A publication of ISCA*:
International Society for Computers
and Their Applications

INTERNATIONAL JOURNAL OF COMPUTERS AND THEIR APPLICATIONS

TABLE OF CONTENTS

*** "International Journal of Computers and Their Applications is abstracted and indexed in INSPECT and Scopus."**

Volume 26, No. 4, Dec. 2019 **ISSN 1076-5204**

International Journal of Computers and Their Applications

A publication of the International Society for Computers and Their Applications

EDITOR-IN-CHIEF

Dr. Gordon Lee, Professor Emeritus
Department of Electrical & Computer Engineering
5500 Campanile Drive
San Diego State University
San Diego, CA 92182-1326, USA
Email: glee@sdsu.edu

CO-EDITOR-IN-CHIEF

Dr. Ziping Liu, Professor
Department of Computer Science
One University Plaza, MS 5950
Southeast Missouri State University
Cape Girardeau, MO 63701
Email: zliu@semo.edu

ASSOCIATE EDITORS

Dr. Hisham Al-Mubaid
University of Houston
Clear Lake, USA
hisham@uhcl.edu

Dr. Antoine Bossard
Advanced Institute of Industrial Technology
Tokyo, Japan
abossard@aiit.ac.jp

Dr. Mark Burgin
University of California,
Los Angeles, USA
mburgin@math.ucla.edu

Dr. Sergiu Dascalu
University of Nevada
Reno, USA
dascalus@cse.unr.edu

Dr. Sami Fadali
University of Nevada, USA
fadali@ieee.org

Dr. Vic Grout
Glyndŵr University
v.grout@glyndwr.ac.uk

Dr. Yi Maggie Guo
University of Michigan,
Dearborn, USA
hongpeng@brandeis.edu

Dr. Wen-Chi Hou
Southern Illinois University, USA
hou@cs.siu.edu

Dr. Ramesh K. Karne
Towson University, USA
rkarne@towson.edu

Dr. Bruce M. McMillin
Missouri University of Science and Technology, USA
ff@mst.edu

Dr. Muhanna Muhanna
Princess Sumaya University for Technology
Amman, Jordan
m.muhanna@psut.edu.jo

Dr. Mehdi O. Owrang
The American University, USA
owrang@american.edu

Dr. Xing Qiu
University of Rochester, USA
xqiu@bst.rochester.edu

Dr. Juan C. Quiroz
Sunway University, Malaysia
juanq@sunway.edu.my

Dr. Abdelmounaam Rezgui
New Mexico Tech, USA
rezgui@cs.nmt.edu

Dr. James E. Smith
West Virginia University, USA
James.Smith@mail.wvu.edu

Dr. Shamik Sural
Indian Institute of Technology
Kharagpur, India
shamik@cse.iitkgp.ernet.in

Dr. Ramalingam Sridhar
The State University of New York at Buffalo, USA
rsridhar@buffalo.edu

Dr. Junping Sun
Nova Southeastern University, USA
jps@nsu.nova.edu

Dr. Jianwu Wang
University of California,
San Diego, USA
jianwu@sdsc.edu

Dr. Yiu-Kwong Wong
Hong Kong Polytechnic University,
Hong Kong
eeykwong@polyu.edu.hk

Dr. Rong Zhao
The State University of New York at Stony Brook, USA
rong.zhao@stonybrook.edu

ISCA Headquarters···•···278 Mankato Ave, #220, Winona, MN 55987···•···Phone: (507) 458-4517
E-mail: isca@ipass.net • URL: http://www.isca-hq.org

Copyright © 2019 by the International Society for Computers and Their Applications (ISCA)
All rights reserved. Reproduction in any form without the written consent of ISCA is prohibited.

Editor's Note: December 2019

This note serves as the transition of Editorship of the IJCA as I (Gordon Lee) hand off the journal to Dr. Ziping Liu. I have served as the interim editor for the past year and Dr. Liu begins her tenure as the long-term editor for our journal.

It has been my honor and privilege to serve as the interim Editor-in-Chief of the International Journal of Computers and Their Applications (IJCA). I look forward to continuing to be involved with ISCA, including working in the ISCA conferences.

I would like to begin this note by giving a review of this past year. In 2019 we received several unsolicited papers and accepted about 20% of them to our journal. We also devoted three of the issues to the best papers of the SEDE 2018 Conference, the CAINE 2018 Conference, and the CATA 2019 Conference. This December issue is devoted to the area of cybersecurity.

The ISCA Board of Directors is still working towards getting IJCA online. Hopefully we can end up with a nice repository soon.

I (Dr. Ziping Liu) look forward to working with everyone in the coming year to maintain and further improve the quality of the journal. I would like to invite you to submit your quality work to the journal for consideration of publication. I also welcome proposals for special issues of the journal. If you have any suggestions to improve the journal, please feel free to contact me (zliu@semo.edu).

In the following year, 2020, we have 4 issues planned (March, June, September, and December). Three of the issues will focus on extended research from the best papers at the Fall 2019 SEDE Conference, Fall 2019 CAINE Conference and Spring 2020 CATA Conference.

We would also like to announce that we have begun a search for a few Associate Editors to add to our team. There are a few areas that we would like to strengthen our board with, such as Image Processing and Cyber Intelligence. If you would like to be considered, please contact us via email with a cover letter and a copy of your CV. We look forward to continue with our high-quality journal, sponsored by the International Society for Computers and Their Applications.

Gordon Lee
Interim Editor-in-Chief 2019

Ziping Liu
Incoming Editor-in-Chief

ISCA Copyright© 2019

Guest Editorial: Issues and Designs for Cybersecurity

Cyberspace, and in particular social media, has brought an effective and efficient mode of communication to most areas of the globe. Especially in less developed countries, it has provided a platform for economic development and growth, for improved public administration, for education and emancipation of the masses, and for social mobility. However, it is becoming increasingly apparent that it also has a negative side that may destabilize social harmony. For example, in the aftermath of the recent violence in Sri Lanka, the government shut down most social media platforms for fear that they might be used to fan hostilities and make it impossible to contain the unrest.

There are many ways in which cyberspace might turn to harm individuals, enterprises, society, or all of humanity. As discussed in a special issue of this journal, entitled "On Humans, and Systems They Create" (IJCA, Vol. 24, No. 4, Dec. 2017), information stored and developed in cyberspace will influence the consciousness of humanity of itself and thereby shape the future of humanity. Potentially, this may lead to humanity losing control of its own destiny, a catastrophic failure from which it cannot recover.

Current approaches to limit the negative aspects of cyberspace are largely limited to harm at a less than global scale. They are mostly reactive and targeted at content, after it has been created, and information, after it has been collected. Freedom of speech is considered as one overarching principle, but certain vaguely defined expressions are excluded. Private platforms are held responsible for policing the content posted on them by independent users. Another overarching principle is privacy of user information. However, platforms are not stopped from collecting, storing, and processing private information to target individuals or groups with messages that are meant to change their minds relative to certain products, political or other theories and opinions, and ethical norms. Finally, it is accepted as inevitable that software and algorithms used to operate cyberspace are fraught with errors through which bad actors can gain illegal access and contain "backdoors" for clandestine access by government agencies. The latter, of course, also may provide access for bad actors. Protection against illegal access is largely limited to correcting software errors when they are discovered, limiting access to "trusted users" who are identified through monitoring the behavior of all users, and obscuring information through encryption. The result of this is often an arms race with the "bad guys." This leads to an ever more complicated structure of cyberspace, which, just by its complexity may escape human control. The intended remedy, thus, turns into a disease of its own.

This special issue explores alternatives that could prevent any of the developments within cyberspace that could result in humans losing control of their destiny. In particular, we look at alternative principles to guide the design of cyberspace from the ground up. We anticipate that this means that the design would start by examining the functions required to operate cyberspace; identifying possibilities in which a loss of any of these functions would cause a critical failure (i.e., a loss through which humanity would lose control of its destiny); and include in the design features that would protect against the possibility of such failures. This would correspond to what we have defined as the paradigm of purposeful systems.

This special issue of the International Journal on Computers and Their Applications evolved from papers presented at the CATA 2019 and also includes specially commissioned papers. It is organized as follows:

In the first paper entitled *Critical Issues of Cybersecurity: Solutions Beyond the Technical,* Maximilian M. Etschmaier explores issues of cybersecurity through the framework of purposeful systems to identify existential threats to humanity that emanate from the current development of cyberspace.

The second paper, *Situational Trust and Reputation in Cyberspace*, by Kendall Nygard, Ahmed Bugalwi, Maryam Alruathi, Aakanksha Rastogi, Krishna Kambhampaty, and Pratap Kotala provides an extensive review of the concept and application of the methodology of situational trust management and how it can be used to mitigate some of the threats to the security of transactions in cyberspace.

In the paper entitled *The Inadequacy of Domestic and International Law for Cyberspace Regulation*, Jeremy Straub identifies how the current legal and regulatory regime and system of international treaties can be adapted to assure order for the global cyberspace.

ISCA Copyright© 2019

Farah Kandah, Amani Altarawneh, Brennan Huber, Anthony Skjellum, and Sai Medury in their paper entitled *A Human-Understandable, Behavior-based Trust Management Approach for IoT/CPS at Scale* present an interesting quantitative model that can serve as a platform for development of trust management in a wide range of localized system such as the Internet-of Things and connected vehicles.

We hope you agree with us on the urgency of the topics that are presented in this special issue of the International Journal on Computers and Their Applications.

Guest Editors:
Maximilian M. Etschmaier, Florida State University
Kendall Nygard, North Dakota State University
December 2019

ISCA Copyright© 2019

Critical Issues of Cybersecurity: Solutions Beyond the Technical

Maximilian M. Etschmaier
Florida State University, Tallahassee, FL

Abstract

Within one decade, cyberspace has evolved to an existential threat to the sustainability of the human sphere. Cybersecurity is the collection of measures intended to mitigate this threat. Following the paradigm of purposeful systems, the most critical ones of these threats are characterized. At the level of individual persons, they include threats to privacy, deprivation of access to reality and the truth, and threats to personal freedom and to property rights. These threats are projected to the level of businesses, to affinity groups and formal social organizations, to sovereign states, and to the global human sphere. It is argued that each one of these threats, if unmitigated, will lead to the end of humanity as we know it. Mitigation measures require combinations of technical and human-centered tools. Their effectiveness is discussed. Militarization of cyberspace and current business practices of providers of services in cyberspace are seen as irredeemable obstacles to sustainability of the human sphere.

Key Words: Cybersecurity, purposeful systems, system design, end of humanity, privacy, reality, truth, personal freedom, property rights, sustainability, and cyber-war.

1 Introduction

Starting with the development of electronic representation of information in the middle of the 20th century, a range of new technologies have been introduced that, together as pillars of "cyberspace," have radically changed every aspect of human life. The most important innovations have been direct communication between computers through the internet, the World-Wide Web, and the Internet of Things; wireless digital communication, and global positioning, and Artificial Intelligence, They made possible changes of the human sphere, the way people, businesses, and social, cultural and political entities carry on their day-to-day activities, interact, relate to the world around them, and shape their opinions, attitudes, desires and ambitions, and understanding of their own existence. These changes have led to wholesale transformations of social structures, the organization and conduct of commerce and industry, transportation systems, academic institutions, and the practice of engineering and science. It has also led to a rapid evolution of systems that span the whole world.

Every one of the new technologies has brought new vulnerabilities to the systems and processes that are based on them. Since the technologies are not ends in themselves but constitute critical elements of systems that include parts of the human sphere, the potential damage from these vulnerabilities is not limited to technological artifacts but equally impacts the systems and processes of the human sphere that are dependent on them. As applications of new technologies were developed and implemented in a rather spontaneous and unregulated way, often at the border of existing conventions and laws, they greatly expanded the scope of the vulnerabilities of elements of the human sphere. Many of them started as innocuous experiments but quietly created situations that are all but irreversible and may challenge the dominion of humans over systems they create [4, 7, 9]. Vigilance and protection against these vulnerabilities requires new approaches. These will recognize the interdependence of the human and the technological spheres and develop holistic solutions that simultaneously address human and technological issues.

Restraining and mitigating negative outcomes is proving to be increasingly difficult and laden with conflicts between various principles and expectations. In general terms, this is the aim of what is commonly called cybersecurity. However, there are wide differences in what is considered the scope. And it is those differences that explain the differences in approaches, methods, objectives, and rights and responsibilities of the various participants in any segment of cyberspace. We are proposing a rational, holistic framework through which it should be possible to analyze and interpret any existing or proposed approach or measure intended to achieve security for all or parts of cyberspace. The framework is based on the paradigm of purposeful systems which we have introduced [4]. Militarization of cyberspace and certain practices of providers of services in cyberspace are shown to be irredeemable obstacles to sustainability of cyberspace.

The paper is based on a presentation given at the 32nd International Conference on Computer Applications in Industry and Engineering, 2019, in San Diego [5].

2 Cyberspace

What today is commonly referred to as cyberspace grew from an effort to develop a robust computer-based system of many-to-many communication that could survive a hostile environment such as a military conflict. Different from the telegraph and telephone systems that required the existence of a communication channel between the endpoints of the

* metschmaier@fsu.edu.

ISCA Copyright© 2019

communication for the duration of the communication, the communication was broken up into discrete packets, each of which could independently find its way through a network of communication links. Thus, a communication will not break down when individual links fail or are congested. The price for this is an increase in the complexity of the communication. Instead of just inert data, it also needs to include parts of code that, combined with code and data that reside elsewhere, will dispatch a packet toward its destination. The same mechanism can also be used to distribute the execution of programs among various processors. For example, the originator of a communication can include code in the message that the recipient can use to turn the message into usable information. And it may cause the code to be stored in the processor of the recipient for application to future messages. Additional complexity is introduced because ownership and control of the system may be divided between numerous entities which cannot be assumed to share the same motives, objectives and legal norms.

In a short span of time, scope and functionality of this system evolved opportunistically to fundamentally change the way individuals, groups, and societies interact and business is being conducted. Fora ("platforms") evolved which facilitated the formulation and identification of what might be viewed as the "public" or "common" opinion of various levels of groups. Other platforms made possible the identification of common business interests across the globe and brought about phenomenal efficiency, increases in the production of goods and services, and a concomitant growth in national economies. The opportunistic growth has also led to developments that are not in agreement with the common interest and with prevailing ethical norms. The complexity of the system has provided opportunities to manipulate the system and produce outcomes that violate the legitimate interest of some system participants and operators. Also, like in any system, complexity brings about the possibility of errors in design which in themselves may produce harmful results and, beyond that, may be exploited to the detriment of the operators and users of the system.

2.1 Threats to Security

There is increasing concern that a range of activities in cyberspace are posing a serious threat to the order of commerce and society. And there is evidence that these threats are increasing rapidly. According to its 2018 Report, the Internet Crime Complaint Center ("ic3") of the FBI, in the calendar year 2018, received a total of 351,937 million complaints about cybercrime with a claimed loss of $2.7 billion [15]. Compared to 2017, this represents increases of 16% in the number of complaints and a startling 90% in claimed loss. Compared to 2014, the increases are 30% and 238% respectively.

The report lists 34 different types of "cybercrime." For the vast majority of cases the central element is identified as some form of financial loss by the victim (over 90%). In these cases, either the victim was identified and/or contacted via the internet, and/or the business propositions or transactions were at least partially carried out in cyberspace. Other types of cybercrime include the theft of information by gaining unauthorized access to computers and planting "malware" on the victim's computer. Interestingly, the harm that can be caused by the use of such information and malware are considered as separate crimes, presumably to be prosecuted separately. It appears that, for some cases, this might preclude law enforcement dealing with the whole scope of many types of cybercrime.

