A Structure to Counter Fake News

Policy Practicum: Fake News and Misinformation

Stanford University
Department of Management Science and Engineering
Decision and Risk Analysis

Travis Trammell
travist3@stanford.edu
8 January 2018
Introduction

Fake news can drastically alter political, military and economic decisions. This paper presents a structure for counter fake news options when resources are limited and priorities need to be set. As is common with other societal scourges that develop quickly and with little warning, governments and corporations have been taken by surprise and are playing catchup to deal with this issue. As a result, funding allocation and the development of institutional capacity to address the problem of fake news has thus far been ad hoc and reactionary. In order to improve the efficiency of this effort, a more deliberate approach is essential. This paper provides the first iteration of this model.

Historical Examples

Fake news is not a new phenomenon. In fact, it at minimum dates back to ancient Rome and the use of “fake news” tactics by Octavian, Julius Caesar’s adopted son. To further his cause of succeeding the murdered Caesar, Octavian unleashed a false smear campaign on Mark Antony, his main rival for power. This campaign included multiple counts of inaccurate character defamation of Antony (Kaminska 2017).

During the formation of the U.S., fake news was used by Thomas Jefferson to undercut political support in Britain for continued control of the American colonies (Figure 1). The fake story was intentionally designed to emulate the most popular newspaper of the time in the colonies, the Boston Independent Chronicle. It asserted that the British military was paying Native Americans to scalp colonists.
A more modern example during World War II further expanded this tactic. British intelligence supported the distribution of a newspaper and associated radio broadcast for German citizens that described manufactured claims internal corruption in the Nazi regime (Figure 2).
Motivating Examples

Case Study #1 – Fake Tweet Causes Stock Market Flash Crash

Figure 3: Fake Associated Tweet (Keller 2013)

The financial risk associated with fake news is no better demonstrated than from a fake Tweet announcing two explosions occurring at the White House in April 2013. Hackers were able to gain access to the official Associated Press Twitter account and release the false breaking news information. Within minutes of the tweet, the Dow Jones Industrial Average began to drop quickly, 143 points in total, before Associated Press employees were able to delete the tweet and issue a correction (Figure 3) (Moore 2013). Bloomberg News estimated that the flash crash resulted in a loss of $136 million in market equity as seen in Figure 4 (Fisher 2017).

The thirst by the stock market traders for the latest information to gain a competitive advantage over competitors is insatiable. The speed of information consumption and demand has only increased with the rise of high frequency trading which in part relies on pre-programmed algorithms to analyze text in news stories and other online content (Rapoza 2017). For high speed trading, the speed of information is so important that in 2009 firms were willing to pay an estimated $300 million to install a new fiber optic network to connect the New York and Chicago markets (Najarian 2010). The implications are obvious for the potential impact of fake information given the huge financial incentives to react to information first.

A nefarious actor could easily establish a market position in preparation for a market dip and then adjust that position to benefit from a quick rebound with the expectation that fake information would be quickly proven false. Additionally, the actor can target a specific element of the market with the content being produced. For example, the actor could release false information about a particular company or a specific industry. These examples offer a multitude
of lessons for risk management and certainly points to the fact that an effective defense against fake news must be multi-faceted.

Figure 4: Dow Jones Drop Due to Fake Tweet (Rampell 2017)

Case Study #2 – Kamilla Bjorlin Firm Utilized Fake News to Inflate Stock Prices

The potential for fake news to artificially inflate the value of a stock has recently been exposed by the U.S. Securities and Exchange Commission with a crackdown on fake investment newsletters (Stempel 2017). Unlike the use of traditional news cycle announcements to impact the market in a nefarious way, these actors created fake investment informational newsletters to generate interest and increased investment in preferred companies and stocks for niche readers. Increased investment based on false pretenses raises the value of the stock already owned by the conspirators. The notoriety of this crackdown was inflated due to the inclusion of a firm owned by Kamilla Bjorlin, a U.S. television and movie actor. Her firm paid authors to produce fake content for distribution that artificially portrayed the investments to be more attractive than an unbiased assessment would warrant.

