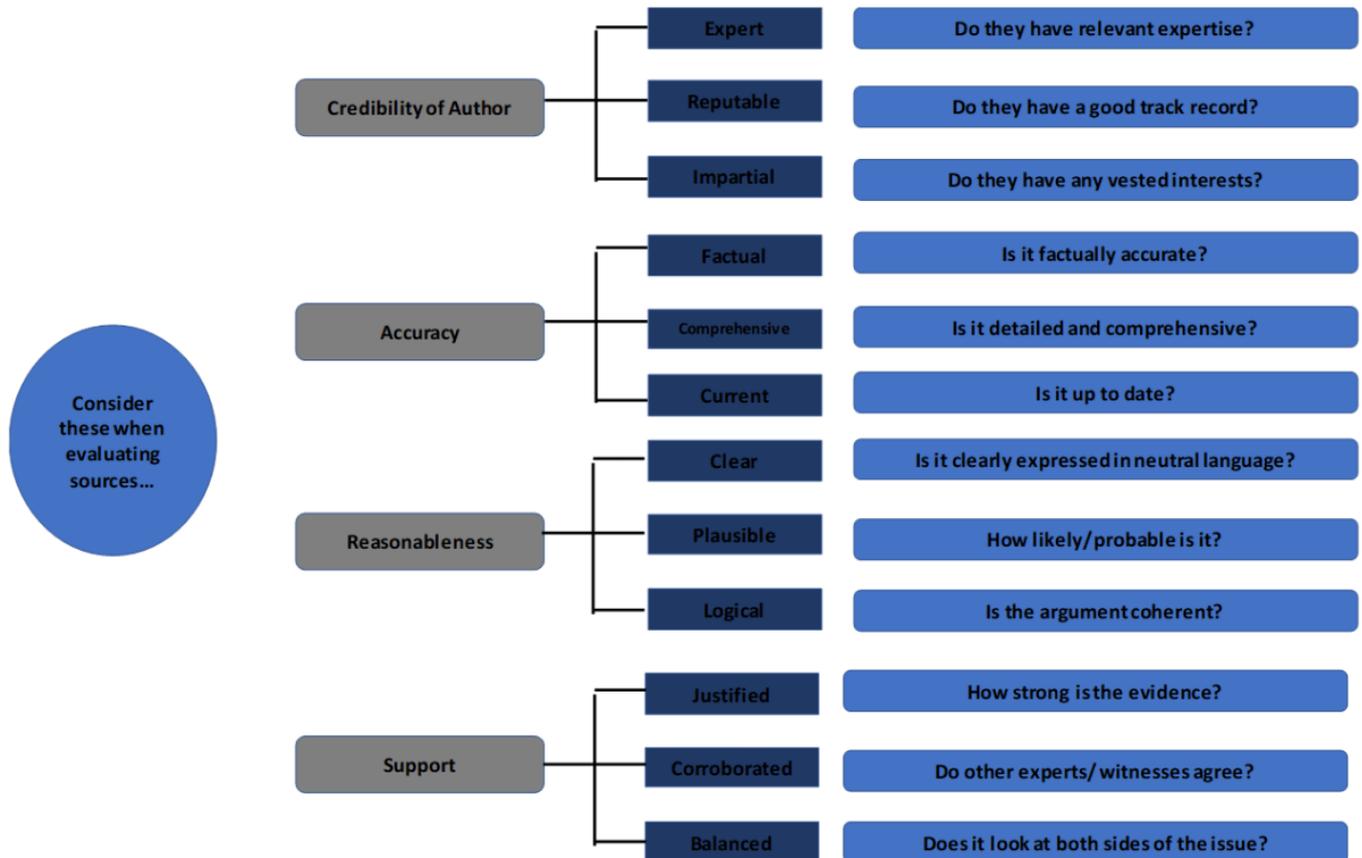


## Some things you should understand before jumping headfirst into the information environment

By Larry Kay

Last week was “media literacy week,” which unlike national doughnut and Twinkie day, should be elevated to a more prominent occasion given how central the internet, media and social media are to our lives. Given how clouded and competitive the information environment is, it is supremely important that people become ‘media and internet literate.’ What I urge everyone to recognize is that the information environment is as open and amusing as it is caustic and dangerous in today’s strategic context. To put a necessary point on it: these are dark times and for every piece of truthful and accurate information, there is an equal if not greater amount of falsehoods masquerading as truth. Many discussions today about the information environment or information operations are concerned primarily with how to win, but often do not apply much thought or consideration toward not losing or identifying disinformation. This article aims to help people navigate the treacherous waters of the web, to prevent them first from losing to disinformation and falsehoods. However, before you search on Wikipedia for the definition of ‘media and internet literacy,’ please consider the following before you begin your journey.

1. Internet literacy is an essential preliminary to thriving in the information environment. Below is a checklist, which describes how to evaluate sources of information. It is applicable to all mediums but especially important for the internet, where anyone can just conjure information with the tap of a key.