For example, extortion through "ransomware," which threatens a target (individual, company, political entity) with destruction of all information held in its computer system and has evolved into globally networked businesses [11] would be divided into several separate acts, each one of them considered separately for prosecution: the development and publication of software, the transmission of the software to the computer systems of the victim, and the facilitation of clandestine payment of the ransom through cryptocurrency [30]. In this division, in the first and the last acts, there is no victim and no damage that could readily be identified. If these acts are prosecuted at all, they would be regarded as "victimless crimes."

In fact, ic3 admits to being relatively powerless, stating that "as ransomware techniques continue to evolve and become more sophisticated, even with the most robust prevention controls in place [at the target computer], there is no guarantee against exploitation." Ic3 recommends "contingency and remediation planning [as] crucial to business recovery and continuity" and identifies "[k]ey areas to focus on … [as] prevention, business continuity, and remediation" [13]. It appears that the FBI is limiting its view of cybercrime as the actual infliction of harm, and its role to solving and prosecuting a crime after it has occurred. It seems to place the onus for prevention on the victim. Implicit in this is that it is taking the mechanisms of cyberspace as given and evolving according to their own dynamic; and is not concerned with suggesting improvements.

Arguably, then, in addition to remediation of the direct damage, the cost of defense against possible nefarious actions by others via the tools of cyberspace constitutes an inherent burden imposed on any participant in cyberspace. While it is difficult to agree on a method of determining this burden, it appears to be significantly higher than the direct damage from cybercrime. For example, just for the domain of the US Federal Government, a White House report states the Fiscal Year 2019 Budget includes "$15 billion of budget authority for cybersecurity-related activities, a $583.4 million (4.1 percent) increase above the FY 2018 Estimate" [41]. However, the report cautions that "[d]ue to the sensitive nature of some activities, this amount does not represent the entire cyber budget." To put this into perspective, the total Budget of Federal Bureau of Investigation for FY 2019 $9.6 billion [12].

The burden on the overall economy is many times that much. Deputy Attorney General Rod Rosenstein, while admitting that "[a]ttempts to quantify just how big a problem we face vary widely," quotes a prediction by Cybersecurity Venture of a doubling of the "the annual cost of global cybercrime … from $3 trillion in 2015 to $6 trillion in 2021," [34]. He quotes private reports that "peg the average cost of a data breach at over $3.6 million." To show just how high the cost for individual business

can be, he cited "[o]ne large retailer … spending $291 million for breach-related expenses, related to one attack on its network. In some cases, smaller businesses declare bankruptcy after a breach". …A case of "theft of technology [the Department of Justice prosecuted] … allegedly caused $800 million in losses. That is more than ten times the largest bank robbery."

But the harm inflicted by actors in cyberspace or using tools of cyberspace is much greater. Two recent books describe in great detail how private data of users of any type of cyber services are harvested, processed and aggregated via a new industry of "data brokers" and sold to be used to target individuals with advertisements and to assemble profiles of individuals that can predict their future behavior [22, 44]. Operators of platforms, like Google and Facebook, are described as harvesting consumer data from their operation of attractive services they offered at low or no cost. As the yield from the data exceeds greatly the cost of providing the services, within a decade, these operators have grown from start-ups to become the most valuable and profitable companies of the world. The individual users are left largely unaware of the value of the information they are surrendering.

The business proposition of the operators is to monetize the privacy of individuals while leaving the individual largely in the dark. "… the essence of the exploitation here is the rendering of our lives as behavioral data for the sake of others' improved control of us. The remarkable questions here concern the facts that our lives are rendered as behavioral data in the first place; that ignorance is a condition of this ubiquitous rendering; that decision rights vanish before one even knows that there is a decision to make; that there are consequences to this diminishment of rights that we can neither see nor foretell; that there is no exit, no voice, and no loyalty, only helplessness, resignation, and psychic numbing; and that encryption is the only positive action left to discuss when we sit around the dinner table and casually ponder how to hide from the forces that hide from us" ([44] p. 94).

Certainly, no rational individual would agree to such a proposition. But "[b]ecause the industry had done so much good in the past, we all believed that everything it would create in the future would also be good" ([22] p39). While possibly not in violation of any positive law, it clearly violates ethical norms. The yield from such operations, therefore, has to be considered ill-gotten gain and harm to the individual. The magnitude of this value transfer can be gleaned from the fact that Google alone is "processing over 40,000 search queries every second on average; more than 3.5 billion searches per day and 1.2 trillion searches per year worldwide in 2017" ([44] p. 93).

2.2 A Definition of Cybersecurity

Cyberspace defines a domain that covers most aspects of the contemporary world. It was made possible by a revolution of technology combined with a market driven capitalistic system that has created an abundance of money searching for investment opportunities. New money can be created in the form of debt almost at will and without limitations [16-17]. And money has become the dominant power of the democratic process, increasingly shaping laws, regulations and administrative processes of states as well as relations between states. The tools and processes of cyberspace have become the expression of the new economic reality. A complex web of power has emerged with numerous centers pursuing often conflicting interests, each articulated by their own self-serving and situation-specific code of ethics. Threats and harm to one party may provide benefits essential to another party's success. In addition to threats by malicious actors, there are large and powerful corporations that sell "cybersecurity products" to protect data and systems of participants in cyberspace (see e.g., [40]). Their business success is greatly influenced by how harm is defined and regulated. It is doubtful then, that there would be one conception of security that could protect all parties fairly and equitably. Rather, any definition of cybersecurity would reflect the position of whoever formulated it. Success is best assured by narrowing the definition of the space for which cybersecurity is being defined.

The narrowest definition of cybersecurity is the one guiding the Internet Crime Complaint Center ("ic3") of the FBI. It is focused on deterring cybercrime by promising to catch cybercriminals and hold them accountable for the damage they caused [14]. Prevention of cybercrime through protection measures is assumed to be the responsibility of the potential victim who is offered advice and guidance.

This interpretation is echoed by a paper by Craigen, et al. [1] that sets out to arrive at a definition of the term "cybersecurity" that would be widely accepted. After an extensive review of the literature they identify and analyze nine archetypes of definitions from which, through a "pragmatic qualitative approach" which "melds objective and subjective research," they arrive at the following definition:

> *"Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights."*

While the focus is on a legal perspective, this formulation does not preclude viewing cybersecurity as an interdisciplinary construct that depends on positions, models and processes from a variety of disciplines. If, as argued in the paper, property rights are understood as a multidimensional concept within the commons as advocated by Ostrom [29], it may serve as one point of departure on a roadmap for the development of holistic constructs of security in cyberspace.

Also based on the thesis that cybersecurity is a public good is the "Doctrine of Cybersecurity" by Mulligan and Schneider [24]. They show that the "effectiveness … of the three doctrines - prevention, risk management, and deterrence through accountability - that have dominated cybersecurity thinking for the past fifty years" has been limited. They argue that "absolute cybersecurity, though a "worthwhile undertaking, is unlikely ever to be achieved. To secure systems that incorporate humans

as users and operators, we need some way to prevent social engineering attacks and intentional insider malfeasance." A "doctrine of prevention would involve a recurring expense" and therefore was "inconsistent with the business model employed by many of today's software providers." They view "mandatory standards … as a way to support the doctrine of prevention" but point out that … a correlation between the absence of vulnerabilities and compliance with standards has not yet been documented."

Regarding a doctrine of risk management, they point out that achieving absolute cybersecurity through it was "cost prohibitive." But "a lack of information about vulnerabilities. incidents, and attendant losses makes actual risk calculations difficult [especially since] companies and individuals do not know how to value (i) confidentiality of information, (ii) integrity of information, or (iii) the pain of dealing with recovery from an attack's effects (bad credit ratings. for example)."

The doctrine of deterrence through accountability "treats attacks as crimes [and] focuses on infrastructure to perform forensics, identify perpetrators, and prosecute them." "Implementations of this doctrine require strong authentication technologies and surveillance of network activity." "Absent an effective means for retribution, this doctrine has no teeth, and fails as a result. Moreover, punishment of perpetrators of cyber-attacks is not always feasible … [and] Attribution of actions by machines to individuals is complicated." Finally, "the doctrine could require individuals to sacrifice privacy and, in the extreme case, abandon the possibility of anonymity and the protections for freedom of speech and association that it affords."

Expanding on the characterization of cybersecurity as a public good, the article points to parallels with public health in public policy, law and enforcement. In both, the interests of individuals and the public do not always align, and laws and frameworks can mediate tensions between them. "Success ultimately depends not only on technical progress but on reaching a political agreement about (i) the relative value of a public good in comparison to other societal values and (ii) the institutions granted authority to resolve conflicts (and the methods they use)."

2.3 Achieving Cybersecurity

It is generally recognized that it is not possible to achieve cybersecurity through technical means alone, but that a holistic approach is necessary to develop a viable framework and processes that can mediate between the sometimes-conflicting expectations of the various players in cyberspace. However, all restrict the analysis to tangible effects that can be quantified and ultimately reduced to the common denominator of money. They use benefit-cost analysis – or its probabilistic equivalent, Risk analysis – as a basis for decision-making. This is the problem. Even when the quantification is only conceptual, it permits the illusion of rationality and optimality of an approach and a solution while ignoring the intangible dimension. But it is the intangible dimension that is critical to the success of a system that involves humans and machines and especially one that spans the whole of the human sphere, as cyberspace increasingly does.

While the approaches of "benefit-cost analysis" and "risk management" are generally accepted as a valid tool for decision-making within an enterprise, it is easy to see that they fail to adequately address the complexity of global systems. Because by nature they aggregate cost and benefits over the entire system, it is not possible to assure that any subsystem that earns a benefit also bears the concomitant cost. In fact, it can be shown that it is possible that economically or socially powerful groups may be able to control the allocation of benefits and cost in a way that is favorable to their domain at the expense of less powerful domains. The result will be increasing disparity within the system. This has been shown to exist in certain proposals at mitigation of carbon emissions and to be a core feature of the utilitarian ethic that underlies much of current teaching in economics and social sciences[2].

A recent paper by Rastogi and Nygard [33] focuses on recognition of vulnerability as the critical step in the development of secure software systems. It identifies vulnerability as flaws or weaknesses in a system's design, implementation, or operation and management. It emphasizes the importance of identifying potential vulnerabilities early in the design engineering phase and to define preventative measures and approaches to control vulnerabilities early in the design process as possible. However, it points out that in software engineering security is considered a non-functional requirement, which means that it is often treated as an afterthought and given less importance than functional requirements throughout the stages of the software development lifecycle. This may be responsible for a tendency to replace security requirements with the specification of security specific architectural constraints; which may narrow design choices; lead to only considering the user's point of view; and make it impossible to continuously adapt detection methods to match the evolution of defects throughout the system life cycle. Rastogi and Nygard also point at parallels between software engineering and design science which is iterative and allows an artifact to emerge and opportunistically evolve as a solution or innovation.

An alternative approach attempts to achieve security within cyberspace by limiting access to trusted participants [27]. Through observation of their behavior, participants are scored for their trustworthiness, and untrustworthy participants are barred from access to sensitive areas or barred altogether. The scoring algorithm is a probabilistic construct that, over time, is improved through statistical analysis. As any such procedure, it is associated with certain error margins. The "type 1 error" will assume a participant to be trustworthy when in fact he is not, which limits the success of the approach. It also may encourage an unworthy participant to learn the scoring algorithm and thus manipulate the system. This may lead to a tug of war with the system and might ultimately destroy the system's effectiveness. The "type 2" error will judge a participant non-trustworthy when in fact he is trustworthy. While this may be acceptable in a private system, it is clearly discriminatory and should not be acceptable in a public system, especially one that leaves the

discriminated no alternative.

It is widely recognized that tools of cyberspace can influence the opinion and choices of individuals and groups. This is what all forms of communications can be and have been used for since the beginning of language. The power to do this has grown with the advent of mass communication and has been used to steer consumption habits, lifestyle, as well as ideological, religious and political preferences. The powers unleashed by cyberspace are just unfathomably more powerful and differentiated. It has already been proven that it can sway the outcome of democratic elections toward otherwise unlikely candidates and causes, potentially choosing between war and peace and life and death for millions [20]. With its global spread, tools of cyberspace can alter the direction of evolution of the human sphere and impact sustainability of humanity and the conditions for human survival. This may open exciting new possibilities. It also opens the possibility of humans losing control of their own destiny [4]. The choice of an approach for achieving cybersecurity thus is one that is critical to the future of humanity. It is a moral choice.

It is remarkable how Tim Cook, the CEO of Apple, expressed the gravity and complexity of the situation at the 2019 Stanford graduation speech [38]:

"Silicon Valley is responsible for some of the most revolutionary inventions in modern history ... social media, shareable video, snaps and stories that connect half the people on earth ... But lately, it seems, this industry is becoming better known for a less noble innovation: the belief that you can claim credit without accepting responsibility.

We see it every day now, with every data breach, every privacy violation, every blind eye turned to hate speech. Fake news poisoning our national conversation. The false promise of miracles in exchange for a single drop of your blood. Too many seem to think that good intentions excuse away harmful outcomes.

... what you build and what you create define who you are. ... if you've built a chaos factory, you can't dodge responsibility for the chaos. Taking responsibility means having the courage to think things through.

And there are few areas where this is more important than privacy.

If we accept as normal and unavoidable that everything in our lives can be aggregated, sold, or even leaked in the event of a hack, then we lose so much more than data. We lose the freedom to be human.

Think about what's at stake. Everything you write, everything you say, every topic of curiosity, every stray thought, every impulsive purchase, every moment of frustration or weakness, every gripe or complaint, every secret shared in confidence.

In a world without digital privacy, even as you have done nothing wrong other than think differently, you begin to censor yourself. Not entirely at first. Just a little, bit by bit. To risk less, hope less, to imagine less, to dare less, to talk less, to think less. The chilling impact of digital surveillance is profound, and it touches everything."

Faustian bargains let developers create "chaos factories" without regard for the ultimate outcome; monetizing basic human values; and a waning regard for truth and compassion limiting human conscience and poisoning the national and global consciousness spell the end of humanness and, with it, humanity as we know it. Human freedom is sacrificed to the "machine" of cyberspace. The term "cybersecurity" covers only part of the threat that humanity is facing. It is the design of the entire cyberspace with all its functions and facilities it provides individuals and society, combined with human weakness that needs to be reexamined for actual and potential threats it is posing. Concern that human-created artifacts might assume control over humans who created them has occupied thinkers for much of history [3, 7 , 42].

As long as human activity was limited to disjoint regions, much of this discussion could be limited to esoteric speculation. Today, as the world has become finite, and, aided by increasingly powerful technology, much of human activity affects the entire globe, it is increasingly obvious that the prospect of humans losing control of their sphere has become a real possibility. The issue is sustainability. "Cyberspace" has become an inseparable part of the sustainability equation. Cybersecurity, or more appropriately the issue of designing cyberspace, therefore can only be examined within the frame of global sustainability. This does not mean that the entire issue of global sustainability, or even just the design of cyberspace, has to be treated in one step. But it is necessary to craft a framework within which every issue in the global system can be related to every other issue in a meaningful way.

Part of this effort is to question prevailing views and examine to what extent they have been shaped by powerful players in cyberspace to their benefit. For example, a recent article takes issue with efforts to tackle "deepfakes," purposely false information, through technological means, proclaiming that "Deepfakes aren't a tech problem. They're a power problem" [36]. The search for technological solutions to all problems related to cyberspace may divert attention from the real cause, the business models of the tech industry and the perceived needs of national security organizations and military services. And it may create business opportunities for the tech industry and research institutions, ultimately making society more and more dependent on their solutions.

