2016

Is Social Media a Threat or Can It Be a Trusted Agent?

William Ward
University of Nebraska at Omaha, wward@unomaha.edu

Katherine Cole-Miller
University of Nebraska at Omaha, scolemiller@unomaha.edu

Ann Fruhling
University of Nebraska at Omaha, afruhling@unomaha.edu

Kathryn M. Cooper
University of Nebraska at Omaha, kdempsey@unomaha.edu

Is Social Media a Threat or Can It Be a Trusted Agent?

WD Ward[1], KS Cole-Miller[2], A Fruhling[3], and K Dempsey-Cooper[4]

[1, 2]*College of Business Administration*
University of Nebraska, Omaha
E-mail: wward@unomaha.edu; scolemiller@unomaha.edu

[3, 4]*College of Information Science and Technology*
University of Nebraska, Omaha
E-mail: afruhling@unomaha.edu; kdempsey@unomaha.edu

Abstract: *There is a prevailing belief within the United States Department of Defense (DOD) that social media is a threat to national security, leading to restrictions in workplace use of social-media applications. However, instead of dismissing social media as a threat, leaders should be asking whether or not the information received via social media can be trusted, thus leveraging the information-sharing capabilities of social media. This article presents a theoretical case for quantifying social media trustworthiness by exploring the factors that influence trust in social media and proposing a trust framework to be used to quantify trustworthiness.*

Keywords: *Decision Making, Social Media, Trust*

Disclaimer: The views expressed are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

Introduction

According to the last major U.S. Department of Defense (DOD) release of guidelines for secure social media use, there is a prevailing belief that social media is a threat to national security, particularly threats associated with phishing, social engineering and web application attacks (Council, CIO 2009). The concern for maintaining security on U.S. DOD information systems led to the release of these guidelines for social media use that has resulted in some DOD workplaces to restrict use of social-media applications such as Facebook and Twitter. As of January 2016, a search of the *DOD Social media hub* revealed no change to US DOD policy since the 2009. Policy updates have maintained the same perspective that social media remains a threat to national security.

The concern for security is based, in part, on occurrences and impacts of users' social media accounts being hacked. For example, on 23 April 2013, the Associated Press's (AP) Twitter account released a 'tweet' (a 140-character or less social media message) falsely stating that there had been two explosions at the White House and that President Obama had been injured. Within 2 minutes, the tweet had reached U.S. stock traders and the Dow Jones dropped over 143 points (a

$136.5 billion loss). The Syrian Electronic Army had hacked the AP's Twitter feed and released the 'bogus' headline. Although the tweet was discovered to be erroneous and taken down within minutes, the damage was done. Traders on Wall Street and national security analysts were reminded of how fast information can spread via social media and how great the impact of believing false information can be (Foster 2013).

While concern for the security of information systems regarding social media is warranted, it is short-sighted to simply consider social media a threat. In many cases social media can be considered helpful and trustworthy. Facebook has been credited with helping to find a kidnapped new-born from a Quebec hospital. Because information about the kidnapping had been posted to Facebook, four teenagers were able to identify and locate the kidnapper and baby within hours (Kelly 2014). Such occurrences suggest that rather than dismissing social media and perceiving it as a threat, individuals, companies, and governments should be asking how they can determine whether or not the information received via social media can be trusted, thus allowing them to leverage the information sharing capabilities of social media.

The aim of this article is to explore the relationship between the trust precursors for social media and overall trustworthiness of social-media information. The end result is a proposed trust framework that can be used to quickly evaluate the trustworthiness of information received via social media to aid senior leader decision making. Because trusting social-media information introduces another level of uncertainty into a leader's decision-making process, it is necessary to think through uncertainties in a way that allows a senior leader to understand how the uncertainties will impact an outcome (Hammond, Keeney & Raiffa 1999). This trust framework is only an initial concept; however, efforts to refine the trust framework may lead to tools that will help senior leaders assess how trusting particular social-media information will affect their decisions. While the intended audience is US DOD decision makers and those doing research to enable their decision making, this concept could have broad global benefits as well.