The network for this type of fake information production is illustrated by a table produced and distributed by the SEC to help educate investors of this practice (Figure 5). In one case, Bjorlin’s firm utilized this practice to increase the value of a small pharmaceutical firm, Galena Biopharma, by approximately 925 percent. In return for increasing the value of these
firms, Bjorlin’s firm received compensation fees which increased as the value of the deception continued to grow.

Figure 5: SEC News Twitter Feed (SEC Twitter 2017)

At the heart of this issue, lies a subset of the broader discussion concerning the ability of the public to identify false information. On one hand, the potential exists that investors are a more discerning audience and therefore more successful at evaluating information than the general public. Unfortunately, early research in this area does support this aspiration. A recent study by the American Institute of Certified Public Accountants (AICPA) stated that “58 percent of Americans believe that fake news is a serious threat to their financial decision making” (AICPA 2017).

A nefarious actor could certainly identify numerous variations of this type of for profit fake news creation to exploit but the following are a few twists that we deem most likely. First, releasing false sales data to create an overly optimistic perception of the value of a particular company and encourage investment in the company’s stock. Second, releasing false information concerning product testing relative to competitors, i.e. consumer reports, in order to either promote actual sales or just to build greater enthusiasm for the product. Finally, fake information concerning a merger between two firms could be released in order to temporarily drive up the stock price of two companies simultaneously until the information is corrected.
Case Study #3 - Russian Fake News Campaign to Support Incursion into Crimea

“The most amazing information warfare blitzkrieg we have ever seen in the history of information warfare.”

*General Phillip Breedlove, Commander U.S. European Command, 2014*

The blitzkrieg that General Breedlove speaks of is the coordinated effort by the Russian government to impact the outcome of the struggle with the Ukraine for control of Crimea. This barrage included fake news and mass text messaging (Peterson 2017). A sample of the Russian produced fake news concerning Crimea is illustrated in Figure 6. The fake article attempts to influence the Crimean population by providing false figures and supporting charts as evidence of economic growth following the Russian occupation of the Crimea (StopFake.org 2017).

The continued use of fake news by the Russians even after the primary invasion is interesting to say the least. Identifying this fake news effort as “after the fact” provides a wrinkle to an already established tactic of launching fake news in coordination with other military or paramilitary action which has now been demonstrated a second time by the Russian military operations in Syria. Not only does this tactic continue to suppress opposition to Russia presence in Crimea but it also serves as propaganda influencing other ethnic Russian populations in Europe, most notably in Estonia, Latvia, and Belarus. This propaganda is also contributing to a potential flashpoint in Estonia, a NATO member and defended under Article 5, among ethnic Russians seeking reunification with Russia and the elected government.
Following fake news involvement in the 2016 U.S. Presidential Elections, experts expected a deluge of fake news to accompany the lead up to the 2017 French Presidential Elections. Fake news was certainly present in the French Presidential Elections and the volume remains concerning according to NewsWhip data (Figure 7). However, a study by Oxford University indicates that the volume of fake news shared by French citizens was significantly lower than the fake news volume observed during the 2016 U.S. Presidential Election cycle (Howard et al 2017). In fact, according to this study, legitimate news was shared by French Twitter users at a rate of 2 to 1 compared to fake news (Figure 8).

A similar analysis of the U.S. Presidential Election demonstrated this ratio being much worse for U.S. citizens, at times approaching 1 to 1. Opinions vary as to the reason that fake news was less “viral” during the French elections in comparison to the U.S. First, the world community was undoubtedly more aware of the threat of fake news based on the media coverage...
it had previously received. Citizens were more informed and likely more discerning of the news that they were reading. Second, the Russian effort in the French elections primarily supported the National Front, whose popularity has suffered for a variety of reasons. Thus, the fake news effort suffered from supporting a relatively non-competitive party.