We believe that the paradigm of purposeful systems can provide a framework for re-examining the evolution of cyberspace and for developing a new model for cybersecurity. Our past work examining systems ranging from simple technological systems to global environmental sustainability gives us confidence that the purposeful system paradigm does provide a suitable framework and will yield results that are consistent and compatible with and can add to a model of global sustainability. In the following, we will briefly outline the central features of the paradigm of purposeful systems as they pertain to the present problem and outline how a sustainable solution can be developed.

3 The Purposeful Systems Approach

The paradigm of purposeful systems views any system as a construct the boundary of which is drawn in such a way that the system purpose, to the extent possible, is included within the boundary. Designing a purposeful system is an iterative process of defining and redefining the scope (boundaries) and purpose until this balance is achieved. The mechanism of iteration between purpose and scope continues throughout the entire life of the system, driven by a "historian" who develops insight into the nature and behavior of the system, and a "designer" who turns the insight into modifications of functions and scope of the system. This requires the participation of a being that is capable of insight and reasoning, like a human element, in the system. The result is a system that, similar to a living organism, can learn and adapt to a changing environment, in particular emerging threats to its existence. The system possesses consciousness of itself and its environment. An essential part of the system purpose is avoidance of failure states from which there is no recovery ("critical failures"). The design process eliminates the possibility of critical failures through proper design of system functions. The only exceptions are potential failures the possibility of which cannot be recognized within the state of the art. In such cases the resilience that results from the self-consciousness of the purposeful system will provide mitigation. Examples from our past work for the design of a purposeful system range from relatively simple technological systems [6, 8, 10] to a design for achieving global environmental sustainability [2].

4 Ontology of Cyberspace and Cybersecurity

Cybersecurity is an extremely complex system that is affecting much of human existence in many different ways. Since it has evolved in an opportunistic manner and without much central coordination, its structure and the interaction between its various components as well as the interdependence between its various functions are not easily recognized in all their complexities.

Figure 1 shows a top-level view of what is today viewed as cyberspace and that can serve as a point of departure for analysis as a purposeful system.

The figure is divided into four sections:

(i) The Technical Sphere which is the "physical" network infrastructure that handles all transmission and routing of communication between users and between users and various communication platforms like social media and filesharing, user services like search engines, and shopping and financial transaction services. The network infrastructure also provides direct links to entities in Section 3.

(ii) The Consumer Sphere, which includes the individual users, service providers, and platforms and user services. These, together with the network infrastructure, represent the original view of cyberspace as perceived by individual and business users. For a fee, users connect to a service provider who manages their communication across cyberspace and defines their user experience.

(iii) The Commercial Sphere which represents the commercial entities that may extract data for use towards a variety of purposes, including predicting and influencing personal tastes and shopping behavior, as well as political preferences; and various governmental agencies especially concerned with national security and defense that monitor traffic in order to identify emerging threats to national security and a variety of illegal activities. All these entities, in addition to using the network infrastructure for their own communications, draw significant benefits from their access to user communications and in return often provide free services to the users. This is their ultimate value proposition.

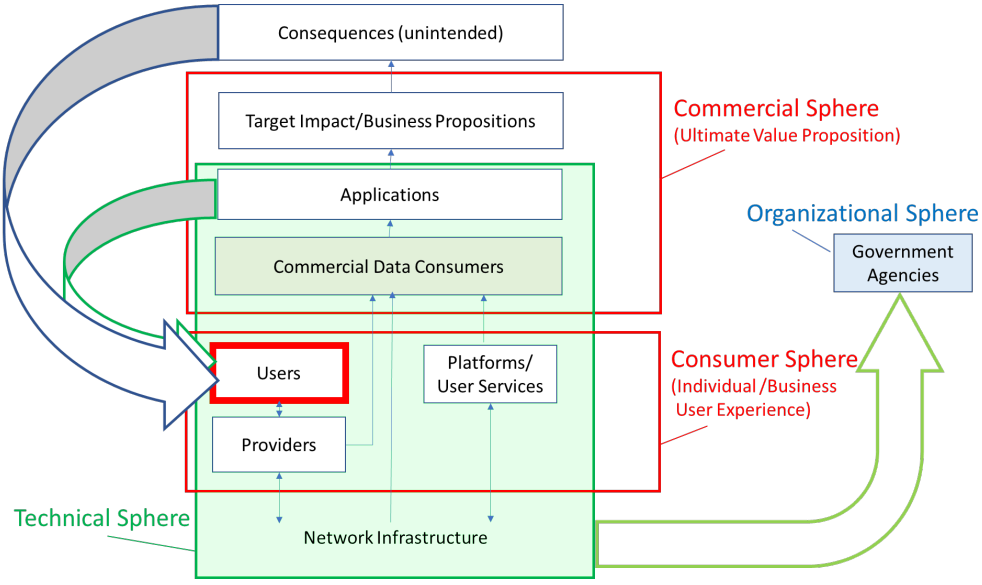


Figure 1: Overview of the components of cyberspace and their interactions

(iv) The Organizational Sphere, within which originates all external impact on cyberspace. This includes, in particular, governmental bodies which formulate and enforce laws and regulations and also the human sphere as the origin of rules of human thought, ethical norms and customs.

(v) The Sphere of Intended and Unintended Consequences which is the highest section and concerns the impact that activities in cyberspace may have on national and global economic, social, political and natural systems. This may be perceived as largely unintentional. Decision-makers may view it as coincidental externalities. However, it is becoming increasingly clear that forces emerging through cyberspace can literally change the course of human evolution. This may well be recognized by certain interest groups as an opportunity to shape the future of the human sphere according to their vision.

5 Analysis of Potential Harm

The system "Cyberspace" is made up of countless functions and components, each of which may be impacted by various types of threats. The purpose of the design of this system must be to assure the availability of all functions when needed. The focus must be on "critical functions," the loss of which would be an irreversible "critical failure." A system for which this cannot be assured is not fit for its intended purpose.

Figure 2 provides an overview over the different paths which threats can take toward their effect. Threats may be the result of conscious action, possibly malicious, or they may arise unintentionally, like e.g., through faulty hardware, software, or data. They may originate from either within or outside the subject domain within cyberspace.

Functions can be grouped according to the system components they are attached to and which bear the ultimate harm. There are two such distinct categories of components that can be identified. Each one is subject to a unique set of threats which require specific functionalities within cyberspace to be mitigated so that they can be kept from leading to critical failures. The first category covers direct users, which include individual users like persons and businesses users, and groups of users comprising affinity groups, formal organizations, sovereign states, and the global human sphere.

Opposite to this category are components that have a stake in the mechanisms of cyberspace and are in a position to actively shape the structure of cyberspace and guide its evolution. Any measure to regulate cyberspace in order to avoid critical failures will target members of this category and limit their freedom. This category includes internet access providers; network platforms and user services; data consumers, commercial users and processors and resellers of data; government agencies; and national security and military organizations.

In the following, we shall focus on the first category of components and examine the types of critical failures they need to be protected against. Clearly, components of the second category are also exposed to potential critical failures. However, their failures are mostly of a technical nature and are the focus of much of the research in computer science and related disciplines. While they can trigger failures in the first group of components, they are subsidiary to the overall system and receive their purpose from the first group. Their analysis, therefore, will have to follow the analysis of the first group.

5.1 Threats to Individual Persons

The concept of a person suffering irreparable harm constituting a critical failure is not a new concept but follows directly from Kantian ethics. Applied to technological systems, at the very least, it evolved in civil aviation in the 1960s when it was recognized that an aircraft for which it might not be possible to prevent a critical failure, i.e., harm to human life, through operational procedures and maintenance actions would not be fit for service [26]. While in that case, harm to human life was interpreted as physical harm (and death), humans can be harmed

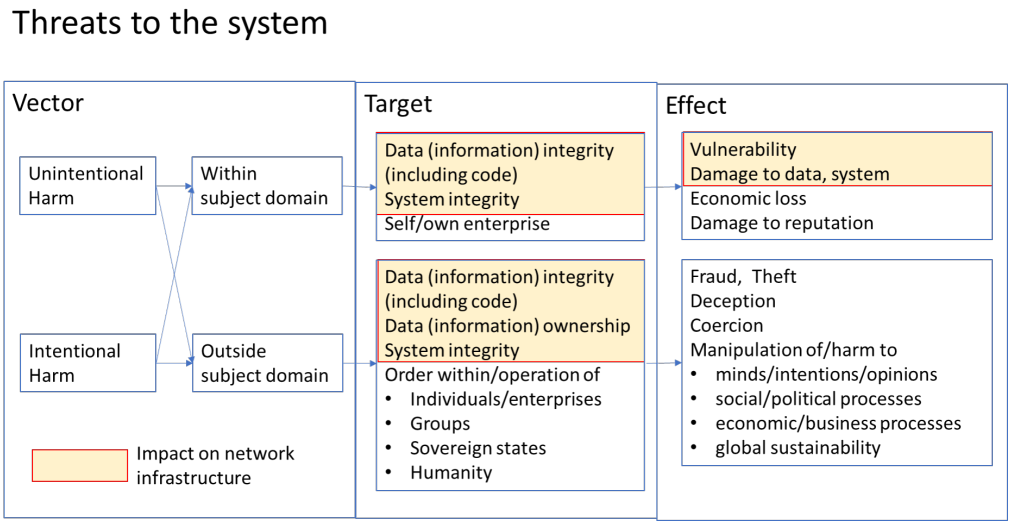


Figure 2: Potential harm and damage to the network infrastructure and to individual/business users

in non-physical ways as well, and that harm may be graver and more persistent than physical harm. An extreme example of this is the "Post Traumatic Stress Symptom" of soldiers returning from combat. While non-physical harm may not kill a person outright, it may alter the essence of a human existence and ultimately deprive the human of his free will. This is what Tim Cook referred to in the remarks to the Stanford graduates quoted in Section 2.0.

Failures of cyberspace through threats to humans can take on many different forms, including:

i. Threat to privacy
ii. Deprivation of access to reality and the truth
iii. Threats to personal freedom and to property rights

5.1.1 Threat to Privacy. If we can view a human through the lens of a purposeful system, privacy is the space where introspection takes place. It is where the human examines input from the environment and uses it to adjust their sense of purpose and the reach of their person within the environment. Destruction of this space would deprive the person of their free will and turn them into a slave of the forces of his environment. In the ultimate state, any thought, any desire, and any affection would be intercepted by an external force and channeled into directions determined by that external force.

To some extent, limitation of privacy is a necessary part of any social system. It is the place where the commitment to a common ethical norm in a society resides, the glue that holds a community together. Also, some measure of privacy is surrendered voluntarily in any relationship with another person. However, it is the remaining private sphere that makes these relationships possible.

The threat to privacy from cyberspace is different. It is motivated by a quest for economic, social, and political power over other people. And it is wielded surreptitiously, piggy-backed on the need and desire of persons to communicate with friends, make new friends, and be part of a community; by their need to engage in commerce, to move around, and to operate everyday vehicles, machines and appliances. By providing a venue for communication, private companies like providers of internet access, operators of a social platform, or operators of any other internet-based service necessarily gain access to private information (data) transmitted through these communications. While much attention is being paid to protect the information from access by "bad actors," the service provider assures access to the information to themselves through clauses buried deep in the fine print of the user service agreement.

A recent study estimated that reading all the privacy notices an average user encounters in one year, would take 76 eight-hour working days [19]. The "Terms and Condition" includes that "[Facebook] may use all of the information [they] receive about [users] to serve ads … this includes information [users] provide at registration or add to [their] account or timeline; things [they] share and do on Facebook, such as what [they] like, and [their] interactions with advertisements, partners, or apps; keywords from [their] stories, and [things we infer from your use of Facebook]" [35].

This is a contract that provides something of monetary value in return for a user's privacy. Since privacy is an essential part of a user's persona, the relationship defined by this is essentially the same as indentured servitude, which in most civilized countries is considered as violating ethical and legal standards. There appears to be no way why the same would not hold in cyberspace.

One rationale for this situation is the opportunistic growth of cyberspace which was initially largely supported by enthusiastic volunteers excited to explore the potential of new technologies outside the norms of business and society. As described in a new book on "Surveillance Capitalism," another one was that national security and military organizations recognized the benefits of similar rules for the use of private data between their domain and the private sector [44].

As cyberspace has significantly changed and grown into one of the most important business sectors and to be dominated by a small number of at least near-monopolistic players, there is no reason to continue the legislative and regulatory neglect. It may be time to consider prohibiting the use of information provided to cybernet service providers and to strictly limit access for government agencies. The model should be the extensive national legislation and regulation regarding the protection of privacy of the mail as well as international treatises regulating trans-border communication which in one form or another have been in existence for centuries [31].

5.1.2 Deprivation of Access to Reality and the Truth. From a technological perspective, cyberspace appears as a complex communication system through which information passes from some source to one or more destinations. During this passage, the information may be accumulated, aggregated, divided, sorted, and translated into a different format. Cybersecurity is a state of cyberspace that assures that the information is not materially changed by any of these processes without consent by the originating and receiving entities as it passes through cyberspace. Threats can arise from faulty design of the mechanisms of cyberspace, faulty intervention of human operators controlling the mechanisms, all unintentional; but also, from malicious intervention by hostile actors from outside of the space through which the information travels, or by rogue operators of the mechanisms within that space.

From a technical perspective, access to reality and truth (a breach of cybersecurity) is denied when information received at a destination is not consistent with information entered by any of the legitimate sources. Based on this definition, the information arriving at a destination may be considered to be "correct" or "incorrect." Determining correctness would require comparison of the information entered at the origin with the information arriving at the destination. This could be accomplished by using independent parallel channels or by comparing the value of a suitable statistic on the information at the origin and at the destination.

In situations when the information undergoes complex transformations between the origin and the destination, neither approach would work. In this case, some determination of the

plausibility of correctness of the information arriving at the destination may be an alternative. Would such a measure of plausibility be robust enough to determine the effect of surreptitious, willful modification of the information? And, given knowledge of the measure of plausibility employed, would it be possible to construct modifications of the information that would evade detection? If this were possible, it would be necessary to find some other measure of truth or process of verification to determine if the message as received was correct.

Equally important, in an absolute sense, the question of reality and truth applies to the content of any message that enters cyberspace, i.e., before it undergoes any transformation within cyberspace. Reality and truth are very elusive concepts that have occupied philosophers and theologians, as well as scientists and engineers throughout the ages. Only simple minds could possibly claim to see or understand the reality that creates their perceptions. And the truth is inaccessible except for trivial statements about finite domains. Nevertheless, it is often possible to agree on standards that determine the absence of reality or truth, such as in a lie.

Any person considering an object of the real world may come away with a different perception of the object. A priori, each perception has to be considered as equally true ("correct"). There is a rich literature on repeatable experiments to show how people may not see prominent elements in a picture or movie and may see what is not in the picture. A much different reality is addressed by the neuroscientist Eric Kandel pointing to a portrait by Oskar Kokoschka that depicts an old man in bold brush strokes far different from what a photograph would show [18]. While a casual observer would undoubtedly consider the photograph as a true representation of the man's face, an introspective person can recognize behind the brushstrokes features of the person's character, history. The question is which is the more accurate depiction of the man's face. On the other hand, one may recognize that the photograph is taken from one particular angle, at a particular configuration of light, and at a specific time in the life of the person. All of which may create a particular snapshot of the person. But it is not at all clear to what extent this is a "true" image of the person's face.