Based on a review of the literature, research conducted to date has either focused on trust using only one social-media application (Lucassen & Schraagen 2010; Lucassen & Schraagen 2011; Shen, Cheung & Lee 2013; Rowley & Johnson 2013; Mendoza, Poblete & Castillo 2010) or a particular domain's website (Kim, Ferrin & Rao 2008; Harris, Sillence & Briggs 2011; Moturu & Liu 2011; Costante, den Hartog & Petkovic 2011). Thus, there is a need for more research to take a closer look at the trust factors for social media as a whole and how those factors influence decision making. A comprehensive examination and measurement of the various trust factors is necessary because some factors may have different effects depending on the situation. As a result of this research, an initial list of trust factors have been compiled that can be applied more generally to any social media outlet (existing or future) and used in a holistic trust framework to assist senior leadership decision making.

In the next sections, the article begins by defining the terms 'social media' and 'trust'. Second, it describes each attribute of the framework based on previous literature. Then, it proposes how the framework can assist senior leaders who may be interested in including social-media information as part of their data gathering. The article concludes with recommendations of future areas for research.

Definitions

Before beginning a discussion of the precursors for trust of social media, it is necessary to have a common understanding of what is meant by the terms 'social media' and 'trust.' Having a shared understanding is important because this will provide the foundation for the precursors and frameworks presented in the following sections. 'Social media' and 'trust' are defined based on publically available (both academic and US DOD) resources.

Social media

While several aspects of social media can be found and defined in various sources, a consolidated, agreed upon definition of social media does not currently exist. For example, the US DOD has established the *DOD Social media hub* web page (DOD Social media hub), but it still lacks a common definition of social media.

The social media definition presented below combines definitions from various sources to define social media for this study. The following is a sample of the definitions reviewed. Social media has been defined as a set of technologies that "support interpersonal communication and collaboration using Internet-based platforms" (Kane *et al.* 2014). Functionally, "social media refers to the interaction of people and also to creating, sharing, exchanging and commenting contents in virtual communities and networks" (Ahlqvist *et al.* 2008). Social media is also made up of applications that inherently connect people and information in spontaneous, interactive ways (Council, CIO 2009). Specifically referencing the implementation of social media for information exchange, Kaplan and Haenlein (2010) noted that these platforms lean "on the ideological and technological foundations of Web 2.0, and allow the creation and exchange of User Generated Content". Air Force Instruction (AFI) 35-113 states that social media includes, but is not limited to, weblogs, message boards, video sharing, and other media sharing websites (Air Force Public Affairs Agency 2010).

After an extensive review of the literature and of current government policies, the following definition for social media is presented: a set of Internet technologies that allows for interpersonal communication and collaboration, is made up of applications that interactively connect people and information, and allows for the creation and exchange of user-generated content**.** This definition is the foundation to evaluate trust precursors using a variety of social media-applications, including (but not limited to) applications that allow users to add, delete, or modify content (wikis); websites that allow for user reviews and feedback; and blogs and microblogs (such as Twitter).

Trust

While there has been considerable research on trust, there is little agreement on the definition of trust in the context of social media venues (Rowley & Johnson 2013). An initial review of the historic literature revealed four different levels of trust for researchers to consider: individual, relational, societal, and interpersonal (Kelton, Fleischmann & Wallace 2008). Of these four levels, research indicates that interpersonal trust is the appropriate category in which to discuss digital trust because it represents the "social tie directed from one actor to another" (Kelton, Fleischmann & Wallace 2008) and is the category most appropriate for this article.

'Interpersonal trust,' the most common category for discussing trust, refers to the relationship between a trustee and a trustor (Mayer, Davis & Schoorman 1995). Early research defined interpersonal trust as the "expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon" (Rotter 1967). It has also been defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectations that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer, Davis & Schoorman 1995). The first definition addresses the trustor's belief that the trustee will perform as stated. The second definition adds the lack of control that the trustor has over the trustee. While various researchers have cited both definitions, one key attribute appears to be missing: the trustor's *intent* to act based on the information provided by the trustee. Intention to act is imperative to the discussion of trust, because any proposed framework should be used to enable senior leaders to pursue a particular course of action based on the trustworthiness of the information.

A 2013 study took a similar stance regarding the willingness to act on social-media information in its trust definition: "trust in digital information indicates a positive and verifiable belief about the perceived reliability of a digital information source, leading to an intention to use" (Rowley & Johnson 2013). This definition finds its foundation in the trust research cited earlier, but it also captures the essence of action. If a senior leader is not expected to act on a particular piece of information, it does not matter how much he or she inherently trusts it. For these reason, this is the definition selected for this research.