Figure 7: Fake News Volumes in 2017 French Presidential Elections (Secret 2017)

<table>
<thead>
<tr>
<th>Table 3: French Political News and Information On Twitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Source</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Professional News Content</td>
</tr>
<tr>
<td>Major News Brands</td>
</tr>
<tr>
<td>Minor News Brands</td>
</tr>
<tr>
<td>subtotal</td>
</tr>
<tr>
<td>Professional Political Content</td>
</tr>
<tr>
<td>Political Party or Candidate</td>
</tr>
<tr>
<td>Government</td>
</tr>
<tr>
<td>Experts</td>
</tr>
<tr>
<td>subtotal</td>
</tr>
<tr>
<td>Other Political News and Information</td>
</tr>
<tr>
<td>Citizen or Civil Society</td>
</tr>
<tr>
<td>Junk News</td>
</tr>
<tr>
<td>Other Political</td>
</tr>
<tr>
<td>Russia</td>
</tr>
<tr>
<td>Humor or Entertainment</td>
</tr>
<tr>
<td>Religion</td>
</tr>
<tr>
<td>WikiLeaks</td>
</tr>
<tr>
<td>Political Merchandise</td>
</tr>
<tr>
<td>subtotal</td>
</tr>
<tr>
<td>Other</td>
</tr>
<tr>
<td>Social Media Platform</td>
</tr>
<tr>
<td>Other Non-Political</td>
</tr>
<tr>
<td>subtotal</td>
</tr>
<tr>
<td>Inaccessible</td>
</tr>
<tr>
<td>Language</td>
</tr>
<tr>
<td>No Longer Available</td>
</tr>
<tr>
<td>subtotal</td>
</tr>
</tbody>
</table>

Source: Authors’ calculations from data sampled 03/13/03/19

Figure 8: Twitter distributed Fake News compared to other News (Howard et al 2017)
Case Study #5 – Fake News to Undermine NATO Support to Latvia

In an effort to influence the population of Latvia concerning NATO military exercises within the country, Russian backed news sites have generated significant fake news content. One fake news story headline reads, “You will pay for that: Latvia will pay millions to deploy the NATO battalion”, and speaks to the deployment of a NATO Battalion (multinational unit led by Canada) (Figure 9) (Goble 2017). A primary focus for the U.S. and NATO in the effort to deter Russian aggression and intimidation after actions in Crimea is centered around forward deployment of NATO forces along the Russia border combined with integration and training exercises with the militaries of the host nations. Independent of the wishes of the governments of Russian border states, the Russians see a potential to sway the opinion of some members of the population of these nations. If successful, the population could in turn pressure their political leaders to limit involvement with NATO exercises and even reject forward deployment of NATO forces. This strategy has obvious consequences for the rest of NATO and could ultimately undermine the strength and commitment of the alliance.

Figure 9: Latvia Fake News on NATO Battalion
The ongoing conflict in Syria between forces loyal to President Bashar al-Assad and opposition forces has certainly resulted in numerous areas of study for students of warfare. However, of note, a recent action by the Russian government is believed to be without precedent. In the ongoing effort to discredit the U.S. involvement in the Syrian conflict the Russian Defense Ministry claimed that the U.S. was in fact providing support to ISIS forces which are opposing President al-Assad and is actively supported by the Russian military (O’Connor, 2017). As evidence of this claim, the Russian Defense Ministry offered purported imagery of a ISIS convoy that it claimed was being over watched by a supporting U.S. AC-130 gunship (Figure 10). Fact checkers eventually determined the image was actually captured from a video game entitled “AC-130 Gunship Simulator: Special Ops Squadron.” When confronted with external evidence of the inauthenticity of the photo, the Russian Defense Ministry admitted that the photo was false and claimed the release was the result of a mistake by a low level employee.

