community.
5. Use all of the above to design and push a narrative likely to succeed in displacing a narrative unfavorable to you with one that is more favorable.
6. Use continual monitoring and interaction to determine the success of your effort and adjust in real time.

Technologies currently exist that make it possible to perform each of these steps continuously and at a large scale. However, while current technologies support manual application of the type of psychological research results presented by Paul and Matthews, they do not fully automate it. That would be the next stage in technology development.

These same technologies can be used for defensive purposes. For example, you could use the techniques for breaking down communities described above to detect adversary efforts to push a

---

[14] Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model*, Santa Monica, Calif: RAND Corporation, PE-198-OSD, 2016.

[15] Ibid.

narrative and examine that narrative's content. The technology can help researchers focus while searching through massive amounts of social media data.

Way Ahead

"The massive explosion of behavioral data made available by the advent of social media has empowered researchers to make significant advances in our understanding of the dynamics of large groups online. However, as this field of research expands, opportunities multiply to use this understanding to forge powerful new techniques to shape the behavior and beliefs of people globally. These techniques can be tested and refined through the data-rich online spaces of platforms like Twitter, Facebook and, looking to the *social multimedia* future, Snapchat.

Cognitive security (COGSEC) is a new field that focuses on this evolving frontier, suggesting that in the future, researchers, governments, social platforms, and private actors will be engaged in a continual arms race to influence—and protect from influence—large groups of users online. Although COGSEC emerges from social engineering and discussions of social deception in the computer security space, it differs in a number of important respects. First, whereas the focus in computer security is on the influence of a few individuals, COGSEC focuses on the exploitation of cognitive biases in large public groups. Second, while computer security focuses on deception as a means of compromising computer systems, COGSEC focuses on social influence as an end unto itself. Finally, COGSEC emphasizes formality and quantitative measurement, as distinct from the more qualitative discussions of social engineering in computer security.

What is needed is a Center for Cognitive Security to create and apply the tools needed to discover and maintain fundamental models of our ever-changing information environment and to defend us in that environment both as individuals and collectively. The center will bring together experts working in areas such as cognitive science, computer science, engineering, social science, security, marketing, political campaigning, public policy, and psychology to develop a theoretical as well as an applied engineering methodology for managing the full spectrum of information environment security issues."[16]

The center should be nonprofit and housed in a nonprofit, nongovernmental organization that has international credibility and close ties with government, industry, academia, think tanks, and public interest groups internationally. It should have the following ongoing functions:

1. Bring together experts in a broad range of fields to develop Cognitive Security policies, strategies and implementation approaches.
2. Create clear and practical technology goals in support of the policies and strategies developed.
    i. Identify and evaluate appropriate commercial technologies.
    ii. Identify and evaluate relevant research results and develop and execute strategies for transitioning them into practice.

[16] Rand Waltzman, "Proposal for a Center for Cognitive Security," *Information Professional Association*, September 2015.

3. Work with end users from all communities to develop techniques, tactics and procedures for applying technologies identified and developed to policies and strategies.
4. Create a research agenda for policy and strategy formulation, implementation, and supporting technologies.
5. Develop education and training materials and conduct workshops and conferences.
6. Maintain a response team that will coordinate with all communities to identify influence campaigns and distribute alerts and warnings.

This center should be wholly financed for its first five years by the U.S. government until it can establish additional sources of funding from industry and other private support. The center should also have the authority and funding for grants and contracts, since, apart from a group of core personnel employed by the center, many of the participants will be experts based at their home institution. Although the Center as described would be a non-profit non-governmental organization, this funding model runs the risk of creating the appearance that the U.S. government has undue influence over its activity. This could raise concerns about the credibility of the Center and the motives of the US Government. An alternative would be to seek a combination of private foundation funding and support from international non-partisan non-governmental organizations (e.g. the United Nations).

Conclusion

We have entered the age of mass customization of messaging, narrative, and persuasion. We need a strategy to counter Russian, as well as others, information operations and prepare the United States organizationally for long-term IO competition with a constantly changing set of adversaries large and small. It is said that where there is a will, there is a way. At this point, ways are available. The question is, do we have the will to use them?