Ultimately, every person should have the right to determine for themselves how they perceive reality and what they hold as true. Clearly, their judgement will be influenced by other people they relate to. While in the past, it was relatively easy for any person to have some perception of the trustworthiness of people they relate to, the ubiquity of news sources that come with cyberspace, and the proliferation of "friends" promoted through social media makes such judgement increasingly difficult. The individual is inundated with news to such an extent that they lose the capacity to make their own judgement of what is right or wrong and what is true or false. In this situation anything may be subjectively true or false. The term "Fake News" does not illuminate the situation but adds to the general insecurity about the truth in anything. Individuals lose access to the meaning of truth because of manipulations of cyberspace. This would be a critical failure for an individual as well as for humanity as a whole.

There are efforts to determine the veracity of statements through algorithms of "Artificial Intelligence." Even if there were a chance for these to succeed, they would only increase the alienation of humans from the truth. Humans would lose confidence in their own judgment because they learn that their judgement is perceived as inferior to that of the algorithm. This diminishes the private space of individuals and with it the capacity for insight, another critical failure. Consequently, purely technological means do not appear suitable to protect against the threat to access to reality and the truth.

But there are other means to prevent critical failures. There is no reason why a society would tolerate being bombarded by information they do not possess the capacity to determine the truth of and why "social media" through clever production ("Inszenierung") and manipulation of relationships multiply information of questionable veracity, especially if the bombardment directly enriches the bombardier. The public should have a right to fully understand the business models, including the revenue streams of the various actors in cyberspace, so they can determine for themselves whether they want to serve as a (mostly free) resource. However, legal limits on these models will be difficult to enact because they are extensions of models that are as old as commercial mass communication and are deeply rooted in modern economies.

Finally, it is doubtful whether a decision of the Supreme Court meant to protect political speech ("Anonymity is a shield from the tyranny of the majority" and "protections for anonymous speech are vital to democratic discourse") should be used to provide a shield of anonymity to creators of fake realities [21]. Clearly, without knowing the offender, targeted individuals have little chance to seek redress, especially if, as is currently the case, law enforcement agencies have limited capacity to support their efforts or to pursue offenders on their own. Other democratic countries have press laws that require that every publication identifies who is responsible for the content [39].

A special situation is posed by the emergence of "Deep Fakes." Algorithms of "Artificial Intelligence" are making it possible to efficiently create photo-like images and videos of people in made-up situations. Bad actors are using these pictures to damage reputations or for blackmail. They have also been used in political propaganda. Clearly, deep fakes can do irreparable harm to individuals and to groups if they are used as weapons. However, manipulating photographic images is a long-established practice and not in itself malicious. Besides, just the selection of the parameters, angles, and backgrounds alone can greatly distort the impression of an object in positive as well as negative ways. Finally, there is a long tradition of cartoons and caricatures that attempt to provide graphic commentaries about a person, a group or a situation. While there are limits to what is acceptable in a cartoon, the cartoonist is given great latitude in how they present the subject.

It seems that stopping the production of fake or doctored images would be a futile undertaking as would development of algorithms that could identify "Deep Fakes." Instead, a legal requirement to mark "Deep Fakes" as such and identify the person responsible for them could suffice.

The business model of the various types of internet services

have to be outed as corrupt and damaging to society. Unfortunately, inundating the population with information they have limited capacity to verify, to some extent, has been practiced at least since the emergence of "mass media." The advent of radio, cinema, and television, as well as of personal telecommunication has just accelerated the momentum. But the mechanisms of cyberspace are building on that and taking the momentum to unsustainable levels through chain-mail-like mechanisms. Therefore, these business practices need to be outlawed.

5.1.3 Threats to Personal Freedom and to Property Rights. Personal property, no matter how small that property might be, is the physical equivalent of privacy. Both, together, define personal freedom. A person deprived of all private property has lost the ability to express themselves in a space that is totally controlled by them. The object of this expression is formed in the space of privacy.

Property comes in many forms. It may be a physical object that a person is free to shape according to their vision, or it may be something non-physical, like a vision of some order, or an idea. Social media, through extrapolation from the masses of data they are collecting can take possession of property without the collaboration or even knowledge of the owner. In fact, the owner may firmly believe they own a piece of property without realizing that they have surrendered any ability to manipulate the property to communities that have formed in cyberspace. Any change requires the approval of more or less anonymous communities lest it results in some form of shaming or other expression of disapproval. The force of cyberspace makes this impossible to bear. As a result, the person has lost their free will, the ultimate expression of freedom. The current expansion of copyright takes this process into the legal arena by assigning property rights to spurious claims of first use of ideas that any person might develop.

This phenomenon is not new and did not arise with cyberspace. It is essentially the same as what Ortega y Gasset described as the phenomenon of the "Mass Man" [28]. It is also the basis of the method by which fascist dictatorships control the masses, making their subjects feel good about themselves without realizing that they have given up all control of themselves. In the end, it amounts to the equivalent of "Genetic Engineering" of the human mind. And it can be scaled to formal and informal groups of humans, sovereign states, as well as humanity itself.

The process of expropriation of property and personal freedom through cyberspace is well advanced and will be difficult, if not impossible, to reverse. Any remedy will need to target the root of the problem: the ability of providers of services in cyberspace to collect personal data. This will stop the development of algorithms that create insight into a person's private space deeper than the person themselves possess. Breaking the monopolistic control of cyberspace by service providers appears to be a necessary first step. It will curtail their influence over the political process that supports the process of expropriation.

5.2 Threats to Businesses Users

Business users are on the opposite side of the coin from individuals. They benefit from the collection and analysis of private data of individuals. Their first attention will be to protect their ownership of data through various security arrangements. This is where the technological parts of cybersecurity, algorithm-based measures, including encryption, have their place. An abundant collection of literature is dealing with this.

5.3 Threats to Affinity Groups and Formal Social Organizations

Affinity groups and formal social systems are exposed to threats from cyberspace in ways analogous to those an individual is exposed to. Those threats are to their own sense of identity, their ability to keep information private, and their ability to chart their own destiny as a group. Depending on designs of some anonymous institutions within cyberspace, they may be led to admit uncontrollable numbers of new members, or they may be moved to tighten their circle and form "Filter Bubbles." In the end, their filter bubble may be "Weaponized" for political ends of the institution that fostered their establishment, or, through commercial arrangements, by some other institution. This may include battles with some other filter bubbles directed by the same or different institutions.

Clearly, in any case, the group loses control of its identity and destiny. The end state may be much worse than it could be for individuals. However, the tools of control are similar. Consequently, the measures to protect against any threat will be the same as for individuals.

5.4 Threats to Sovereign States

Sovereign states are groups that control a specific territory and have dominion over their citizens. They issue laws and regulations to maintain social, economic, and political order within their territory and to assure the freedom and safety of their citizens and properties owned communally and by individual citizens. Being sovereign, the state is free to arrange its affairs according to its preferences. And it is free to join other states to develop and implement common rules.

The threats identified for individuals and groups apply within the territory of a state. And any state should be free to shape measures of protection in accordance to the actual threat and their preferences.

Due to the transnational reach of cyberspace that developed in an opportunistic fashion over large part of the world, sovereignty of states over cyberspace has been eroded without much public awareness. Sovereign states, therefore, find themselves in the situation described for affinity groups and formal social organizations. Increasingly, they find themselves victims of manipulation of their political, social and economic affairs. Citizens are more closely connected to institutions in cyberspace than they are to the constitutional agencies in the state. For a state, regaining control of its sovereignty is a

difficult undertaking because the interest of the state is positioned against the interest of a largely anonymous entity in cyberspace that controls the opinions, if not the mind, of a large segment of the population. For the state to succeed in this confrontation, it has to use the facilities of cyberspace that are controlled and protected by institutions that are largely outside the domain of the state. And those institutions may be beholden to other sovereign states which may have their own designs for the state's evolution. This will require delicate diplomacy. Also, in a previous paper, we observed that

> *[the business model of cyberspace service providers] "is not only reaping enormous profit for the host of the platform. It is also contributing its entire revenue to the growth of the economy. Curtailing that would violate the central ethical principle that is currently driving the economy, the notion of the invisible hand that turns even ill-gotten economic gain into a positive contribution to the economy. Any government that would attempt to curtail the success of a social-media platform would be seen as hurting the interests of the state, violating the commitment it made to the nation."*[7].

In any case, if the state wants control of its future, the state has to claim its segment of cyberspace as integral part of its sovereign domain. It has no choice other than taking full control of cyberspace as it applies to its territory and citizens. This will require active control of all transborder traffic of information to assure that it meets at least the standards for intra-state traffic. It will also require the design and application of algorithms and other systems and processes. From the point of view of the state that domiciles the major players in cyberspace it may be desirable to have their ideas permeate to other countries. But it needs to be recognized that any interference in the internal affairs of a sovereign country is a violation of international law.

The experience of the "Arab Spring" demonstrates the power cyberspace can have over the emotions of people and how these emotions can be mobilized to bring about irreversible change in a range of countries [23]. As that experience shows, that change may not really be in the interest of the nationals of those countries. It may, therefore, ultimately prove unsustainable and leave the states worse off than they were before.

5.5 Threats to the Global Human Sphere

What distinguishes the human sphere from a simple accumulation of individuals, or even groups or sovereign states is that there is nothing beyond it. Humans being inside it, according to Wittgenstein, cannot control it, since that would require them to also be outside it, a logical impossibility [43]. Similarly, cyberspace which is inside the human sphere, as it approaches the limits of the human sphere will elude human control – a stark prospect, since the rate of growth of cyberspace seems to make that inevitable for the not too distant future.

Clearly, the human sphere and cyberspace are not defined in physical terms alone. According to Teilhard de Chardin, the human sphere includes the noosphere, which is the locus of human introspection [37]. This is where human evolution is currently focused. It is also where much of cyberspace is located. Extrapolating from the above discussion about cyberspace increasingly extracting from humans that which is the essence of humanness, as cyberspace covers the entire human sphere, there will be no humanness left. This will be the end of humanity, at least as we know it. Humans will have lost control over the system they themselves created. And there will be no return from this state.

There have to be limits on the kind of experimentation with, and instrumentalization of human minds and freedoms. It is difficult to see why a process like the Institutional Review Board (IRB) process required for experiments with human subjects cannot equally be applied to experiments in the infinitely larger domain of cyberspace. Beyond that, there are all the measures that have been outlined in this paper that, combined, would be a foundation for effective control.

6 Obstacles to a Sustainable Cyberspace

Unfortunately, implementation of this proposal would face vehement opposition from a number of directions. And as the dominance of the human sphere by cyberspace increases, the ability to overcome the opposition would diminish. It will be those who oppose reform who will seize control over cyberspace and through it over an expiring humanity.

There are two main sources of obstacles to effective control of cyberspace: military and national security interests and the community of businesses benefitting from the current situation of cyberspace. The challenge in overcoming them is that both are expressions of ethical norms that are vying to govern the human sphere.

6.1 Military and National Security Interests

Even if a military strategy for operations in cyberspace is meant to be truly defensive, the military will be tempted to follow the adage that the best defense is a good offense. In a world of several superpowers, even if one power intends to act purely defensively, it needs to match the aggression of other powers to avoid losing. This is setting up cyberspace as a permanent battlefield, which only ends when one of the parties has reached total dominance – or all are exhausted. As Gen. Paul M. Nakasone, the head of the US Cyber Command (which was upgraded to a Unified Combat Command in May 2018) articulated: "If we are only defending in 'blue space,' we have failed. We must instead maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries" [25]. Clearly, this eliminates the possibility of any part of cyberspace remaining outside the battlefield.

As recurring reports of cyberattacks conducted by various government agencies indicate, a cyberwar is in full progress (see e.g., [32]). In other words, military and national security organizations are functioning like the "bad actors" that cybersecurity intends to defend against. The end-state they are

working toward is nothing less than what we have defined as the end of humanity. Unless some way can be found to end this cyber war, the military and national security agencies cannot but oppose the proposals developed in this paper.

6.2 Community of Businesses Benefitting from the Current Situation of Cyberspace

Within barely a decade, a handful of companies have risen to be today's highest value companies and their founders have amassed unimaginable fortunes. The dynamic of this process is well described as Surveillance Capitalism, which is characterized as "not an accident of overzealous technologists, but rather a rogue capitalism that learned to cunningly exploit its historical conditions to ensure and defend its success. [44] "They prey on weakness in human psychology, using ideas from propaganda, public relations, and slot machines to create habits, then addiction" ([22], p81), …surveillance capitalists are impelled to pursue lawlessness by the logic of their own creation. Google and Facebook vigorously lobby to kill online privacy protection, limit regulations, weaken or block privacy-enhancing legislation, and thwart every attempt to circumscribe their practices because such laws are existential threats to the frictionless flow of behavioral surplus ([44], p 105).

Their rise was made possible by the rise of Neoliberal economics which believes in the unfettered power of the free market that, unconstrained by government regulation, will deliver "optimal" outcomes. By the time they got their start, "the United States was more than a generation into an era dominated by a hands-off, laissez-faire approach to regulation, a time period long enough that hardly anyone in Silicon Valley knew there had once been a different way of doing things. This is one reason why few people in tech today are calling for regulation of Facebook, Google, and Amazon, antitrust or otherwise" ([22], p 47). In fact, a large portion of users and developers of cyberspace services have become indoctrinated to believe that government is the most significant threat to their freedom and to democracy. Which led the CEO and cofounder of the largest cybertech company, Google, to defend Google's unprecedented power suggesting that people should trust Google more than democratic institutions: "In general, having the data present in companies like Google is better than having it in the government with no due process to get the data, because we obviously care about our reputation" ([44], p 60).

The businesses active in cyberspace possess all the tools to defend and, in fact, expand their unprecedented power. They have the financial resources to dominate the political process, and they have the means to convince people of their merits and benevolence. There is no reason to believe that this will not enable to continue concentrating their power and wealth at the expense of privacy, access to reality and the truth, and personal freedom and to property rights for humanity.

7 Summary

Following the paradigm of purposeful systems, cybersecurity is framed as part of the global sustainability equation. Mitigation strategies need to be directed at the totality of the threat and need to consider the impact on and response capabilities of the global human system. At this level, a complex web of forces is interacting with each other, each force itself being the result of many-directional interactions. As a result, the global human system, as any such system, will defy efforts to characterize it through linear hierarchies. This rules out purely technological approaches, such as in particular, encryption, anonymity and trust management as anything but parts of a system of cybersecurity.

Measures that could stop the threat focus on legal and institutional issues. They presume the existence of a stable infrastructure that is secure against attacks by "bad guys." However, military and national security agencies use of cyberspace are following paths that are directly opposite to the proposed measures. Businesses providing services in cyberspace possess an extraordinary combination of tools to cement their dominance and to reap increasing benefits from collecting and processing information gathers incidental to the attractive services they are offering people at low or no cost. The challenge is that both are deeply rooted in ethical norms that are currently vying to dominate the human sphere.

This paper, therefore, concludes that in order to maintain sustainability of the human sphere it is necessary to find an end to the cyberwar that is already in full progress and stop private companies from accessing and processing highly personal information on individuals that passes through their domains incidental to even legitimate business transactions. Urgency is indicated because many of the conditions created in cyberspace become increasingly irreversible.

Acknowledgements

The author thanks Judson MacLaury for the skillful professional editing, Gordon Lee for suggesting and help in framing this paper, and Christoph M. Etschmaier for research and editorial assistance as well as valuable discussion of the conclusions.

References

[1] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining Cybersecurity," *Technol. Innov. Manag. Rev.*, p. 9, 2014.

[2] M. M. Etschmaier, "Designing an Ethical System of Global Sustainability as a Purposeful System: GEBAT, Global Equity of the Burden Added Tax," *Int. J. Sustain. Policy Pract.*, 14(1):17-35, 2018.

[3] M. M. Etschmaier, "Can Humans Stay in Control of Systems They Create?", *Int. J. Comput. Their Appl.*, 24(4):149-154, Dec. 2017.