Trust Precursors

With these definitions in place, next the precursors of trust are considered. Some have argued earlier research has focused too narrowly by only considering precursors under the specific umbrella of the domain being researched. This creates a challenge for future researchers, as it requires them to modify the definitions to apply to different forms of social media. Therefore, in order to provide a comprehensive tool to evaluate the factors that influence a leader's trust, it is recommended that a holistic approach to creating a framework that uses a broad enough spectrum of precursors that may be applied (in varying degrees) to all forms of social media is used.

Trust precursors background

This section summarizes the literature on trust precursors. Early research examining social media trust precursors were based on websites such as e-commerce (Kim, Ferrin & Rao 2008; Harris, Sillence & Briggs 2011) and e-Health websites (Harris, Sillence & Briggs 2011; Moturu & Liu 2011; Costante, den Hartog & Petkovic 2011) that incorporate user review and feedback. While the U.S. DOD is unlikely to depend on these websites for decision making, the precursors identified are still relevant to social media as a whole. Research in e-commerce identified four categories of trust precursors: cognition-based (information quality, perceived privacy protection, and perceived security), effects-based (for example, reputation, referrals, buyers' feedback), experience-based (familiarity and Internet or e-commerce experience), and personality-oriented (disposition to trust and shopping style) (Kim, Ferrin & Rao 2008). Some of these factors, such as information quality, can be carried over into the broader context of trust in social-media information. Other factors, such

as perceived privacy protection and buyers' feedback, are specific to e-commerce and are not included as precursors.

Research in e-Health websites identified information quality, personalization, and impartiality as important precursors to trust (Harris, Sillence & Briggs 2011). Additionally, research has shown that threat (information the user may not want to hear) and corroboration (ability to find additional information that says the same thing) also influences trust (Harris, Sillence & Briggs, 2011). Harris, Sillence and Briggs (2011) also noted that impartiality actually plays a larger role in e-Health than in e-commerce.

Wikipedia is another website that has been the subject of significant research regarding trust. Wikipedia is a wiki website, a web application that allows users to add, remove, or modify content. Because any user of Wikipedia can change content at any time, researchers have looked at how users evaluate the accuracy of Wikipedia information (Lucassen & Schraagen 2010; Lucassen & Schraagen 2011; Shen, Cheung & Lee 2013; Rowley & Johnson 2013). Precursors such as information quality (completeness, accuracy, and currency) and format play an important part in how users evaluate the accuracy of the Wikipedia information (Shen, Cheung & Lee 2013). The U.S. DOD uses wikis internally to share information internally with other U.S. DOD members and as an open source data mining tool (Mergel 2011).

Along with wikis, blogs and microblogs have also become more prevalent. Twitter is a popular example of a microblog, a much smaller version of a blog (short for web log). In Twitter's case, currently only 140 characters can be used to convey a message. Researchers of Twitter have identified precursors such as reputation (number of followers), recommendations (number of retweets), and user knowledge (use of twitter hashtags) as important precursors to trust (Mendoza, Poblete & Castillo 2010). Grammar and format on Twitter are typically truncated due to space. Therefore, precursors such as style do not have as great an impact on trustworthiness when the information is limited to 140 characters.

In order to organize the various precursors under a manageable trust framework, a list of categories was created to form a common baseline. Common terms were manually reviewed from the literature review (using both listed precursors and definitions) to create these categories. The newly established common categories became the precursors used in the proposed trust framework. The recommended categories are: Information Quality, Personality, Recommendations, Style, User Knowledge, Security, Usability, and Risk. The categories, precursors, and research sources are summarized in **Table 1**, below.

Category / Source	Information Quality	Personality	Recommendations	Style	User Knowledge	Security	Usability	Risk
Costante 2011	Reliability and Availability Third Party Seals Reputation Brand Name	Disposition of Trust		Quality and Look and Feel	User's Knowledge	Security	Usability	Risk
Harris 2011	Information Quality Impartiality Credible Design	Personalization						
Kane 2014	Authenticity		Third Party Contributions	Profile Content				
Kelton 2008	Reputation Competence Context	Propensity to Trust	Confirm with Multiple Sources Recommendations		Experience with Source	Standards and controls		Vulnerable
Kim 2008	Information Quality Third party seals Positive Reputation	Consumer Disposition of Trust			Familiarity			
Li 2008	Cognitive	Personality			Knowledge			Calculative
Lucassen 2011	Source Experience				Domain Experience Information Skills			
Mayer 1995	Integrity	Benevolence			Ability			
Moturu 2011	Reputation Performance			Appearance				
Shen 2013	Completeness Accuracy Currency Credibility			Format				

Table 1: Literature review of trust precursors

Proposed trust precursors

In this section each of the trust precursors and their definition with respect to the social media environment are presented, beginning with Information Quality.