Lessons learned from this event for the study of fake news are numerous but two of particular significance relate to the potential difficulty associated with verifying imagery of this type and the ever increasing sophistication of virtual environments for production of imagery. First, photos and videos are commonly released by military forces to document a particular action or at times to refute a specific accusation. However, much of the details surrounding the circumstances of the video or the event remain highly classified for operational security reasons. Thus, the willingness or ability of military officials to offer specific evidence associated with a particular event are often very limited. At the very least, this complicates the task of refuting fake evidence of military actions. Additionally, military release of information is naturally a very deliberate process for operational security reasons to avoid the potential of giving enemy forces an unintended advantage. In an effort to be thorough and accurate, the military is often slower to officially respond to an incident and this often advantages the purveyor of a false narrative. A second takeaway from this incident is just how life like the virtual environments within gaming platforms have become. These environments are designed to be as life like as possible to contribute to the experience of the player. However, for relatively insignificant cost and with virtually no technical skill a nefarious actor can create a fictitious battle scene to support a fake news narrative. The increasing sophistication of these games only points to a
future environment where telling difference between actual drone footage and that of a video game will be even more problematic.

![Image](image.png)

Figure 10: Video Game Image Used by Russian Defense Ministry

Case Study #7 – Fake Evacuation Announcement for U.S. Military Families in Korea

Non-combatant evacuation operations (NEO) are a key element of U.S. military plans to protect the families of military personnel deployed overseas. When ordered, these operations utilize U.S. military capabilities to move family members to a safer location, most often back to the continental U.S. To the international community the initiation of NEOs serve as indicator of the increased likelihood of conflict or a deteriorating security situation in a particular area of the world. Resultantly, the decision to execute a NEO is not taken lightly and is the subject of significant administrative review by U.S. officials. Thus, when U.S. service members and families residing in South Korea received text messages apparently issued by U.S. Forces Korea concerning the initiation of a NEO, social media was quickly a buzz with the topic (Haltiwanger 2017). Thus, what began as emanating only through text message was soon spread across social media. U.S. military officials acted quickly to discredit the announcement and to provide resources for U.S. personnel to report any additional information releases related to this topic (Figure 11). An investigation into this incident by the U.S. military remains ongoing and few answers as to the source of the messaging including a potential motive are currently available.
While the source of this action remains unknown, the potential implications for this type of attack should be discussed. First, the use of this type of misinformation would be very valuable for an adversary planning a conventional attack. Not only would it sow confusion among U.S. forces but it would also cause the diversion of much needed resources to refute the false orders. Second, the use of this tactic introduces the potential for the “cry wolf effect” in that actual evacuations or announcements may be incorrectly ignored. Third, this type of attack could be used by a third party actor to attempt to initiate conflict between two competitors. In this case, a nation state that felt it would benefit from a U.S. and North Korean conflict could utilize this tactic to push the two nations closer to actual war. North Korean leadership could interpret the commencement of a NEO as indication of plans for future offensive military by the U.S. In turn, the leadership could conclude that in light of this belief, a pre-emptive strike on South Korea is advantageous.

Figure 11: U.S. Military Alert concerning Fake Evacuation Order
Holistic Strategy to Counter Fake News

The rise of fake news as a primary arm for Russian in the struggle against NATO and the U.S. requires a more sophisticated analysis of the techniques available to counter this misinformation. I divide these efforts into two broad categories: Offensive and Defensive. These categories, by design, align with those of the U.S. military addressing conflict situations. The following list is by no means exhaustive. If anything, this is only the beginning of the development required to successfully address the scourge of fake news.

Offensive Options

Offensive capabilities to combat fake news are incredibly diverse and I begin with the least intrusive and then move to most intrusive. Starting at the bottom of the pyramid in Figure 12, the options range from fairly benign to options likely to result in a kinetic response from a nation state at the top. One size does not fit all and each situation and threat must be evaluated separately to determine the appropriate response.