[4] M. M. Etschmaier, "Purposeful Systems: A Conceptual Framework for System Design, Analysis, and Operation, *International Journal for Computers and Their Application,* 22(2):87-100, June 2015.

[5] M. M. Etschmaier, "A Purposeful Systems Design Approach for Cybersecurity," *Proceedings of 32nd International Conference on Computer Applications in*

Industry and Engineering, San Diego, CA, 63:90-100, 2019.

[6] M. M. Etschmaier and G. Lee, "Defining the Paradigm of a Highly Automated System that Protects Against Human Failures and Terrorist Acts and Application to Aircraft Systems," 23(1):8, 2016.

[7] M. M. Etschmaier and G. K. Lee, "Integrating Humans and Machines into Purposeful Systems that Keep the Human in Control," *Int. J. Comput. Their Appl.*, 23(2):55-168, Dec. 2017.

[8] M. M. Etschmaier and Gordon K. Lee, "Designing Secure Computer Systems as Purposeful Systems," *IJCA*, 23(2):105-115, Jun. 2016.

[9] M. M. Etschmaier, K. E. Nygard, and E. Oliveira, "Guest Editorial: On Humans, and Systems They Create," *ISCA*, 24(4):147-148, Dec. 2017.

[10] M. M. Etschmaier, S. Rubin, and G. K. Lee, "A System of Systems Approach to the Design of a Landing Gear System: A Case Study," *CAINE 2014, 27th International Conference on Computer Applications in Industry and Engineering*, New Orleans, LA, p. 6, 2014.

[11] K. Fazzini, *Kingdom of Lies: Unnerving Adventures in the World of Cybercrime*, St. Martin's Press, New York, 2019.

[12] "FBI Budget Request for Fiscal Year 2019," *Federal Bureau of Investigation*, [Online], Available: https://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2019 [Accessed: 26-Oct-2019].

[13] "FBI Cyber Task Ransomware_Trifold_e-version.pdf.," June 2019.

[14] FBI Internet Crime Complaint Center, "FBI Internet Crime Complaint Center - Internet Crime Schemes," [Online], Available: https://www.ic3.gov/crimeschemes.aspx, [Accessed: 09-Jun-2019].

[15] M. Gorham, "2018 Internet Crime Report," Federal Bureau of Investigation, Internet Crime Complaint Center 2018 Internet Crime Report, Washington DC, Annual Report, 2018.

[16] D. Graeber, *Debt - The First 5,000 Years*, Upd Exp Edition, Melville House, Brooklyn, 2014.

[17] H. Henderson, "Between Debt and the Devil by Adair Turner - Review," *Seeking Alpha*, 19-Dec-2015, [Online], Available: https://seekingalpha.com/article/3765876-review-debt-devil-adair-turner, [Accessed: 13-Aug-2019].

[18] E. Kandel, *The Age of Insight*, Random House, New York, 2012.

[19] A. C. Madrigal, "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days," *The Atlantic*, 01-Mar-2012, [Online], Available: https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/, [Accessed: 08-Jul-2019].

[20] J. Mayer, "How Russia Helped Swing the Election for Trump," https://www.newyork.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump, 24-Sep-2018.

[21] *McIntyre v. Ohio Elections Commission*, 1995.

[22] R. McNamee, *Zucked: Waking Up to the Facebook Catastrophe*, Penguin Press, New York, 2019.

[23] A. Mitchell, H. Brown, and E. Guskin, "The Role of Social Media in the Arab Uprisings, Pew Research Center," http://www.journalism.org/2012/11/28/role-social-media-arab-uprisings/, 28-Nov-2012.

[24] D. K. Mulligan and F. B. Schneider, "Doctrine for Cybersecurity," *Daedalus*, 140(4):70-92, Oct. 2011.

[25] P. M. Nakasone, "A Cyberforce for Persistent Operations," *Jt. Force Q.*, 92:10-14, 2019.

[26] F. S. Nowlan and H. F. Heap, *Reliability-Centered Maintenance*, Dolby Access Press, San Francisco, 1978.

[27] K. E. Nygard, M. Chowdhury, and P. Kotala, "Trust and Purpose in Computing," *Proceedings, 32nd International Conference on Computers and Their Application (CATA 2017)*, p. 6, 2017.

[28] J. Ortega y Gasset, *The Revolt of the Masses*, W.W. Norton & Company, New York, 1993.

[29] E. Ostrom, *Governing the Commons*. Cambridge University Press, 2015.

[30] N. Perlroth and S. Shane, "In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc," *The New York Times*, 26-May-2019.

[31] S. Powers, "Where did the Principle of Secrecy in Correspondence Go?," *The Guardian*, 12-Aug-2015.

[32] A. Press, "US Launched Cyber Attack on Iranian Rockets and Missiles – Reports," *The Guardian*, 23-Jun-2019.

[33] A. Rastogi and K. Nygard, "Software Engineering Principles and Security Vulnerabilities," Proceedings of 34th International Conference on Computers and Their Applications, pp. 180-168, 2019.

[34] R. J. Rosenstein, "Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Cambridge Cyber Summit," 04-Oct-2017. [Online] Available: https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit, [Accessed: 29-Oct-2019].

[35] Amanda Scherker, "Didn't Read Facebook's Fine Print? Here's Exactly What It Says," *HuffPost*, 39:44-400AD, [Online], Available: https://www.huffpost.com/entry/facebook-terms-condition_n_5551965. [Accessed: 08-Jul-2019].

[36] O. Schwartz, "Deepfakes aren't a Tech Problem. They're a Power Problem," *The Guardian*, 24-Jun-2019.

[37] P. Teilhard de Chardin, *The Phenomenon of Man*, Harper and Row, New York, 1975.

[38] S. University, "2019 Commencement Address by Apple CEO Tim Cook," *Stanford News*, 16-Jun-2019, [Online], Available: https://news.stanford.edu/2019/06/16/remarks-tim-cook-2019-stanford-commencement/, [Accessed: 17-Jun-2019].

[39] A. Unternehmensberatung, "§ 118 StGB (Strafgesetzbuch), Verletzung des Briefgeheimnisses und Unterdrückung von Briefen - JUSLINE Österreich," [Online], Available: https://www.jusline.at/gesetz/stgb/paragraf/118, [Accessed: 08-Jul-2019].

[40] "What is Cyber Security? Definition, Types, and User Protection | Kaspersky," [Online], Available: https://usa.kaspersky.com/resource-center/definitions/what-is-cyber-security, [Accessed: 14-Nov-2019].
[41] "White House Report ap_21_cyber_security-fy2019.pdf.," 2019.
[42] N. Wiener, *God and Golem, Inc., A comment on Certain Points where Cybernetics Impinges on Religion,* The MIT Press, 1964.
[43] L. Wittgenstein, *Tractatus Logico-Philosophicus*, Cosimo Classics, ISBN 978-1-60206-451-5, 2007.
[44] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 1st Edition, Public Affairs, New York, 2019.

Maximilian M. Etschmaier's professional work is focused on the analysis, design, and operation of complex systems in a wide variety of domains. He is a Senior Research Scholar at Florida State University and he has advised clients on policy and strategy development, led system development and process improvement ventures, and supported international technology transfer. Previous positions include Chairman of the Management Board of Joanneum Research in Graz, Austria, Professor of Engineering at the Universities of Pittsburgh and Massachusetts, Senior Scientist at the United Technologies Research Center, Head of Operations Research of Deutsche Lufthansa AG, and Visiting Professor at the University of Graz and University of Innsbruck. Dr. Etschmaier is a native of Austria. He holds a Doctorate in Engineering from the Technical University in Graz, Austria, and an MS in Operations Research from Case Western Reserve University, where he was a Fulbright Scholar.

Situational Trust and Reputation in Cyberspace

Kendall E. Nygard*, Ahmed Bugalwi*, Maryam Alruwaythi*, Aakanksha Rastogi*,
Krishna Kambhampaty*, and Pratap Kotala*
North Dakota State University, Fargo, North Dakota, 58102, USA

Abstract

Interactions in cyberspace are an essential element of daily life today, as people and the systems that they use support email, social media, electronic commerce, automated decision-making and other services that benefit people in their private lives and in their work. However, great harm also occurs, through crime and fraud, identity theft, the spreading of misinformation, and the violating of ethical principles surrounding civil society. Trust refers to the degree of belief that people and systems act dependably, reliably, and securely in the context in which they operate. Trust is a social construct with deep roots in personal interactions among people. When extended into the digital world of today, the concept of trust broadly involves groups of people, entire societies and governments, and the platforms and systems that they use. We describe data gathering and models that apply to interactions among people, devices, machines, computational platforms, and intelligent decision-support systems, and ways in which trust can be quantitatively modeled and measured. The concept of identity management is discussed in relation to trust as a personal asset of an actor. A new graph-theoretic trust model that can function within blockchain environments is described, and analytical results are applied using available data for a Bitcoin community. Comparisons are made with competing trust models, potential for blockchain technologies to support trust as an asset of an individual entity.

Key Words: Trust, security, monitoring cloud, purpose, identity, social, blockchain.

1 Introduction

Trust refers to the state of belief that an entity will act dependably, reliably and securely within a specific situation or context. As a social construct that applies to relationships and actions among people, an acceptable level of trust is essential to a meaningful interaction. When a person engages within a system in cyberspace, the interaction is satisfactory only if the system is trustworthy at some acceptable level. We take an encompassing view of the concept of trust, including applying the concept to interactions among people, phones, devices within the internet of things, high performance computational platforms, social media, and data sources. Activity among these many heterogeneous entities is highly dynamic and massively distributed. Anthropomorphizing, we treat the active entities as actors that interact with one another in a community. Each actor must be trusted at an acceptable level in order for interactions to be positive and satisfactory. For example, a cloud provider is an actor that enters into service level agreements that specify access and provisioning of their services that meet standards that include mapping into pillars of cybersecurity, including integrity, confidentiality, and availability. But trust goes well beyond security. Lapses in cybersecurity do result in bad outcomes, often through no fault of the actors involved. Bad outcomes that occur independently of cybersecurity problems include provisioning of bad data and information, deliberate lying and deception, misunderstandings, and technical glitches. These problems underscore the importance of users continuously assessing their level of trust in the systems that they employ in seeking the ends that they pursue.

If a cloud provider betrays a client actor by failing to adhere to specified standards of service, the level of trust that the client has in the provider goes down. A two-way relationship between any actor who serves as a trustor on one hand and as a trustee on the other is fundamentally the same as interpersonal social relationships among people that have been of importance for centuries. In the digital age, many systems and devices act like humans, doing things like responding to requests, providing data and information, making decisions, and carrying out services. Ensuring positive, purposeful, and secure interactions among actors in the systems of today is a massive challenge. We work within a framework of situational trust as a means of avoiding harm and disappointment in the digital lives of people that can result from things like breaches of ethical standards, criminal activity, and failure to meet performance guarantees.

The digital currency Bitcoin is a blockchain technology that uses distributed ledgers to support anonymous payments over the internet. Blockchain systems are peer-to-peer, carrying out interactions directly between two parties with no intervention, regulation, or supervision by a third party or government. Viewing these peer-to-peer interactions as social networks in which edges represent relationships between users, blockchain systems provide a foundation for modeling trust relationships among entities. We describe a model called TrustMe that captures the dynamics of community development in distributed systems and provides a new approach to modeling trust between

*Department of Computer Science. Email: {kendall.nygard, ahmed.bugalwi,maryam.alruwaythi,aakanksha.rastogi,krishna.kambhampaty,pratap.kotala}@ndsu.edu.

ISCA Copyright© 2019

peers.

The work described is centered on the potential for trust models to be integrated into online computing and communication interactions to improve security [10]. By so doing, people can potentially gain enhanced empowerment to manage their personal digital lives.

Portions of this paper are based on a presentation given at the 32nd International Conference on Computer Applications in Industry and Engineering, 2019, in San Diego [10].

2 Trust and Situation Dependence

Trust is fundamentally a social construct, formed in terms of how humans interact with one another. When a trustor and trustee interact, there are intended outcomes, regardless of whether the interaction is among people or digital systems. The interactions have a context, which makes them situation dependent. Both trustee and trustor have goals, which may be at cross-purposes with one another. With the roots of trust being in human affairs, researchers in the social sciences such as sociology, psychology, economics, and political science have examined trust in various contexts and situations [16].

Trust modeling often assumes a context-free environment, i.e., that the trust level of an entity has no dependence on a particular situation. However, we assert that situational awareness is critical in trust modeling. For example, a restaurant on the oceanfront may legitimately receive high reputation scores online for seafood dishes, but low scores for barbeque. A recommendation system for restaurants can utilize predictive analytics with tools such as collaborative filtering and information about the user to predict the rating that a user would give the restaurant certain types of dishes. Context also matters for the so-called "cold-start" problem, in which there is little or no historical record or reputation track record to provide information and guidance [3].

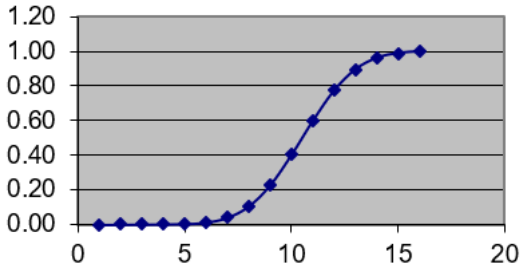


Figure 1: Hysteresis effect in trust

In social networks, people normally expect truthfulness and an adequate level of mutual trust when we interact with our close friends. However, it is generally understood that trust levels change nonlinearly over time, rising when sequences of positive interactions take place, falling when negative interactions occur, and diminishes transitively when we interact with friends of friends or more remote systems. This is called the hysteresis nature of trust [4, 11]. Figure 1 illustrates the hysteresis effect in a simple model in which trust is scaled to the range [0,1], with 0 being minimum and 1 being maximum trust. Trust changes in increments as a function of positive and negative interactions. In the hysteresis model, trust is dependent on historical values, and builds asymptotically to the maximum value in successively smaller increments. In most situations, betrayals are dramatically inimical to trust levels, while positive experiences only modestly raise them in comparison.

Cyberspace is inherently multi-actor, distributed, decentralized, and dynamic. The distributed nature means that data is generated and actions are taken at dispersed sites. Decentralized means that controls and decisions are under no fully central authority. Dynamic means that much of cyberspace is constantly changing, implying that very little can be relied upon to be static in nature. As people, devices, and resources come and go and carry out various functionalities, there is a great challenge inherent in evaluating and using trust as a basis for entering into system activity and engagement. At a minimum, there must be support for mechanisms for tracking and modeling events that are relevant to trust assessment [8,13].

3 Orchestration of Information

As system interactions take place, information that pertains to trust modeling is accumulated. To maintain relevant trust models, the information must be gathered, managed, and made available in prescribed ways to populate trust models. Using terminology from trends in cybersecurity, we refer the need for these sources to interoperate quickly to populate trust models as the orchestration and automation problem, or briefly, just orchestration.

In Figure 2, the Interacting Cyberspace Entities are illustrated as accessible systems that source information such entities as people, devices, and cloud resources. These sources are heterogeneous, ranging from massive data management services, to real-time streaming of movies and music, and massively parallel processing systems.

To be useful, information from diverse sources must be monitored, automatically captured and made available for orchestration within the context of the activity taking place. Much of the monitored data enables cybersecurity processes. Context orchestration also includes tracking of the dynamic data history of an information source, such as a user habitually exhibiting suspicious or known bad behaviors. Multiple trust models can potentially be merged into a combined trust measure. Trust levels associated with a source must be adjusted in nonlinear increments over time. To mitigate potential harm and to support positive outcomes, a decision-making engine must be supported to direct action actuations that instantiate appropriate responses. Responses could range from simply continuing activity as usual, modifying how the interaction is taking place, or actually shutting down activity altogether because of low trust.