Information quality

Information Quality is a cognitive-based trust factor "associated with [a user's] observations and perceptions" (Kim, Ferrin & Rao 2008). Information Quality itself refers to the "general perception of the accuracy and completeness of … information" (Kim, Ferrin & Rao 2008). These perceptions can be formed based on the credibility of the source of the information (Shen, Cheung & Lee, 2013), the individual's trust in the website where the information is posted (Li, Hess & Valacich 2008), or the information itself (Kelton, Fleischmann & Wallace 2008) (see **Figure 1**, below). Thus, based on these definitions, 'credibility', 'reputation', and 'content' are considered the three sub-factors for Information Quality. The following defines each sub-factor of Information Quality.

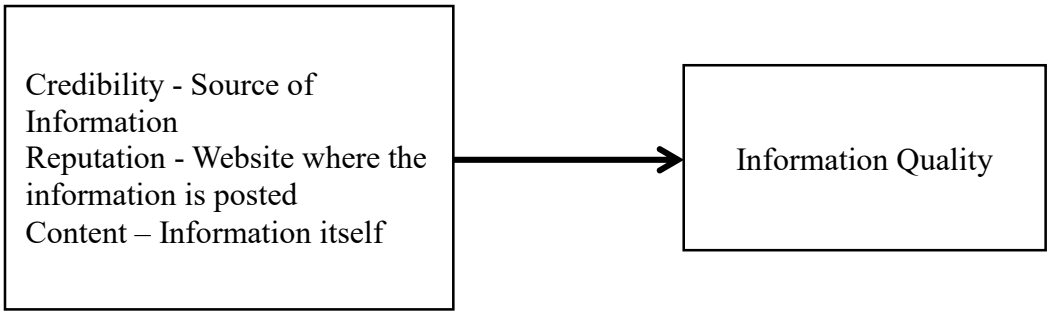

Figure 1: Information quality subfactors

Information quality sub-factor: credibility

The first sub-factor, credibility is "a recipient's perception of the believability of an information source" (Shen, Cheung & Lee 2013). Referring back to the AP Twitter hack, individuals reading the headline could reasonably assume the source was credible because the Associated Press is an independent, non-profit news-gathering repository that the majority of mainstream media uses for its breaking news. Source Credibility differs from Reputation because the source is believed to be credible (or not) regardless of the form of media used.

Information quality sub-factor: reputation

The second sub-factor, reputation, represents how others report their experiences with a website or social-media application (Costante, den Hartog & Petkovic 2011). With limited first-hand experience, a leader may believe a website with a good reputation is trustworthy (Li, Hess & Valacich 2008). For example, if a leader has limited experience with a website or application, but his or her trusted advisors have positive experiences using it, the leader might deem the website or application trustworthy.

Information quality sub-factor: content

Content is the third sub-factor. It refers to the information itself. Is the information relevant ("the degree to which the information matches the requirement of the user" [Kelton, Fleischmann & Wallace 2008]), complete ("degree to which the information source provides all necessary content"), accurate ("perceptions that the information is correct"), and current ("perceptions of the degree to which the information is up-to-date and timely") (Shen, Cheung & Lee 2013)?

Personality

The next trust precursor is Personality. Personality refers to interpersonal trust or the "expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual group can be relied upon" (Rotter 1967)—in other words, the individual's inclination to trust something or someone (Rotter 1971). Research on the psychological factors of trust has indicated that individuals possess stable personality characteristics influencing the willingness to trust (Rotter 1971). When an individual's propensity to trust is high, he or she is more likely to trust information.

Recommendation

The third precursor to trust is recommendation. Since social media, by definition, uses user-generated content, many websites and applications depend on recommendations to spread information. Whether it is through user reviews on an e-commerce website (Kelton, Fleischmann & Wallace 2008) or a re-tweet of a headline on Twitter (Mendoza, Poblete & Castillo 2010), recommendations have a high level of influence on the level of trust. For example, researchers reviewed the spread of information about the Chilean earthquake via Twitter. They found that social media users questioned false rumours far more frequently than confirmed truths, posting tweets refuting false rumours and thus adding validity to confirmed truths, thus creating a collaborative filter (Mendoza, Poblete & Castillo 2010).

