Cybersecurity Policies and Their Impact on Dynamic Data Driven Application Systems

Conference Paper · September 2017

DOI: 10.1109/FAS-W.2017.175

4 authors, including:

Conrad Tucker

Pennsylvania State University

96 PUBLICATIONS **493** CITATIONS

SEE PROFILE

Cybersecurity Policies and their Impact on Dynamic Data Driven Application Systems

Conrad S. Tucker
Science and Policy Fellow
Brent Scowcroft Center on International Security
Atlantic Council
Washington, D.C., USA
ctucker@atlanticcouncil.org

Mathew Burrows
Director: Foresight, Strategy and Risks
Brent Scowcroft Center on International Security
Atlantic Council
Washington, D.C., USA
mburrows@atlanticcouncil.org

Kevin Lesniak
Data Scientist
Brent Scowcroft Center on International Security
Atlantic Council
Washington, D.C., USA
kevinalesniak@gmail.com

Samuel Klein
Program Assistant: Foresight, Strategy and Risks
Brent Scowcroft Center on International Security
Atlantic Council
Washington, D.C., USA
sklein@atlanticcouncil.org

***Abstract*—The objective of this paper is to explore how cybersecurity policies pertaining to data privacy, data acquisition, data fusion and data mining, impact the feasibility and functionality of Dynamic Data Driven Application Systems (DDDAS). In this work, a social media network model, will serve as the DDDAS of study in order to reveal how varying cybersecurity policies, could alter the functionality and usefulness of the system. At its fundamental level, the social media network model proposed in this work, TEchnology PHobia readiness CONdition (TEPHCON), seeks to serve as a decision support system that dynamically captures and visualizes society's affinity/aversion towards current or emerging technologies. However, at its core, this DDDAS is built upon a data platform that is highly susceptible to changes in cybersecurity policies. For example, a change in cybersecurity policies pertaining to freedom of speech in a cyber environment, may significantly alter the access and availability of publicly-available data. On the other hand, a more hands-off cyber policy pertaining to who controls cyber infrastructure networking speeds, may result in an imbalance of data that may threaten the veracity of TEPHCON. Therefore, cybersecurity policies are an integral component of DDDAS systems such as TEPHCON and as such, their impact should be explored in detail.**

Keywords—DDDAS; social media; text mining; data visualization; technology phobia;

I. CONTRIBUTIONS

Cybersecurity seeks to protect both hardware and software components of computer systems from theft, damage, disruption, misdirection, and unintended use [1]. Policy makers have a direct impact on the success of cybersecurity efforts, as a stringent or lenient cybersecurity policy, could be the deciding factor in determining society's trust in cyber systems. Dynamic Data Driven Application Systems (DDDAS) inherently rely on a strong cyberinfrastructure that is robust against cybersecurity threats. Formally defined, DDDAS dynamically incorporate measurement data into a system's execution model in order to improve the accuracy or the speed of the model, with the execution model having the ability to control the measurement process [2]. From the definition of DDDAS, it can be seen that cybersecurity policies could impact DDDAS' ability to be *dynamic*, incorporate *measurement data*, and advance *execution models*.

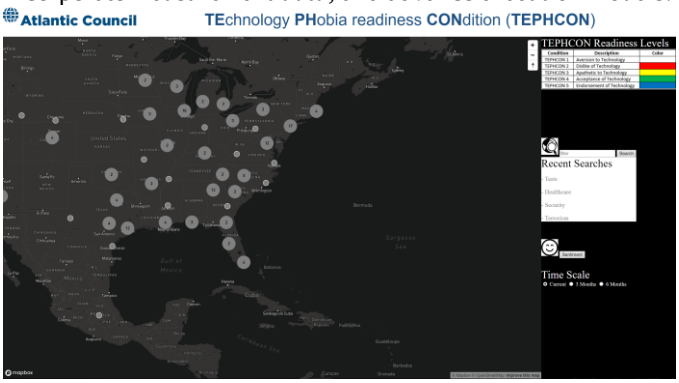

Figure 1: Visual Example of the TEPHCON Platform

The DDDAS model proposed in this work (Figure 1), TEchnology PHobia readiness CONdition (TEPHCON), is a data acquisition, data synthesizer, data mining and data visualization platform that seeks to serve as a decision support tool for assessing society's phobias (or lack thereof) towards current and future technologies. The readiness levels quantified within the TEPHCON platform are analogous to the Department of Defense's DEFense readiness CONditions

(DEFCON), with TEPHCON 5, being the lowest phobia level (i.e., affinity) of a given technology, and TEPHCON 1, being the highest phobia level (i.e., aversion) of a given technology. Here, the term *technology* is used in a general sense to include man-made hardware (e.g., smartphone) and software (e.g,. social media app) products across a wide range of domains.