4 Monitoring Systems and Trust

When a customer accesses an electronic commerce system

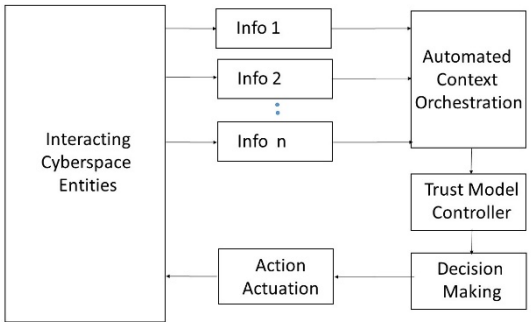


Figure 2: Trust monitoring and control framework

like Amazon.com, many pieces of information are gathered, including what items are purchased, browsed, or placed on a wish list; the length of time spent looking at specific products or types of products; the products that were reviewed or rated; product reviews that were examined; and the zip code of the customer [17]. These data populate models that are specific to the individual customer. These use various modeling, statistical, and predictive analytical methodologies, such as collaborative filtering, decision trees, regressions, and deep learning neural networks. These analyses are remarkably accurate in profiling customers, classifying them according to their age, gender, income level, and buying patterns. Not limited to just electronic commerce, similar models have many applications for which there is potential to use evidence and modeling to identify the likelihood of future outcomes [7].

There is considerable commonality between the types of analytics used in e-commerce and the concept of trust. The concept of trust has elements of meaning that include confidence, risk, reliability, truth, belief, conviction, skepticism, and assurance. Basically, trust refers to a degree of belief on the part of one person that another will act appropriately and with integrity within a specific context. Within a situation, context, or for a given purpose, if person A trusts person B we write A → B, where A is a trustor and B is a trustee. Extending the context beyond person-to-person interactions, we consider interactions involving the acquisition of resources, seeking information, soliciting opinions, controlling or monitoring a process, carrying out a service, or making a decision. The analytics employed in commerce broadly provide approaches that can be utilized to model trust among digital entities in cyberspace.

From a cybersecurity view, interactions that require high levels of trust must rely upon encryption, including digital signatures. But encryption provides only one element needed to establish an adequate level of trust. More specifically, unacceptable outcomes can easily occur even when all of the communication between A and B provides confidentiality, integrity, and non-repudiation.

An endpoint user must have a reasonably high level of trust in a system that is accessed. In some sense anthropomorphizing, we assert that the system itself must have some means of trusting the user, at least for access control. Thus, we assume that all entities must be both trusters and trustors. How should a system know that a user is trustworthy and should be granted access privileges? One approach is to monitor specific user behaviors [2, 15]. Some suspicious behaviors exhibited by a user include the following: a) scanning of an important port, b) carrying a virus, c) inputting security sensitive keywords, d) using proxies, e) making multiple unsuccessful login attempts, f) logging in frequently, g) originating access from an unusual IP address or location, h) spending an unusually amount of time logged in, i) atypical frequency of usage, j) atypical data storage usage, k) attempting to access the accounts of another user, and l) triggering atypical data error or packet loss rates. Some of these behaviors can be detected through the use of intrusion detection systems, such as Tcpdump, is used as long as the network card is set to licentious mode [18]. System logging and audit trails, bandwidth monitors, firewalls, and various network management tools can reveal a number of these anomalies [9,19,20,21, 22].

Capturing and parameterizing these user behaviors and using them to populate functional expressions provides a modeling framework for evaluating trust. Bayesian networks, fuzzy logic, and the analytical hierarchy process are modeling frameworks that can provide quantitative trust models [5, 18]. General principles of importance in modeling user behavior include the following:

- As user behaviors age, they become less important.
- Abnormal user behaviors incrementally diminish trust levels
- Normal user behaviors incrementally increase trust levels.
- Recent user behaviors are of high importance in trust modeling.
- Data for large numbers of users over time is critical in modeling user behaviors.
- Increases in trust levels increase slowly – the slow rise principle.
- Decreases in trust decrease rapidly – the rapid fall principle.

Organizations often evaluate commitments to cloud computing carefully because of concerns for security and loss of control of their data. Hence, once an organization makes a cloud computing commitment they normally have a high level of trust that Quality of Service (QoS) agreements will be met. However, experience shows that in practice that service levels can easily fall short, quickly impacting trust negatively. This leads to the need to fully monitor performance in the cloud, including populating trust models.

5 Identity and Trust as Assets of the Individual

The digital identity of a person is the collection of available information stored in a system that characterizes them as an individual. A digital identity typically includes information like user names, passwords, and purchasing history. An important ethical issue concerns privacy, in that it is widely held that publically available digital identities, even with personal information suppressed, can often easily be used to discover the individual's personal identify. The country of Estonia has

established a state issued digital identity [14]. Estonians carry national ID cards with an embedded chip that employs public-key encryption to access electronic services. These services are comprehensive, and support authentication and access for services such as health insurance, bank accounts, voting, and travel. In China, nearly all of their approximately 1.4 billion citizens is in a facial recognition database. A system called the Dragonfly Eye, can scan and identify an individual from a database in just a few seconds. In conjunction with images captured by huge numbers of security cameras, technologies like Dragonfly Eye are being employed to keep people under surveillance, capture fugitives, track purchases, and help prevent crime. The assertion is that such systems will make the country safer. Civil liberties advocates express great concerns about violations of privacy that are inherent in these types of systems.

In 2004, Kim Cameron developed the following seven laws of identity;

1. User Control and Consent – Information identifying a user must have consent
2. Minimal Disclosure for a Constrained Use – Limit the personal information disclosed to only what is necessary
3. Justifiable Parties – Disclosure of identifying information must be justified
4. Directed Identity – Identity systems must fulfill their purpose, yet avoid correlation handles
5. Pluralism of Operators and Technologies – Multiple types of identity providers must be supported
6. Human Integration – The human user must be a component of the distributed system integrated via unambiguous communication between humans and machines and supported by multiple identity providers
7. Consistent Experience Across Contexts - Support separation of contexts through multiple operators and technologies

Adhering to the spirit of these seven laws is critical to the instantiation of a trust-based distributed system [6]. Maintaining reputation data is a primary approach to employing evidence to drive trust evaluation [3, 4, 14]. Reputation is defined as "an expectation about an agent's behavior based on information about or observations of its past behavior [1]." Most online e-commerce systems record and publish reputation using things like 5-star ratings.

Reputation factors that can be used in modeling are numbers of positive and negative ratings, a history tracking of ratings, and popularity factors. Reputation is a complex concept that is not exactly the same as trust. However, reputation is typically viewed as an antecedent of trust, providing a fundamental source of evidence to use in establishing trustworthiness.

6 Blockchain Technology and Trust

The purpose of Identity Management is to appropriately connect a specific entity to one that is remote. Most identity management systems are either centralized with a single authority or federated with a trusted identity provider supporting a single sign on. Federation avoids proliferation and replication of identity credentials, but the storage and transmission of logins, passwords, and auxiliary authentication tokens does leave open possibilities for identity theft. Identity is obviously a fundamental asset of an individual entity, and we assert that trust and reputation can and should be as well.

Blockchains are a relatively recent technological advance, with cryptocurrencies such as Bitcoin being well-known examples. Blockchains have several characteristics that result in a transaction having a high level of trust. Blocks are stored in ledgers that are distributed, accessible, and have a unique hash identifier [12]. Blocks have the immutability property, in that they cannot be changed. A consensus algorithm ensures that all copies of the distributed ledgers are identical. Data can be appended to a Blockchain but prior data cannot be modified, so there is no supervising central authority [12]. The first and most prominent use of blockchain technology is the capability to transfer funds transparently in a peer-to-peer fashion, avoiding the need to involve money-management organizations such as banks. By virtue of not being issued by any central authority, blockchain systems have a built-in immunity to regulation. Private blockchains have been proposed and developed, but inherently have conditions on who can interact with the chain, basically destroying a critical feature of the technology. Blockchains applications established or under development include monitoring of supply chains, managing digital IDs, protecting copyrights, voting digitally, transferring titles, tracking weapons, managing internet of things devices, and tracking prescription drugs. Blockchains provide a natural mechanism for individualizing trust and reputation. With blockchain technology, trust can be established by validating a transaction and blocks for tamper-proofing, and verifying the resources availability to guarantee the transaction execution. Essentially, blockchain systems are unhackable. Another advantage of basing an identity management system on Blockchain technology stems from the well-known linkability problem of centralized or federated identity management systems. For example, even if a user created distinct logins and passwords for, say, eBay and Walmart ordering systems, a hacker might link the identifiers by matching related information, like credit card numbers or shipping addresses. Blockchains provide technological mechanisms that reduce or eliminate the need for institutions to provide or adhere to contracts, procedures, and regulatory systems.

7 Mathematical Modeling of Trust

Developing a distributed computational trust modeling framework at scale is a substantial task. We view trust models with peer-to-peer interactions as a community, similar to social networks, with edges that model the relationships between peers. This provides a means of identifying how actors interact with each other and how trust evolves over time through appending new interactions as edges. The interactions between actors can be represented in a directed graph $G=(V,E,W)$ where V denotes a finite nonempty set of vertices as actors, $E \subseteq V \times V$

indicates a set of direct associations (interactions) of ordered pairs of nodes/actors, and W denotes judgments in the form of weights. In our work, an edge represents a direct judgment based on an interaction between two parties. The phenomenon of evolving trust is elusive, and motivates the approach used in the analysis in our model. We first consider the topology of the network as a large community G that may consist of many sub-communities/sub-graphs G^'=(V^',E^',W^'). The edges hold weights that are used as rating values. As interactions proceed, those edges dynamically change and evolve over time. The outcome of the model is a global trust score that is linked to a user. This score reflects the experiences of all peers that interacted with the holder of the trust score. The trust model introduced in [3] is one example. Called "TrustMe", this model is reputation-based and consists of several factors. To accommodate the many varying contexts in cyberspace, the TrustMe metric can be adapted. In formal terms, this model handles peers/entities and their interactions denoted as follows: $e \in E \equiv \{e_1, e_2, \dots, e_n\}$, and $i \in I \equiv \{i_1, i_2, \dots, i_m\}$. Entity e can be viewed as a composition of subsets of popularity, and neighbor, whereas interaction i is a composition of rating, timestamp, and context subsets.

$$e \equiv \{P \cup D\} \equiv \{\{p_1, p_2, \dots, p_n\} \cup \{d_1, d_2, \dots, d_n\}\}$$

$$i \equiv \{R \cup H \cup C\} \equiv \{\{r_1, r_2, \dots, r_m\} \cup \{h_1, h_2, \dots, h_m\} \cup \{c_1, c_2, \dots, c_m\}\}$$

$$r \equiv \{r\} \quad \text{for one-way rating}$$

$$r \equiv \{r_{e_i}, r_{e_j}\} \quad \text{for two-way rating}$$

These factors can be measured with a value that falls between minimum and maximum values. For example, the minimum value may represent the ultimate dissatisfaction and the maximum value represents the ultimate satisfaction. The *Popularity Set* represents the level of sociality of a peer/entity in a given community, and its values range between

$$[0, 1] \equiv [fully\ unpopular, fullyly\ popular]: 0 \le p_i \le 1\ where\ i \in \{1, \dots, n\}.$$

So, trust (T) can be computed using the driving forces: e and i.

$$T \equiv \{t_1, t_2, \dots, t_n\}$$

$$T_e(E \cup I)$$

The trust attributes/factors collaborate together to build the trust model and generate a trust score. The following formula specifies the trust model and Table 1 summarizes the factors.

$$T(e_i) = \left(\theta * d^+ * \left(median\left\{_{j=0}^{d^+} tv_j * p_j * h_j * r^+(e_i, e_j)\right\}\right) + * d^- * \left(median\left\{_{j=0}^{d^-} tv_j * p_j * h_j * r^-(e_i, e_j)\right\}\right)\right)$$

In order to guarantee the efficiency of a trust model, a fraud/deception model must be plugged into the equation. The fraud model is a complementary model that aims to filter out dishonest feedback based on predefined criteria. Figure 3 shows a general state transition diagram of the trust model. The figure depicts how the fraud component interacts with the trust component to filter out dishonest ratings/feedback. The diagram also illustrates the dynamism of trust and popularity when an interaction takes place. A new trust score will be generated and updated after the ratings are filtered out by the fraud analyzer, whereas the popularity value will be updated if a new relationship is established. Additionally, the decision of categorizing a peer as trusted or distrusted is based upon the value of a threshold so that $if\ (T \ge Trust\ threshold) then\ state = trusted$. The diagram is divided into three sections (popularity, trust, and fraud analyzer). Each section portrays the change of states from one to another according to specified rules.

Table 1: Summary of the factors of the trust me model

Factor	Description	Range
h	indicates the prevalence of the rating historically (the age of the rating/timestamp).	[0, 1]
p	indicates the level of sociality (how the user is popular in a community).	[0, 1]
$\boldsymbol{d^+}$	denotes the centralization of the positive received ratings.	[0, 1]
$\boldsymbol{d^-}$	denotes the centralization of the negative received ratings.	[0, 1]
tv	denotes the transaction volume (context); to ignore its influence, let $tv=1$.	[$Min, $Max]
d	denotes the number of transactions that one user performs. the total number of incoming rates for a user representing the number of positive ratings and the number of negative ratings.	[0,Max]
$\boldsymbol{\theta}$	a weight for the second part of the equation; determining the influence level of this part.	[0, 1]
$\boldsymbol{\gamma}$	a weight for the second part of the equation; determining the influence level of this part.	[0, 1]

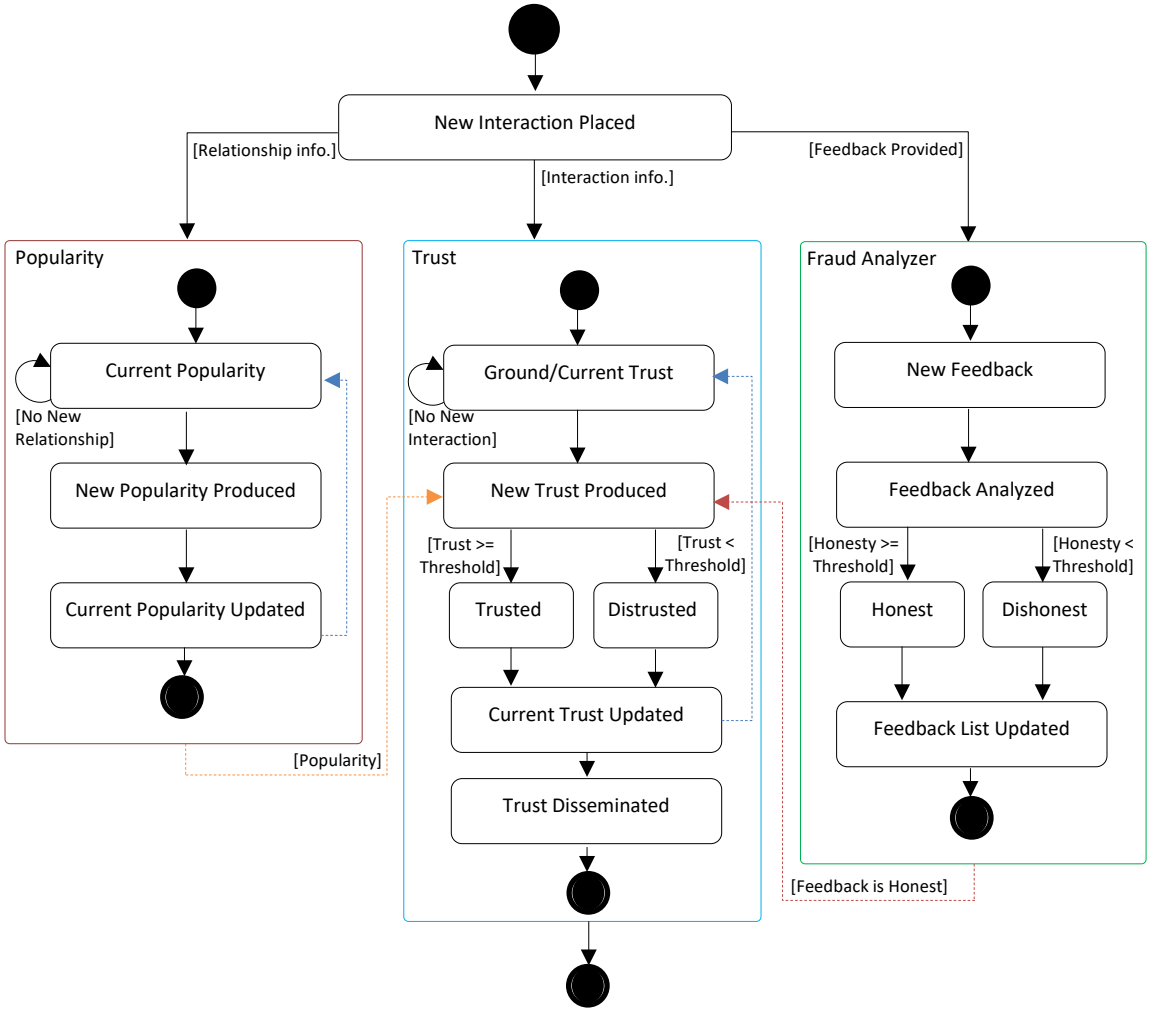


Figure 3: A State Transition Diagram of the TrustMe Model

The TrustMe model provides an indication of the computational modeling and work involved in invoking and maintaining a near real-time trust model that can be fully decentralized.