Another example involving the recommendation precursor is an existing "fact-finding tool designed to jointly assess both the credibility of information and the reliability of sources" called Apollo (Schaffer *et al.* 2014). Apollo "computes the credibility of [a source's] claims given their degree of corroboration, and the credibility of sources given credibility of their claims" (Schaffer *et al.* 2014).

Style

In the context of this research, the precursor style is defined as the manner in which information is presented. For instance, Wikipedia research has evaluated how grammar and sentence structure affect trust (Shen, Cheung & Lee 2013). Users have more confidence in a Wikipedia article that follows the approved format and contains good grammar and sentence structure (Shen, Cheung & Lee 2013). However, other applications that follow a different rule set are viewed and evaluated differently. Twitter is used to spread information using only 140 characters or less; thus, there is more flexibility on style. Style can affect the way a user perceives the quality of the information presented (Costante, den Hartog & Petkovic 2011); however, the extent that this affects trust depends on the website and/or the application used.

User knowledge

The user knowledge factor is an important precursor to trust because an individual's understanding of a particular social-media application can influence his or her level of trust in a piece of information. For user knowledge, a leader's expertise in the particular subject area (*Domain Expertise*) (Lucassen & Schraagen 2011) and his or her familiarity with the application being used (*Experience*) both significantly affect a leader's willingness to trust the information (Kelton, Fleischmann & Wallace 2008).

User knowledge sub-factor: domain expertise

Domain expertise is a volatile precursor to trust. Experts approach problems differently than novices. A novice focuses on concrete surface characteristics (for example, grammar in a Wikipedia article) while an expert focuses on more abstract qualities (for example, how well the Wikipedia article describes facts about a particular field) (Lucassen & Schraagen 2011). A leader receiving information that he or she has expertise in will be able to use that expertise to further determine their perceived level of trust.

User knowledge sub-factor: experience

The precursor experience refers to an individual's familiarity with a particular social-media application. If leaders have little experience with a particular social-media application, they must depend more heavily on other precursors to determine trust. Once they have experience with a particular application, they begin to develop a perception (positive or negative) of trust towards the application. Experience can eventually influence the reputation precursor, for example, when leaders' experiences becomes public knowledge through feedback (Kelton, Fleischmann & Wallace 2008). While experience and reputation appear to be similar, experience is internal to a user, while reputation is an external input to a user (for example, senior decision makers or senior leaders).

Security

Security is becoming more and more important as a precursor that influences trust. Security refers to the specific protection controls that are in place, such as a secure login and encrypted data (Costante, den Hartog & Petkovic 2011). For example, shortly after the AP's Twitter feed was hacked, Twitter instituted a two-factor authentication (Moore & Roberts 2013). Two-factor authentication uses a second check beyond just the login and password when accessing an account. In Twitter's case, the user registers a phone number with Twitter. Whenever the user tries to log in, a six-digit code will be sent via text message to the phone number. This code must then be entered before the user can access his or her account (O'Leary 2013). Websites with additional security features are likely to increase the level of trust in a particular social-media application.

Usability

Usability is "a quality attribute that assesses how easy the user interface is to use and how useful it is" (Nielsen 2003). Additionally, according to Costante, den Hartog, and Petkovic (2011), usability refers to how easy it is for a user (in this case, a senior leader) to meet his or her goals using the website or social-media application. Costante, den Hartog, and Petkovic (2011) observed that usability is of high enough importance that e-commerce and e-banking websites include features specifically to walk the user through various steps (like a 'wizard') to ensure ease of use. Costante, den Hartog, and Petkovic (2011) also observed that as the user's familiarity with the website increases, the importance of usability decreases.

Risk

The final precursor to trust involves the assessment of risk. Risk assessment can influence whether an individual chooses to trust user-generated information (Li, Hess & Valacich 2008). Users tend to trust a trustee when the user perceives the trustee has nothing to gain from others acting on the

information, or that the cost of not trusting the information overwhelms the benefit (Li, Hess & Valacich 2008). For a senior leader, not taking action on a piece of information may have greater consequences than taking the action. For example, assume a base commander receives a tweet notification that there is an active shooter. This tweet could be received before emergency notification systems are activated. The consequences of an active shooter being in the area are significantly high due to the level of risk; therefore, the commander cannot discount the information. Including this precursor allows for situations in which the senior leader must respond to information without additional corroborating data.