Figure 12: Counter Fake News Pyramid
Block or Disable Social Media Bots

Social media provides a low cost and easy to access platform to promote fake news. With the rise of fake news, certain accounts have become associated with the promotion and dissemination of misinformation. In fact, Twitter and Facebook have taken action to disable specific accounts associated with fake news (Burch 2017). However, this occurred post facto and after the damage had been done. This technique must be updated to respond more quickly and should include the capability to temporarily suspend versus revoke. Given the appropriate indications, the U.S. government must maintain the capability to strategically limit the ability of certain actors to promote these messages.

While the threshold for limiting the ability for an individual to communicate ideas to other people should certainly be subject to due process, the bar should be much lower for so called “bots.” These bots are tied to a centralized control structure that is able to quickly generate “fake” popularity which in turn then draws in genuine interest and popularity. A variety of technical measures, both those that are currently known and those that could be developed, should be leveraged in order to limit the ability of these elements to spread their messages. Perhaps most effective of all should will be the ability to accomplish this limitation without the knowledge of those impacted. It could be as simple as surreptitiously slowing the connection speed of the “bot” master. The bot issue shows no sign of dissipating and will likely get worse as more sophisticated methods for developing and controlling the bots are developed. In fact, a joint study conducted by USC and Indiana researchers concluded that as many as 15% of all Twitter accounts are bots (Varol et. al 2017). Problematic to say the least for the purposes of limiting their impact.

Figure 13: Blocked ISIS linked Twitter Account (Olajide 2015)
**Fake News Counter Offensive (Authoring and Promoting Offensive Misinformation)**

Our first option in a fake news counter offensive is to “give the Russian government a taste of its own medicine.” The vast resources of the U.S. intelligence community can easily be leveraged to create a fake news capability equal or exceeding those of Russia. Ideally this loose network would be distanced from the U.S. by a confusing web of proxies and employing a group of “independent contractors” such as the much publicized Macedonian teenager. This web is not unlike many of the activities already associated with the U.S. intelligence agencies. Direct control over the messaging must be limited in order to mask official involvement and to take advantage of creative development of content. Guidance could be as simple as to push articles that are anti-Putin for example.

The objective in the development of this capability is threefold:

1. Provide a deterrent by demonstrating capability
2. Cause the Russians to divert misinformation resources to respond to attacks
3. Limit Russian misinformation resources by adding competition to the marketplace for “independent contractors”

![Figure 14: Anti-Putin Propaganda (Redice TV 2017)](image-url)
**Fake News Counter Offensive (Credibility Attack on Fake News Authors)**

Currently fake news authors can operate with basic impunity. Granted, personal credibility may not be of the greatest concern for a “Macedonian teenager” there are points of leverage in this area that can be exercised by the U.S. government. While actions against American citizens would require greater legal oversight and approval, non U.S. citizens would be subject to methods that would likely be deemed inappropriate or even illegal against individuals that are subject to the U.S. Constitution. Some of these methods could include but are not limited to: online smear campaign, reaching out to online associates with threats of exposure of links, online monitoring to capture potentially embarrassing habits, financial manipulation or ransomware type schemes. Additionally, deterrence can prove to be an effective tool in this arena. The threat of these actions will, at a minimum, cause high volume fake news authors to reduce their public exposure, lower the probability of some type of advertising mechanism, and generally push the enterprise deeper in to the recesses of the online community.

![Figure 15: Sasha Obama Fake News (Snopes 2017)](image)

**Blocking or Degrading Internet Connectivity to Regions of the Globe**

While a marked escalation in the fight against misinformation, in a similar approach to the declaration of martial law during a national emergency, the U.S. must maintain the capability to “flip the switch” on information sharing from a particular country or region and elements within the U.S. The modern telecommunications infrastructure has certainly made this a much
more difficult task but not impossible. Beginning with the social media community, the U.S. should develop relationships with social media companies where based on official Presidential requests, utilized in only rare occasions and with oversite safeguards established, temporary regional or country blocking is possible.