To empirically test the model, we use the Bitcoin dataset described in [9] that provides an example of an online community for sharing bitcoins that adheres to a social network graphical model. New actors joined the community if they found that community conditions are appropriate for exchanging Bitcoins. Also, existing actors leave the community if they found that the conditions are inappropriate. Entering and leaving a community is common when, for example, the network activity becomes trendy or when a wave of fraud occurs. Table 2 shows the network topology information.

To understand how the structure of the community evolves over time and how actors change in the environment, the network is divided into years from 2010 to 2016. Table 3 summarizes the statistics of the community dynamics over time. Figures 4a and 4b depicts how the community metrics change.

Table 2: Network topological information

Graph Metrics	Value
Graph Type	Directed
Vertices/Nodes/Actors/Users/Entities	5,881
Edges/Interactions	35,592
Diameter	11
Radius	1
Avg. Path length	3.79
Avg. Degree	6.052
Graph Density	0.001
Modularity	0.484
Avg. Number of Neighbors	7.309
Communities	22
Weakly Connected Components	4
Clustering Coefficient	0.149
Isolated Nodes	0
Self-loops	0
Multi-edge Node Pairs	4.005
Reciprocated Edge Ratio	0.56

Table 3: Summary of community statistics over time

G. Metrics	2010	2011	2012	2013	2014	2015	2016
Nodes/Actors	55	1637	3162	5161	5753	5879	5881
Edges/Interactions	142	7900	17332	30314	34539	35550	35592
Avg. Degree	2.582	4.826	5.481	5.874	6.004	6.047	6.052
Avg. Weighted Degree	7.109	8.396	7.925	6.028	6.006	6.113	6.125
Diameter	8	10	11	11	11	11	11
Avg. Path Len	3.24	3.87	3.798	3.75	3.73	3.719	3.718
Graph Density	0.048	0.003	0.002	0.001	0.001	0.001	0.001
Modularity	0.437	0.451	0.457	0.494	0.494	0.491	0.480
Possible Communities	6	11	13	15	15	17	22
Connected Components	2	2	2	3	3	4	4
Clustering Coefficient	0.066	0.099	0.120	0.136	0.144	0.149	0.149

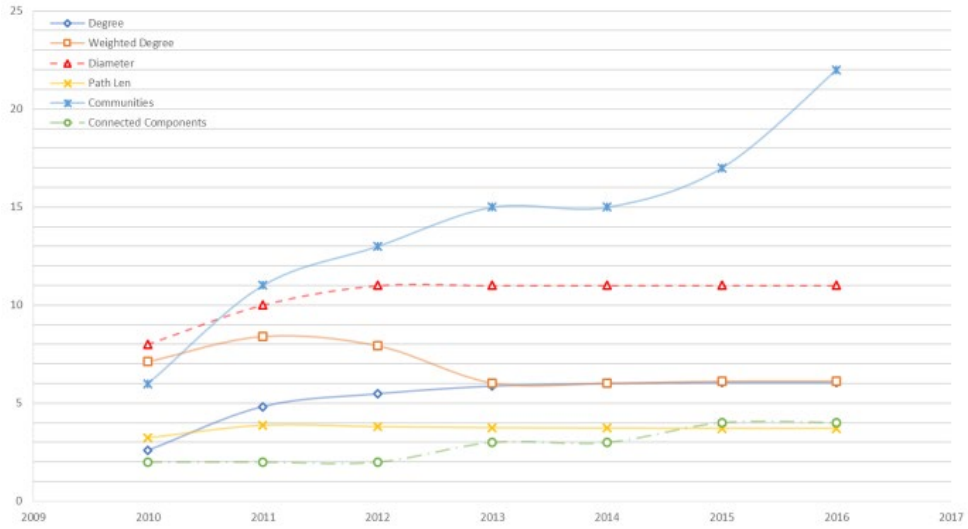


Figure 4(a): Network topology change

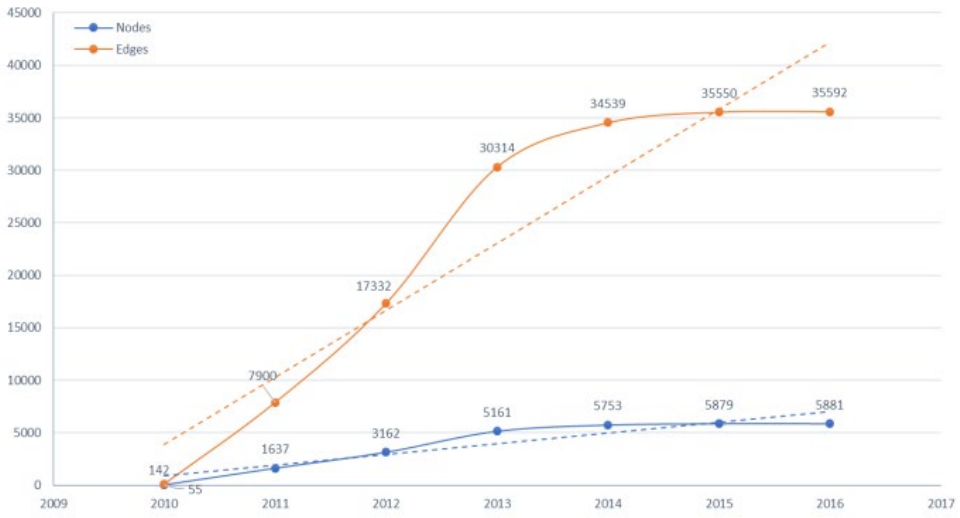


Figure 4(b): Change in the number of actors and their relationships

We observe that from 2010 to 2011, the number of new actors who joined was 1,582, which is a growth rate of 2976%. The population in 2012 was about twice what it was in 2011. There were 1999 new actors who joined the community in 2013. By 2016, only two joined the community. In terms of highest and lowest numbers of interactions, 2013 had 12,982 interactions, and 2016 had 42. It is evident that the community became less attractive in the last two years for which data is available. It is also the case that the average degree changed. The graph diameter, which is the maximal distance between a pair of nodes, remained at 11 from 2012 until 2016. This is a sign of low change in the network topology even after carrying out a large number of interactions in 2013, and represents an average of 0.019 of interactions per actor for the year.

We calculated the TrustMe metric score and the raw mean trust score, which is a simple average. The raw mean is widely used in reputation. Degree centrality denotes the number of edges a node has to other nodes. The concept of centrality is to grade nodes of a graph in terms of their importance. The positive in-degree is the number of incoming edges that hold a positive weight, and the negative in-degree is the number of incoming edges that hold a negative weight. Betweenness centrality is a measure of the importance of a node by quantifying how many times this node serves as a bridge between the shortest paths of other nodes. Eigenvector centrality measures the importance of a node by calibrating the importance of the neighboring nodes to which it is linked. A high eigenvector-centrality measure means that the node is connected to many other nodes that have high eigenvalues and so forth. We calculated the top 10 actors for each metric.

Table 4 summarizes the top 10 actors who have the highest score for the six metrics. Betweenness centrality is normalized for comparison purposes. Table 4 (f) shows the top 33 actors for the raw.mean metric obtained a 1.00 trust score, which represents ultimate trust. The details in the data reveal that all of those specific actors received exactly one positive rating, with an exception for actor 4733 who received two positive ratings. This reveals the basic problem that happens when an actor has an orphaned interaction with a positive rating due to the number of interactions not affecting the score for the raw.mean metric. The raw mean, which remains widely used in many online communities, is highly vulnerable, and can easily be exploited by dishonest actors who wish to produce a misleading score. Another indication that discredits the raw mean is that no actor in the top 10 of the raw.mean metric appears in the other top 10 tables. The other metrics are in much closer agreement with each other. We conclude that the new TrustMe metric has consistency and properties that capture nuances of the data.

Table 4 (a): Top 10 In-Degrees^{+}

$Actor$	$in.degree^{+}$	$TrustMe$
27	535	0.89
2588	411	0.74
1765	270	0.65
1982	234	0.63
1	226	0.68
865	226	0.62
7	216	0.67
4093	211	0.63
4116	203	0.66
11	190	0.62

Table 4 (b): Top 10 In-Degrees^{-}

$Actor$	$in.degree^{-}$	$TrustMe$
3669	75	0.00
1982	45	0.63
1342	45	0.47
1765	41	0.65
865	38	0.62
2447	36	0.24
1971	33	0.33
3820	26	0.55
792	26	0.52
1999	25	0.55

Table 4 (c): Top 10 Betweenness

$Actor$	$Betweenness$	$TrustMe$
27	1.000	0.89
2588	0.438	0.74
1765	0.349	0.65
865	0.349	0.62
1	0.317	0.68
4093	0.295	0.63
2078	0.293	0.64
7	0.280	0.67
1982	0.272	0.63
1908	0.227	0.59

Table 4 (d): Top 10 Eigenvector

$Actor$	$eigenvector$	$TrustMe$
2588	1.000	0.74
865	0.927	0.62
27	0.885	0.89
1765	0.830	0.65
1982	0.738	0.63
4093	0.706	0.63
1	0.692	0.68
4207	0.643	0.60
1294	0.635	0.60
4116	0.612	0.66

Table 4 (e): Top 10 TrustMe Scores

$Actor$	$TrustMe$	$TrustMe$
27	0.89	0.89
2588	0.74	0.74
1	0.68	0.68
7	0.67	0.67
4116	0.66	0.66
1765	0.65	0.65
2078	0.64	0.64
978	0.64	0.64
1982	0.63	0.63
4093	0.63	0.63

Table 4 (f): Top 10 Raw Mean Scores

$Actor$	$Raw.Mean$	$TrustMe$
490	1.00	0.51
774	1.00	0.51
1082	1.00	0.51
1221	1.00	0.51
1286	1.00	0.51
1299	1.00	0.51
1459	1.00	0.51
1503	1.00	0.51
1618	1.00	0.51
24 More	1.00	0.51

Another type of issue is revealed through examination of actors such as number 1982, who appears in all tables. A closer look shows that this actor obtained 234 positive ratings, representing 84% of all received ratings, and 45 negative ratings, representing the other 16%. When the weights of these ratings are summed, we found that this actor has 544 in positive weighted ratings and -342 in negative ones. This reveals that the negative ratings are 39% of the entire received ratings and the positive ones are the other 61%. This suggests that metrics, like the TrustMe model, that has a punishment mechanism when ratings are negative, might be overly tolerant. Investigation into the tradeoffs between the reward and punishment engines may be called for.

Conclusion

System administrators employ security software systems that carry out real-time monitoring of incoming traffic to detect and fend off malicious intruders. Defensive and offensive security procedures must be integrated to collectively manage the threats. Companies like Amazon capture real-time data and model their customers individually to serve them better and run their business efficiently and profitably. Similarly, we argue that it is feasible for arbitrary users in cyberspace to monitor and orchestrate incoming data arriving from systems that they use. These data can be orchestrated and drive trust models. A graph-theoretic model called TrustMe is described and analytical results are presented. The model can be used with detailed peer-to-peer blockchain data and is more insightful than a raw mean metric. The models described can support decision making to provide secure computing and satisfactory interactions and outcomes, regardless of the types of remote systems and people involved. Although challenging, the technologies exist to support a trust-based computing framework, resulting in safe, purposeful, and goal-fulfilling engagement of people and systems.

References

[1] A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities," *Proceedings of the 33rd Hawaii International Conference on System Sciences*, HICSS, p. 6007, 2000.

[2] M. Alruwaythi, K. Kambhampaty, and K. E. Nygard, "User Behavior Trust Modeling in Cloud Security," *Proceedings of the 5th Annual Conf. on Computational Science & Computational Intelligence (CSCI'18)*, Las Vegas, 58:378-386, December, 2018.

[3] A. Bugalwi, A. Algarni, and K. E. Nygard, "A Trust Model for Bitcoin using Unsupervised Machine Learning," *Proceedings of the 31st International Conference On Computer Applications In Industry And Engineering (CAINE 2018)*, New Orleans, pp. 207-213, 2018.

[4] A. Danek, J. Urbano, A. P. Rocha, and E. Oliveira, "Engaging the Dynamics of Trust in Computational Trust and Reputation Systems," Jędrzejowicz, P., Nguyen, N. T., Howlet, R. J., and Jain, L. C. (eds), Agent and Multi-Agent Systems: Technologies and Applications. KES-AMSTA 2010. Lecture Notes in Computer Science, Vol 6070, Springer, Berlin, Heidelberg, 2010.

[5] B. Dewangan and P. Shende, "The Sliding Window Method: An Environment to Evaluate User Behavior Trust in Cloud Technology", *International Journal of Advanced Research in Computer and Communication Engineering*, 2(2):1158-1162, 2013.

[6] N. Ferguson, *The Square and the Tower*, Penguin Press, 2018.

[7] H. Harris, "Transparency, Trust, and Proprietary Predictive Analytics," Medium https://medium.com/@HarlanH/transparency-trust-and-proprietary-predictive-analytics-e4155030c55f, Feb 27, 2017.

[8] T. Khan, K. Singh, L. H. Son, M. Abdel-Basset, H. V. Long, S. P. Singh, and M. Manju, "A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks," *IEEE ACCESS*, 7:58221-58240, May 15, 2019.

[9] S. Kumar, B. Hooi, D. Makhija, M. Kumar, V.S. Subrahmanian, C. Faloutsos, "REV2: Fraudulent User Prediction in Rating Platforms," 11th ACM International Conference on Web Search and Data Mining (WSDM), 2018.

[10] K. Nygard, A. Bugalwi, M. Alruwathi, A. Rastogi, K. Kambhampaty, P. Kotala, "Elevating Beneficence, in Cyberspace with Situational Trust," *Proceedings of 32nd International Conference on Computer Applications in Industry and Engineering*, (CAINE 2018), San Diego, pp. 160-169, 2019.