Trust Framework

Based on a thorough review of the literature, and using the precursors introduced in the previous section, the Trust Framework shown in **Figure 2**, below, is proposed. The trust precursors presented are believed to have the most likely impact on a leader's willingness to trust information that will be used to make a decision. This framework shows, in a graph format, how the different precursors can be used to quantify an overall trust score for social-media information. This trust score can be used to determine if certain social-media information should be included in the leader's decision-making process. Depending on the trust score, the information can be rejected as untrustworthy or accepted as trustworthy. If the information is considered trustworthy, it would become actionable information. It is recognized that some of these precursors will have a greater importance and impact than others, depending on the source of the information; thus, additional research will need to be conducted to develop an appropriate weight for each factor and information source.

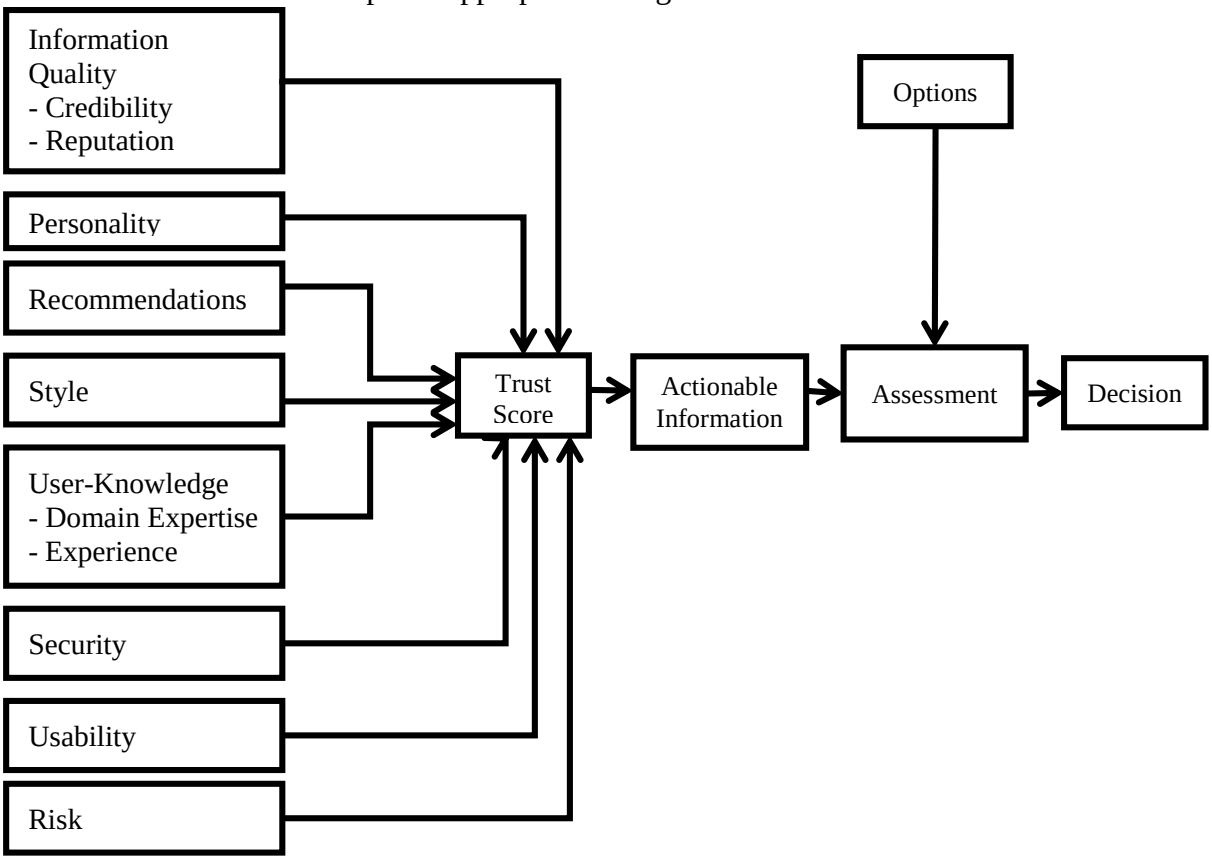

Figure 2: Trust framework

Once the information is considered actionable, the information would enter an assessment phase of decision making, which would introduce possible options or courses of action for the leader to consider. The final outcome of the assessment phase would be the leader's decision.