The social media blocking system could be modelled in a method similar to the Civil Reserve Air Fleet (U.S. Air Force 2017). In short this program allows the U.S. Transportation Command to commandeer aircraft owned and operated by civilian airlines in order to transport U.S. Troops in the event of a major theater war. A similar system, perhaps managed by the National Security Agency, should be constructed in association with the social media giants.

The next level of limiting connectivity to fake news promoters is a so called “hard blocking” strategy which involves the physical destruction of required internet elements within a certain area. These could take the form of a virus to attack software all the way to the extreme of a physical strike on servers or power distribution required for internet operation. While initially envisioned as a method to cause disorganization and degrade command control of enemy military forces during a traditional military conflict, application of this tactic against misinformation is warranted.

**Defensive Options**

Equally important to a capable Offense against fake news is building the Defensive resiliency required to succeed in this space. Defensive options have the benefit of generally being less controversial than the Offensive options previously mentioned. Again, this list is not exhaustive but provides a good starting point.

*Financial Incentives to Assist in the Misinformation Fight*

Research and development across the best universities in the U.S. will be a vital element in the long term effort against fake news, in the same vein as the system that assisted the U.S. in developing a technological edge over the Soviet Union during the Cold War. Research grants need to be tailored to researchers addressing this issue. Reward challenges that offer monetary
compensation for solving certain technical issues seem to be particularly appropriate given the topic.

In general, these reward challenges are much less bureaucratic and encourage teaming of experts in an effort to solve complex issues. An additional benefit to this method is that it often results in the formation of startup companies based on any breakthroughs that will then grow, primarily through private investment, into an independent entity capable of further work in the misinformation space. Much of the capacity in this struggle will certainly reside in private hands.

Figure 16: SOCOM Coding Challenge Announcement (Urban Challenge 2017)

*Steering the Massive U.S. Intelligence Leviathan Against Misinformation*

The U.S. intelligence community spent decades honing its skills and methods during the Cold War. Experts often note that this singular focus on the Cold War limited the ability to highlight the rise of international Terrorism as a threat following the breakup of the Soviet Union. Policymakers cannot fail to marshal the resources necessary to effectively develop the intelligence to be successful in the information environment. Traditional intelligence trade craft must be used to infiltrate these organizations, better understand their goals and objectives, and identify their methods and technology for exploitation. This information must then be effectively paired with methods to limit their effect and to manipulate their understanding of the environment.
Education Strategies

An informed population is the foundation for democracy. Education programs, perhaps leveraging libraries and librarians, must be mobilized to teach the population effective methods for research and confirmation of information.

![How to Spot Fake News](image)

Figure 17: How to Spot Fake News
(International Federation of Library Associations and Institutions 2016)

Public Service Announcements

At times of elevated risk of fake news, during elections season for example, the U.S. government should provide warning for the population. Think of this warning as public service announcements in order to alert the public to the likely increased presence of fake news. A warning system (akin to the much maligned but recently modified travel advisory system) should at least be explored. Whatever form it takes, the public must be warned to be extra vigilant at certain times or based on specific indicators.
The U.S. has long depended on the citizen Soldier for the common defense. We must apply this model to the combating of fake news. The U.S. government needs to bring online actors into the service of the nation but with as reduced administrative requirements as possible. For reference, a similar program was recently announced for the direct commission of Cyber Officers within the U.S. Army (Vergun 2017). We need to these talented individuals working for the public benefit.