2. Ends, ways, and memes. The most imperceptibly threatening arena of battle today is the discursive battlefield of the internet byways of keen rhetoric and clever deception. This warfare will be waged, firstly, lastly and endlessly, in the minds of the people. Given the necessary emphasis on multi-domain operations, it is important to note that information operations are the most central and essential element of multi-domain operations. We must recognize our enemies' informationization of their strategies and respond in kind. The reality is that true power exercises its greatest influence when it remains hidden from view, enchanting the soul, and not the body. When we collectively take a position of passive defense to prevent the belief and spread of falsehoods, we are doing the groundwork of defending the country - like packing sandbags in a position to protect against the flak, everyone can and must do their part. We are at our most vulnerable when we scroll Facebook and Twitter. The seemingly harmless meme chock full of pithy and snarky

platitudes is the most prolific form of propaganda. Do not fall for it. Sharing just one Russian produced meme compounds the problem and risks you and others becoming 'useful idiots' (that's what Russians call people that do what they want them to do).

3. Sourcing. RT, which stands for "Russia Today", and Sputnik (duh) are Russian state-run media. The Global Times is run by China. InfoWars, Breitbart and One America News Network (OANN) frequently repost RT articles. A little more complicated are the talking points of other countries that are packed to appear like another side of an argument. The best propagandists can convince anyone that their ideas are your own when in reality, they subliminally influenced and created them over the course of many months and countless images and arguments. Truth and falsehood are both habit-forming. Before you share something, anything, verify the source to confirm that you are not helping the enemy gain access to the hearts and minds of your neighbors - and that you are not parroting a Kremlin talking point on Syria.

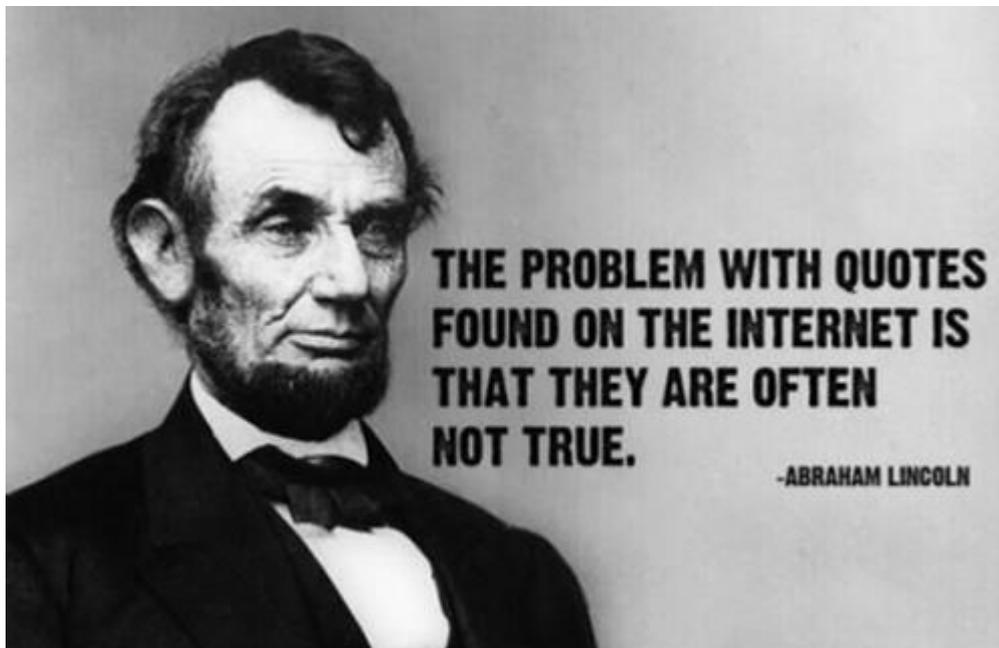
4. Conspiracies theories. Voltaire once said that "those who can make you believe absurdities, can make you commit atrocities." We must always consider the value of narrative in the representation of reality. Logic and reasoning are not synonymous with common sense. In fact, logic is difficult to many and not because those people are ignorant, but because actual logic is not nearly as natural a skill as storytelling is. A well-formed argument and a good story can both be used as a means for convincing a person, but they are implicitly different. The former appeals to logic and evidence to claim a propositional truth. The latter does not claim truth, but plausibility or the appearance of truth. A good story does not necessarily have to be true for people to believe it and for that reason, narratives are often embellished with evocative, sensational language and images making them accessible to an audience. Pizzagate, Area 51, Seth Rich, Hurricane Lane, 9/11, CrowdStrike and the Sandy Hook conspiracies theories are all examples of evidence-less storytelling and they are untruthful. Then again, if you believe that Hillary Clinton abused child, sex-slaves through satanic rituals in the basement of a New Jersey Pizzeria enough that you would share that fantasy with your family, friends, and coworkers, then I know of a former head of the Defense Intelligence Agency that you should talk to. The lesson is that no one, to include the most senior officers and leaders, is immune to the disinformation and everyone should be vigilant about how they come to believe something is true.