A conceptual model of TEPHCON is presented in Figure 2 and includes the variable definitions and structure of data that is acquired and synthesized in this work. Given a total of *N* publicly-available sources of social media data:

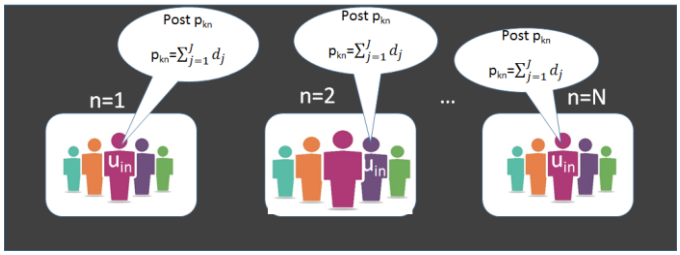

Figure 2: TEPHCON Conceptual Outline

- *n:* represents a publicly-available source of data (e.g., a publicly-available social media network such as Twitter) that contains data pertinent to TEPHCON (*n=1*,…, *N*)
- u_{in}: represents a user *i* of social media network *n*
- p_{kn}: represents a post *k* generated by one of the users of social media network *n*
- d_j: represents a data type (textual, image, geospatial, etc.) that is contained within a social media user *i's* post (*j*=1,…*J*)

Based on the data generated within large scale social media networks, data-driven models can be created that serve as decision support systems. For example, using the textual data expressed by a social media user in their post p_{kn} , a sentiment of a post can be quantified by employing algorithms such as Sentistrength [3]. I.e., when post p_{kn} contains a textual data type d_j= [w_1, w_2,…,w_W], where w_i represents a word or emoticon, the Sentistrength algorithm would transform a textual phrase into a sentiment score [3].

The first objective of the TEPHCON platform is to separate *relevant* data (i.e., a specific topic of interest) from *irrelevant data* (i.e., all other data) by employing query filtering methods. With the time stamped *relevant* data, sentiment mining algorithms are employed to the different data types in order to provide a real time assessment of society's phobia level, given a specific topic of inquiry. This data is then visualized for decision support (Figure 1). Using the conceptual outline of TEPHCON and its associated data structures, several scenarios pertaining to cyber policies are presented in order to demonstrate how DDDAS systems such as TEPHCON may be impacted.

Cyber Policy Impacting the *Dynamic* Nature of DDDAS

- Hypothetical Cyber policy #1: *Providers of cyberinfrastructure have the authority to provide varying data speeds to access different data repositories, based on their economic objectives.*

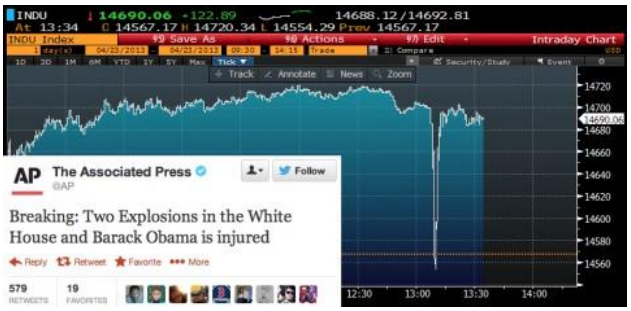

Figure 3: Twitter Hack of the Associated Press Account and the Corresponding Stock Market Plunge [4]

On April 23, 2013, the official Twitter account of the Associated Press was hacked, sending the message "**Breaking: Two Explosions in the White House and Barack Obama is injured**" to its more than 2 million Twitter followers [4]. The economic ramifications of this cybersecurity breach were almost instantaneous, with the stock market losing approximately $136 Billion dollars in value (Figure 3), before correcting itself after another message was sent out informing everyone of the cybersecurity breach.

Given that this cybersecurity breach occurred on one of the social media platforms that could potentially be used as a TEPHCON data source, the question is: how resilient is TEPHCON to misinformation that could potentially threaten users' trust in the veracity of the system? In order to maintain trust, the DDDAS *execution model* must be able to:

- Detect misinformation generated within the data source
- Minimize the time needed to detect misinformation
- Automatically correct/quarantine/delete misinformation

Given the above scenario, let us assume that there exists three unique social media users from two separate social media platforms outlined in Figure 2, where *n=1* contains one user and *n=2* contains two users. Let us also assume that social media platform *n=1* has an existing financial partnership with the cyberinfrastructure provider that enables communication to and from this social medial network, enabling their users to achieve the highest possible data transmission rates. Users of social media platform *n=2* do not have a financial relationship and hence, their data transmission speeds are throttled, in order to give priority to users of social media platform *n=1*. When the Associated Press' Tweet about an explosion at the White House is first disseminated (i.e., at time *t=0*), the probability that the information is indeed true is relatively high, given the reputation and prestige of the source (i.e., the Associated Press). In other words:

$p(\text{bombing at the White House=True} \mid \text{Source=Associated Press}) \geq \beta$

Where β is the threshold for which information is deemed to be true. At time t>0, the objective of a resilient DDDAS would therefore be to ensure the veracity of each piece of information that is disseminated in a timely and efficient manner, especially one that has the potential to instantaneously reach 2 million other users, as is in the case of the Associated Press cybersecurity breach.