Conclusions

From this initial exploratory research, a list of trust factors was compiled that could be measured, scored, and combined to assist senior leader decision making. After the proposed framework has been validated through additional study, it is hoped it will be possible to develop tools that can determine trust scores for information feeding the decision-making process. The validated framework could also be used to evaluate trustworthiness of various social-media applications. Additionally, it could be used to improve instruments currently under development for automated analytical tools and further secure existing algorithms automating financial transactions (reducing the risk of another market crash caused by the AP Twitter hack). Each of these opportunities is expanded on below.

Social media 'information' scoring

This framework can be used to develop tools that can automatically determine a trust score for information from social media. Automated decision-making tools could use this trust score as a filter to prevent possibly erroneous information from negatively influencing decisions. Investment in this area of research could enhance senior leader decision making.

Social-media 'application' scoring

Because the US DOD has expressed concerns that certain social-media applications might present unacceptable risk to U.S. DOD networks (Council, CIO 2009), these factors can be applied to existing (and future) social-media applications as part of a cost-benefit analysis to narrow down which social-media applications should be used in U.S. DOD networks. Instead of using the framework to determine the trust score of the information, the framework could determine the trust score of the application itself, thus, providing additional analytical rigor behind what applications to allow on US DOD networks.

Developing automated analytical tools

Through the research, a study was discovered about an automated analytical tool that can be used to assess large amounts of open source data called Apollo (Schaffer *et al.* 2014). Technically, Apollo "considers non-independence relations between sources to discount rumours that are corroborated only within one social group. Once credibility values are computed, Apollo can rank the information based on credibility" (Schaffer *et al.* 2014). The Army Research Lab, in collaboration with the University of Illinois, Rensselaer Polytechnic Institute, and IBM, has already demonstrated some of the capabilities of Apollo (Le *et al.* 2011). In fact, Apollo combines two of the precursors proposed in this article to assess trustworthiness. The greater corroboration of a source's information (recommendation) adds to the overall perception of the source's believability (credibility). Further research could expand a tool like this to assess even more factors.

Stock market algorithms

Based on the earlier point made, one could question whether the proposed framework could have prevented the market crash following the 2013 AP Twitter hack. It is possible. Currently, high-frequency traders use a set of algorithms to sift through the Internet and make trading decisions based on this information (Matthews 2013). These algorithms caused the automatic selling of stock and created the sudden market drop. By using the framework and subsequent trust tools, the algorithms could be modified to prevent such sudden changes in the market. By establishing a trust score for the algorithm to use, knee-jerk reaction to untrue information could be reduced.

Every day individuals make decisions based on the information they receive. They rarely have a complete picture to consider when faced with any decision. Often the process is based on intuition. Individuals can sift through the information and determine what pieces of information they will trust, what is most relevant, and how comfortable they are with particular courses of action. But with the volume of information that is now easily available to senior leaders, the U.S. DOD needs the ability to assess the trustworthiness of this information to further assist leaders to make the right choices for national security. The proposed framework is an important first step toward leveraging the value and potential of social media for DOD decision-making.

Acknowledgements

The authors wish to thank the National Strategic Research Institute at the University of Nebraska and United States Strategic Command for establishing the United States Strategic Command Leadership Fellows Program that provided the opportunity to conduct this research.

References

Ahlqvist, T, Bäck, A, Halonen, M & Heinonen S 2008 'Social media roadmaps', Edita Prima Oy, Helsinki, Finland.

Air Force Public Affairs Agency 2010, 'Air Force Instruction 35-113', Air Force e-Publishing, <www.e-publishing.af.mil>.

Costante, E, den Hartog, J & Petkovic, M 2011, 'On-line trust perception: what really matters', *Socio-Technical Aspects in Security and Trust (STAST)*, 1st Workshop on IEEE, Milan Italy.

Council, CIO 2009, 'Guidelines for secure use of social media by federal departments and agencies', Federal CIO Council ISIMC NISSC, Web 2.0 Security Working Group.

DOD Social media hub, viewed January 2016, <http://www.defense.gov/socialmedia/>.

Foster, P 2013, '"Bogus" AP tweet about explosion at White House wipes billions off us markets', *The Telegraph*, 23 April 2013.

Hammond, J, Keeney, RL & Raiffa, H 1999, *Smart choices: a practical guide to making better life decisions*, Harvard Business School Press, Boston, MA, U.S.A.