5. Radicalization. Not all social media is political and not everything political is bad. This may upset many senior leaders, who would prefer to remain apolitical, which is sometimes code for 'not my problem,' but we have to be leaders on and off-duty, in real life and in virtual life, because you're more likely to become engaged with both foreign and domestic enemies on the internet than in actual combat. There are too many blogs run by Soldiers

and other service members that are wrought with the worst types of sexism, racism, and bigotry, much like the port-a-johns at a combat training center. Since the information environment is open and accessible to our enemies, and they have cable news like most of us, they understand the social and cultural flashpoints just as much, if not more, than we do, because they are at least a few steps removed from them. The Internet Research Agency and others would be arsonists if they could, but since they don't live in our woods, they're just as content to light and throw a match elsewhere. A bear once told me that, "only you can prevent forest fires."

6. Deep fakes. Deep fakes are a wicked problem that is not likely to become any easier. It's nearly impossible to spot them. However, we must exercise restraint and suspend disbelief and judgment when confronted with a video that is potentially a deep fake. How can you tell the real from the fake and the fake from the real? It depends on how much time you are willing to spend doing research. A lack of history and a lack of context are often clues that you are watching a deep fake. If the speaker is talking out of context i.e. discussing the "deep state" and the "new world order" in what may be a high school commencement ceremony, then it might be a deep fake. Deep fakes should not be confused with highly edited videos, which combine elements of speech and video absent context to convince an unsuspecting and unvigilant audience of falsehoods.

7. Misquotes. People whose arguments lack substance often appeal to precedent, authority or celebrity. They will quote T.S. Elliot, Ernest Hemingway, Thomas Jefferson, or George Washington, etc. Obviously, these notable ghosts of departed wisdom observed, opined and wrote about issues of their day. If you notice a quote that is just too poignant to be believed, or that there is a word within the quote that just does not appear commensurate with the era in which the quoted person lived, there is a chance it is a misquote. Misquotes are often placed within a meme which includes the face of the misquoted person. This is both persuasive and cleverly deceptive. Do research. When in doubt, pick up an old book, and do more research.



8. Grammar. Recognizing poor grammar can prevent enemy infiltration. Seriously. English is not the first or second language for many of our enemies. Pay close attention to unusual grammar or syntax errors, mismatched vernacular, or colloquialisms in articles, blogs, and memes. For example, in baseball there are points and they are referred to as “runs,” and if someone referred to them as “goals,” you would ask if they had actually ever played baseball, or in this case, if English was their first language. The enemies’ language skills are not as good as their computer skills. However, this is becoming more challenging since text messaging seems to be converting to hieroglyphics and phonetic spelling.

9. Satire. If the story, image or meme appears just too satirical or ironic to be believed, then you have likely been duped by the Internet Research Agency. That’s the point! It’s bold, disrespectful and designed to add insult to injury. At this point, the Russian strategy continues despite the risk of discovery - they have already seized and retained the initiative in the narrative space and information environment. Embarrassment and humiliation are the exploitation and they are truly victorious when their enemy (us) normalizes hypocrisy.



GEN Abrams recently and correctly stated that leaders should [get on social media](#). However, initiative, in this case, may be dangerous if not disciplined through education. Much like basic fieldcraft, Soldiers and leaders must hone the skills that will help them survive in a dangerous information environment. They must understand how to tell if a source is bogus or credible by becoming internet literate. Meanwhile, Soldiers and leaders must ensure they do not do the enemy's work for them by spreading or sharing disinformation. Soldiers and leaders must also understand that you can likely spot a baseless conspiracy theory by how easily the story is told and by its uncompromising allegiance to ridiculousness and stupidity. Finally, we all must learn how to enjoy the internet and social media's endless possibilities without suffering from its and our vulnerabilities. Senior leaders do well at hyping up the difficulties with multi-domain operations, but more leaders need to understand and describe the threats within the information environment at home, which, ironically enough, are the same in the information environment abroad. We will not win in the information environment if we do not first prevent ourselves from losing.

*Maj. Larry Kay is an Infantry Officer in the United States Army and is currently assigned as the Operations Officer for 1st Battalion, 18th Infantry Regiment (Vanguards), 2nd Armored Brigade Combat Team, 1st Infantry Division. Maj. Kay is a graduate of the Command and General Staff College and the School of Advanced Military Studies. He is the author of*

*“Making Sense of the Senseless: War in The Postmodern Era.” Follow him on Twitter [@larrykay954](#).*

*The views expressed are those of the author and do not reflect the official position of the 1<sup>st</sup> Infantry Division, the United States Army, Department of the Army, or Department of Defense.*

### **Share this:**

- [Email](#)
- [Tweet](#)
- 
- [Print](#)
- [WhatsApp](#)