Figure 4: 3 different users sharing pictures on social media

In order to falsify the claim of the White House bombing, Figure 4 presents a scenario where 3 images captured by 3 different individuals are shared on different social media networks, moments after the Associated Press cybersecurity breach. Assuming that these three messages were generated within the vicinity of the White House, image 1 that shows a litter of puppies, would do little to reduce the *p(bombing at the White House=true)*. Furthermore, due to the fact that the user of this social media network exists in *n=1* (i.e., the social media network that has a financial partnership enabling faster, priority data sharing), the image from user 1 may be captured by TEPHCON before images 2 (i.e., Northern facade of the White House) and image 3 (i.e,. Southern facade of the White House). For users of social media network *n*=2, the other two images (Northern facade of the White House and Southern facade of the White House) which may actually help decipher whether the Associated Press Tweet is indeed false, may be delayed in terms of data transmission due to the lack of existing partnerships established between *n=2* and the cyberinfrastructure provider. In both images showing the White House, it can be clearly seen that there is no damage done to the infrastructure, hereby bringing into question the news story disseminated by the Associated Press. Bodnar et al. have proposed algorithms aimed at increasing the veracity of information that is disseminated in online social media networks, based on a proposed user trust network [5]. As cyber policies change however, there is an ever-increasing need for novel and robust algorithms that enable DDDAS to maintain their dynamic characteristics.

Cyber Policy Impacting the *Execution Models* of DDDAS

- Hypothetical Cyber policy #2: *Posts by users of social media may be deemed hate speech/speech inciting violence and may be admissible as evidence in court.*

The balance between freedom of speech and national security is an intricate one. While freedom of speech is a fundamental component of free societies, there is a risk that certain speech has the potential to incite violence or be used as terrorist propaganda. Looking at the example in Figure 4, we observe that in addition to the images shared by each of the social media users, a corresponding textual message is also sent. A cyber policy that exposes a social media user to potential legal liability for their posts, may severely limit the quality and quantity of data that is generated within social media networks, hereby potentially diminishing TEPHCON's ability to serve as a real time visual decision support tool that reflects the views of a significant portion of society. For example, the message accompanying the "Northern façade of the White House" reads [*join me in protesting these new policies*], which may in some cases, be viewed as an attempt to incite a rally/protest. Similarly, the message accompanying the "Southern facade of the White House" reads [*I wonder how far I would make it if I jumped the fence?*], a hypothetical question, but however, a question that could be perceived as a preemptive attempt to cause a national security incident. While the textual messages of these users may be concerning, the actual images that they share of the White House being safe from the threat of a bomb, has the potential to separate misinformation from true information (e.g., the Associated Press Twitter breach). A cybersecurity policy that threatens the freedom of speech, may have resulted in the social media users who posted pictures of the White House, to have abstained from posting altogether due to fear of being criminally prosecuted due to their hypothetical statements.

II. Results and Conclusion

The cybersecurity examples presented in this work illustrate how DDDAS systems such as TEPHCON, could potentially be significantly impacted, based on the cyber systems and data policies adopted by a society. The examples demonstrate how the dynamic nature of DDDAS systems could be altered, simply based on a cyber infrastructure policy pertaining to network management and data prioritization. In addition, the quantity and quality of data available for DDDAS systems such as TEPHCON, could be adversely affected due to the cybersecurity policies pertaining to freedom of speech, liability assignment given a cybersecurity incident, etc. These and other cyber security policies are integral to the real-world feasibility of DDDAS systems such as TEPHCON.

Acknowledgment

This research is funded by the Atlantic Council. Any opinions, findings, or conclusions found in this paper are those of the authors and do not necessarily reflect the views of the sponsors.

References

[1] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst. Man Cybern.-Part Syst. Hum.*, vol. 40, no. 4, pp. 853–865, 2010.

[2] A. Aved, F. Darema, and E. Blasch, *Dynamic data driven application systems*. 2014.

[3] M. Thelwall, "Heart and soul: Sentiment strength detection in the social web with sentistrength," *Proc. CyberEmotions*, vol. 5, pp. 1–14, 2013.

[4] "Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism? - The Washington Post." [Online]. Available: https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.9d30b5901b86. [Accessed: 26-Jul-2017].

[5] T. Bodnar, C. Tucker, K. Hopkinson, and S. G. Bilén, "Increasing the veracity of event detection on social media networks through user trust modeling," in *Big Data (Big Data), 2014 IEEE International Conference on*, 2014, pp. 636–643.