Harris, PR, Sillence, E & Briggs P 2011, 'Perceived threat and corroboration: key factors that improve a predictive model of trust in internet-based health information and advice', *Journal of Medical Internet Research*, vol. 13, no. 3.

Kane, G, Alavi, M, Labianca, GJ & Borgatti SP 2014, 'What's different about social media networks? A framework and research agenda', *MIS Quarterly*, vol. 38, no 1.

Kaplan, AM & Haenlein, M, 2010 'Users of the world, unite! The challenges and opportunities of social media', *Business Horizons*, vol. 53 no. 1, pp. 59-68.

Kelly, A 2014 'Social media and quick-thinking teens save Quebec baby', *Global News*, 27 May 2014, viewed May 2014, <http://globalnews.ca/news/1356489/social-media-and-quick-thinking-teens-save-quebec-baby>.

Kelton, K, Fleischmann, K & Wallace, WA, 2008 'Trust in digital information', *Journal of the American Society for Information Science and Technology*, vol. 59, no. 3, pp. 363-74.

Kim, DJ, Ferrin, DL, & Rao, HR 2008, 'A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents', *Decision Support Systems*, vol. 44, no. 2, pp. 544-64.

Le, HK, Pasternack, J, Ahmadi, H, Gupta, M, Sun, Y, Abdelzaher, T, Han, J, Roth, D, Szymanski, B & Adali, S 2011, 'Apollo: towards factfinding in participatory sensing in Information Processing in Sensor Networks (IPSN)', *Proceedings of 2011 10th International Conference*, IEEE, pp. 129-130.

Li, X, Hess, TJ & Valacich, JS 2008, 'Why do we trust new technology? A study of initial trust formation with organizational information systems', *The Journal of Strategic Information Systems*, vol. 17, no. 1, pp. 39-71.

Lucassen, T, & Schraagen, JM 2010, 'Trust in Wikipedia: how users trust information from an unknown source', *Proceedings of the 4th Workshop on Information Credibility*, WICOW '10, pp. 19-26.

——2011, 'Factual accuracy and trust in information: the role of expertise', *Journal of the American Society for Information Science and Technology*, vol. 62, no. 7, pp. 1232-42.

Matthews, C 2013, 'How does one fake tweet cause a stock market crash?' *Time*, 24 April.

Mayer, RC, Davis, JH & Schoorman, FD 1995, 'An integrative model of organizational trust', *Academy of Management Review*, vol. 20, no. 3, pp. 709-34.

Mendoza, M, Poblete, B & Castillo, C 2010, 'Twitter under crisis: can we trust what we RT?', *Proceedings of the First Workshop on Social Media Analytics*, SOMA '10, pp. 71-79.

Mergel, I 2011 'Using Wikis in government: a guide for public managers', IBM Center for the Business of Government Using Technology Series, viewed May 2014, <www.business of government.org>.

Moore, H & Roberts, D 2013, 'AP Twitter hack causes panic on Wall Street and sends Dow plunging', *The Guardian*, 23 April.

Moturu, S & Liu, H 2011, 'Quantifying the trustworthiness of social media content', *Distributed and Parallel Databases*, vol. 29, no. 3, pp. 239-60.

Nielsen, J 2012, 'Usability 101: introduction to usability', Nielsen Norman Group, <www.nngroup.com>.

O'Leary, J 2013, 'Getting started with login verification' Twitter blogs, <www.twitter.com>.

Rowley, J & Johnson F 2013, 'Understanding trust formation in digital information sources: the case of Wikipedia', *Journal of Information Science*, vol. 39, no. 4, pp. 494-508.

Rotter, JB 1967, 'A new scale for the measurement of interpersonal trust', *Journal of Personality*, vol. 35, no. 4, pp. 651-65.

——1971, 'Generalized Expectancies for Interpersonal Trust', *American Psychologist*, vol. 26, no. 5, pp. 443-52.

Schaffer, J, Abdelzaher, T, Jones, D, Hollerer, T, Gonzalez, C, Harman, J & O'Donovan, J 2014, 'Truth, lies, and data: credibility representation in data analysis', *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), Proceedings of the 2014 IEEE International Inter-Disciplinary Conference*, pp. 28-34.

Shen, X, Cheung, C & Lee, M 2013, 'What leads students to adopt information from Wikipedia? an empirical investigation into the role of trust and information usefulness', *British Journal of Educational Technology*, vol. 44, no. 3, pp. 502-17.