Several experts have recently advocated for the establishment of a National Cyber Academy to help develop and nurture the talent needed to address the cyber challenges of the future (Hagerott 2017). While this could be applicable in the area of misinformation, I am not advocating for this specific solution in response to fake news. First, misinformation does not generally involve hacking. Less specific technical knowledge is required. It is oft said that “1 great coder is as valuable as 1000 good coders.” I do not feel this idea applies in the misinformation space. Thus, the answer is not a small group of highly trained technicians, but instead a less formalized but broader network of militia members who are loosely connected as a community. Rewards are perhaps an appropriate method to identify misinformation within the community. Currently, there is not an economic incentive for an individual to combat fake news versus to produce it. We can change this paradigm with an effective rewards or compensation system within a community appropriately motivated to stop fake news.
Create the Lie of the Week List

The U.S. government as a whole needs a more effective method of correcting inaccurate information. One possible tactic could involve the publication of the “top lies of the week” or something of the sort where information correction efforts are focused on the most viewed fake news. The landscape of inaccurate information is much too vast for the U.S. government to attempt to address every aspect with corrections. Not only are the resources not available but by addressing so many elements the government is diluting its own correction message.

The U.S. government must focus on the elements of misinformation at that is the most damaging and needs the most attention. As a society, we have become much more focused on headlines and sound bites. In fact, a recent study reported that “59 percent of all links shared on social networks aren’t actually clicked on at all” (DeMers 2017). Thus, implying that many news articles are being shared based on headline alone. Nothing can hold the attention of the population for an extended period of time in this environment. Thus, practices must be adjusted. Granted, the standard method of a press conference or an official statement release still has a place in the U.S. government communication strategy still has a roll but it must be buttressed by a multipronged approach that is faster and more interesting. This effort will certainly involve increased risk taking but undoubtedly the fake news purveyors have identified a perceived advantage in the relative lethargy of the government media apparatus. In truth, this is only the start of the conversation. A ranking of the week’s top lies is just the beginning. Similar to the focus on innovation through the technical challenges reward system, similar programs need to be developed to spawn entrepreneurial thinking in the area of government communication. Government can and should enlist the help of social media experts to help craft the most effective strategy.

Imbed Reporters in the U.S. Government

As previously intimated, in order to effectively counter misinformation the U.S. government needs to be more open with information versus less. Instead of attempting to clamp down with more control of information, it needs to be offered in more forums. To this extent, imbedding reporters in U.S. government organizations should be more of a standard practice. A precedent for this already exists in the military. For many years, reporters have been embedded with combat troops in order to cover conflict. While challenges must certainly be overcome
including conflict of interest concerns, the benefits outweigh the cost. An independent voice within the government would help to diffuse the potential for fake news articles concerning the actions and motivations of the actors in the U.S. government. Finally, one reason the U.S. military has been so supportive of these programs is that military leaders view the embed program as benefiting the military mission. Accurate reporting generally favors the U.S. military’s method and ideals as compared to an adversary that that holds itself less accountable. A similar mindset should be adopted by other elements of the government.

![Image: Reporter Embed during the Iraq War]

Figure 19: Reporter Embed during the Iraq War

**Greater Use of Video – Less on Written Statements**

Emerging research has shown video to be much more impactful than text at refuting false information (Young et al 2017). Visually oriented platforms certainly dominate the modern information environment so this fact is not surprising. The U.S. government has yet to fully embrace this concept however. The U.S. government needs to leverage this concept at every turn. Instead of a stuffy press release, the U.S. government needs to let the cameras in where possible.
Embrace Social Media at Government Agencies

The U.S. government can enlist the help of its employees to help tell their story. Take some risk and allow employees to post videos of themselves performing their jobs and discussing their responsibilities. A culture that embraces versus shuns social media is required in order to allow employees to become the best possible spokespersons for the institution.

Figure 20: Official U.S. State Department Facebook Page

Conclusion

Fake news is certainly not going away. As technology continues to push the frontier of content production, those actors desiring to deceive people will undoubtedly take advantage. The U.S. government cannot hope for a solution to this problem to arise organically. It must take bold and decisive action to address misinformation. This paper provided an initial Offensive and Defensive based strategy to combat fake news based on current methods and tactics. Continued development and research is vital to continue to confront this scourge and prevent the long term erosion of “truth” in modern society.
Sources


U.S. Securities and Exchange Commission Official Twitter Feed.