[11] V. B. Reddy, A. Negi, and S. Venkataraman, "Trust Computation Model Using Hysteresis Curve for Wireless Sensor Networks," 2018 *IEEE SENSORS*, pp. 1-4, 2018.

[12] M. Risius and K. Spohrer, "A Blockchain Research Framework," Business & Information Systems Engineering, 59(6):385-409, 2017.

[13] M. M. Singh, "A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks," *Access IEEE*, (7):58221-58240, 2019.

[14] B. Sterling, "Estonian E-Residency, an Estonian Primer," Wired, October 10, 2017.

[15] L. Tian, C. Lin, and Y. Ni, "Evaluation of User Behavior Trust in Cloud Computing," 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), pp. 567-572, 2010.

[16] J. Urbano, A. P. Rocha, and E. Oliveira, "A Socio-Cognitive Perspective of Trust," *Agreement Technologies*, pp. 419-429, Springer, Dordrecht, 2013.

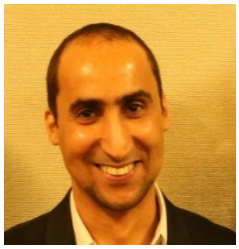
[17] J. Williams, "How Amazon's Focus on Data has Helped them Transform their Business," *Prompt Cloud*, https://www.promptcloud.com/blog/how-amazon-focus-data-business-transformation/, August 10, 2018.

[18] "TCPDUMP and LIBPCAP", [Online], Available: https://www.tcpdump.org, [Accessed 1 Jan 2019].

[19] "Top 20 IPs by Traffic-Daily", [Online], Available:

http://bandwidthd.sourceforge.net/demo/2009, [Accessed: 1- Jan- 2019].
[20] "Cisco Works Software," [Online], Available: http://www.cisco.com/public/sw-center/sw-netmgmt.shtml, [Accessed: 1- Jan- 2019].
[21] "NetFlow Monitor," [Online], Available: http://netflow.cesnet.cz, [Accessed: 1- Jan- 2019].
[22] "nGenius® Probes," [Online] Available: http://www.netscout.com/products/probes_home.asp, [Accessed: 1- Jan- 2019].

Kendall E. Nygard is a full professor and serves as department Chair of Computer Science at North Dakota State University (NDSU). He is also the founder and Director of the NDSU Institute for Cybersecurity Education and Research. He has served in Washington D. C. as a Jefferson Science Fellow and Virtual Fellow at the U. S. Department of State and as a Senior Science Advisor at USAID. Dr. Nygard is also a fellow of the International Academy, Research, and Industry Association. He is a recipient of the Chamber of Commerce NDSU Distinguished Faculty Service Award. Dr. Nygard earned his PhD degree at Virginia Polytechnic Institute. He has advised 27 PhD students and more than 150 Master of Science students. His research is widely published. Application areas in which he has conducted research include cyber security, smart electrical grid, sensor networks, unmanned air systems routing and scheduling, wireless ad hoc networks, encryption, and social media. His primary methodologies are big data analytics, optimization models, artificial intelligence, and simulation.



Ahmed Bugalwi received the Bachelor of Science degree in Computer Science from the Benghazi Institute of Technology and the MS degree in Computer Science from The Libyan Academy. Currently he is a PhD candidate in Software Engineering at North Dakota State University. Ahmed's background includes approximately 10 years in the software industry. Before joining NDSU, he worked as a lead developer and the head of technical support at the Libyan Stock Market. Ahmed's research interests include Blockchain, Software Engineering, Cybersecurity, Trust, Reputation, Privacy, and Social Networks.

Maryam Alruwaythi (Photo not available) has a PhD in Software Engineering from North Dakota State University. She has a MS in Software Engineering, a certificate in big data management and a certificate in business analysis from St. Thomas University, St Paul, MN, and a BS in Information Technology from King Saud University, Riyadh, Saudi Arabia. She is currently working as a teaching assistant in the Computer Science department at North Dakota State University. Her research interests are in software engineering, cloud computing security, and big data management.

Aakanksha Rastogi is a Ph.D. student in Software Engineering at North Dakota State University (NDSU). She also earned her MS in Software Engineering from NDSU and has 4 years of industry experience as a Software Developer and a Quality Assurance Analyst. She has instructed in the UCodeGirl summer camp program in coding and cybersecurity for middle and high school girls. Her research interests include Cybersecurity, Software Engineering, and secure software development practices, autonomous and semi-autonomous systems.

Krishna Kambhampaty earned his PhD and MS degrees in Computer Science at North Dakota State University (NDSU). He is currently a professional Software Engineer and is working towards an MBA degree at NDSU. He has over 5 years of industry experience as a Software Engineer. At NDSU he has been active in the Nurturing American Tribal Undergraduate Research and Education (NATURE) program, summer Cybercamp, the North Dakota Governor's School, and the TRIO Upward Bound program for high school students. He is a recipient of the Tapestry of Diverse Talents award from NDSU. His research interests include Cybersecurity, Network Security, Cloud Computing, and Artificial Intelligence.

Pratap Kotala is a Senior Lecturer in Computer Science at North Dakota State University (NDSU). In over 19 years he has taught a wide variety of Computer Science courses at both undergraduate and graduate levels. He has two years of experience as an IT consultant in the Health Insurance industry. His research interests include Cybersecurity, Software Engineering and Data Mining. Dr. Kotala serves as workshop leader for summer camp programs in cyber security, including special summer camps for middle and high school girls and Native Americans. He has served as organizer and panelist for North Dakota Cyber Security professional and academic conferences. His is a participant in the Stanford University Hacking for Defense program on lean methodologies. Dr. Kotala earned his PhD in Computer Science from NDSU.

The Inadequacy of Domestic and International Law for Cyberspace Regulation

Jeremy Straub*
North Dakota State University, Fargo, ND 58108

Abstract

The internet touches virtually every aspect of society and has created an interconnected global community that is has no parallel in human history. With trillions of dollars of commerce being conducted online, it has become a key component of the lifeblood of modern civilization. Unsurprisingly, it has also become a haven for criminals and a theater and medium for warfighting between nation states, terrorist and loosely affiliated groups and even individuals. This paper discusses the current problems facing the internet and the society that relies on it. It then discusses the requirements for a set of regulations necessary to facilitate the effective policing of the internet. Finally, it explains the impediments to enacting these regulations and evaluates the implications of not being able to effectively police this new global commons.

Key Words: Cyberspace, cybersecurity, cyber law, international law, autonomy, artificial intelligence.

1 Introduction

The internet has become a ubiquitous feature of the modern world. Three trillion dollars of e-commerce flows through it each year and this is projected to double within the next five years [26]. Nearly three billion individuals [24], slightly less than half the people on the planet [30], currently use social media. The internet is used by many to quickly look up information, access government records, to conduct personal and academic research and even to vote, in some areas [9, 28]. It seems that there are few parts of one's life, in highly economically developed regions, that are not touched by the internet.

In fact, even when one is not using the internet him or herself, this does not remove its relevance. The internet is integral to order-placing and fulfillment for items purchased at brick-and-mortar stores, service at restaurants and is even involved in most recreation activities. Even when one is not online, the internet may still be facilitating monitoring the individual via video surveillance [22] and moving data between its point of collection, autonomous screening systems [13] and human managers. It also facilitates normal communications between individuals and businesses via e-mail, video conferencing, social media and other mediums. The internet is even an integral part of the emergency response plan [12] in many areas.

Clearly, from the foregoing, the stakes are very high with the internet. On an average, an IT outage costs $5,600 per minute [10], though this would be considerably higher for high volume websites and service providers. Despite, and perhaps due to, the critical nature of the internet and the services that it provides, there are some that seek to impair its functionality. Others seek to steal data from companies using it [34]. These data breaches can cause losses in the millions or more [2]. An attack that coopts a physical device could prospectively cause it to damage property or even injure or kill a nearby human.

The law is meant to provide redress for losses, in cases like these and others. It is designed to deter crime, through the fear of punishment, and to punish those who fail to be deterred. However, when a crime in one country can be committed by a potentially impossible to identify individual on the other side of the world, the ability to deter criminal behavior, the ability to seek redress for losses and even the ability to punish the offender are severely undermined. Questions about what law applies, the priority of prospective cases against an offender, if he or she is even located, and extradition make pursuing all but the most damaging cases prohibitive. Acts by, on behalf of, or supported by nation states raises the potential that even if a perpetrator is located, he or she may not face justice.

This paper discusses the issues with both U.S. domestic and international law for policing the internet and their implications. It presents requirements for domestic and international regulations aimed at resolving some of these issues. Finally, it discusses the factors that may make implementing these or similar regulations problematic and what the implications of this are for near-term internet regulation. The juxtaposition of the identified issues with the analysis-derived requirements and implementation issue analysis, using standard legal analysis techniques, is the principle contribution of this work.

2 Challenges of U.S. Domestic Law for Internet Regulation

The use of United States domestic law for internet regulation has two principal problems. The first is technical relevance. The second is jurisdiction.

In terms of technical relevance, laws have difficulty keeping up with technical advancements. The introduction of new technologies creates new forms of crime, methods of committing crimes, types of property to be stolen, damaged or

* Institute for Cyber Security Education and Research. Phone: +1-701-231-8196. Fax: +1-701-231-8255. Email: jeremy.straub@ndsu.edu.

ISCA Copyright© 2019

fought over and new methods that may transgress or create liability under existing laws. In some cases, lawmakers try to combat this by creating forward-looking or broad laws; however, these typically have unintended consequences and ensnare behavior beyond what legislators sought to sanction.

In 1978, Florida enacted the United States' first computer crime law, its Computer Crimes Act [16] following publicity regarding an event at the Flagler Dog Track. In response to the several prominent activists, a case regarding Milwaukee's "414 hackers" and the movie *WarGames*, among other factors, laws in other states followed and in 1984 the first federal law, the Counterfeit Access Device and Computer Fraud and Abuse Act, was enacted [16]. Notably the computer crime aspect was added to legislation primarily designed to focus on banking. In 1986, the Computer Fraud and Abuse Act was enacted with a focus on computer access as part of fraud, unauthorized access malicious damage and password trafficking [16].

Jeong and McSiggen [19] contend that the media hype and perception of a hacker as having "the same over-driven personality" and looking "the same: young, white, male" combined with a perception of a "technologically incompetent establishment" created a persistent perception of a hacker and a "anti-hacker panic" in Washington that led to the 1984 and 1986 laws (with a clip from *WarGames* actually being shown at the beginning of a hearing for the 1986 law) [19]. This resulted in a law that they argue was "already problematically over-broad, but fated to become worse over time" [19].

Problematically, the aforementioned can result in laws that are so broad as to be unclear as to what acts they are prohibiting (or creating prospective civil liability for) and laws that are not triggered by behavior similar to, but not exactly the same as, what they were designed to proscribe. One prospective solution to this is to define bad acts in terms of the consequences that they produce or are designed to produce. This, however, is inherently problematic as the former (what is produced) makes individuals responsible for actions' results – instead of the actions themselves. The latter, what effect actions are designed to produce, can be equally problematic as it requires proof of intent. This problem, though, is not specific to technology law.

This general problem is illustrated by California's assault law: "An assault is an unlawful attempt, coupled with a present ability, to commit a violent injury on the person of another" [7]. From this, the Judicial Council of California Criminal Jury Instructions instruct jurors that to convict someone of assault the following must be met [27]:

1. *The defendant did something that was likely to result in the use of force against someone else;*
2. *The defendant did so willfully;*
3. *The defendant was aware of facts that would lead a reasonable person to believe that this act would directly and probably result in force being applied to the other person; and*
4. *When the defendant acted, s/he had the ability to apply force to the other person.*

Points one and four can be reasonably objectively determined (albeit with some ambiguity from terms like "likely to result in" and "ability to apply"). However, points two and three require evidence to suggest that a defendant held a particular state of mind (point two, "did so willfully") and had particular knowledge (point three, "aware of facts").

How then, is intent and knowledge determined? It must be inferred from evidence, such as proximal activities, attitudes and statements of the defendant which would likely come from observations of this individual and his or her actions and statements. Of course, in the cyber realm, this observation may be different. On one hand, online statements and activities are preserved technologically. On the other hand, an attacker need not be visible by others when committing a crime (or tortuous act) by computer. This becomes even more problematic when the defendant (and witnesses) are located outside of the jurisdiction of prosecution or civil suit.

The second issue with U.S. domestic law for internet regulation is one of jurisdiction. Jurisdiction is "the authority given by law to a court to try cases and rule on legal matters within a particular geographic area and/or over certain types of legal cases" [15]. This inherently impacts prosecutions and civil suits as, if the court cannot try a case due to a lack of jurisdiction, charges cannot be filed there, or a civil complaint cannot be made there. In some cases, this results in a need to simply go to another court. However, prosecutors are limited in where they have statutory authority to bring cases and may find a matter outside of their reach due to jurisdictional issues.

In the simplest case, the alleged perpetrator, crime and its impact (or plaintiff and defendant, in a civil case) are in the same physical area. This limits jurisdictional questions to whether local (municipal), state or federal law (or perhaps more than one) is implicated. In a more complex case, an alleged perpetrator is contended to have committed a criminal act in one area, potentially traveling through communications channels in numerous areas and having a result in a completely different area. This though, is not even close to the most complex case.

In an even more complex case, the alleged perpetrator may be alleged to have committed a bad act in one area that caused impact in numerous areas – perhaps even areas that the alleged perpetrator didn't specifically target or intend. In this scenario, could the perpetrator be legitimately charged in multiple locations? It could be argued that this runs afoul of the constitutional prohibition on double jeopardy (an individual being tried twice for the same crime); however, courts have held that each sovereign (each state and the federal government) is separate and that each can enforce its respective laws [14]. Problematically, this would allow a single entirely domestic crime to, theoretically, be tried 51 times (once in each state and once at the federal level).

Time standards [11] for state trial courts suggest that virtually all felony cases (at least 98%) should be completed within a year and that most (75% to 90%) should be completed within 90 to 120 days. Even at this 90-day standard, a string of successive prosecutions could take 13 years and, at the one-year standard, an 18-year-old defendant might be 69 before completing the gauntlet – prospectively held in pre-trial custody without having ever been found guilty of anything. While this is, of course, a

very extreme and unlikely example, it illustrates a key problem with the current system. Further, his example still presumes that the criminal act and all of its impacts are constrained to the United States.

3 International Law & The Internet

When a crime or tortuous act crosses national borders, things get even more complicated. In this case, they are governed by international law. This so-called international law is actually a collection of treaties between independently sovereign states [32] as well as conventions and practices. From these treaties and conventions, a framework of activities has emerged, some of these under the auspices of the United Nations, which has a variety of courts, tribunals, councils and other bodies for dealing with issues between states. Treaties, however, are only binding on their (nation-state) signatories and thus international law varies somewhat depending on which states are implicated. In addition, in some cases, states participate in treaties subject to declarations, reservations and objections, which impact the interpretation of the treaty as it applies to them and others (e.g., see [21]).

There are many international standards for the conduct of individuals (for example, the law of the seas [21], genocide prohibition [17] and human trafficking prohibition [31]). However, for lesser crimes and crimes not necessarily of an international nature, these laws and regulations are left to states to create and litigate, subject to their treaty obligations.

This, in some cases, may result in unanticipated results. For example, individuals and businesses may find themselves subject to laws that they have no direct connection to and have not representation in the creation of. The European General Data Protection Regulation [29] has highlighted this issue, as it has required businesses around the world to accede to a European Union standard, irrespective of them not being in the European Union. In this case, the regulation is at least scoped to require some (albeit sometimes indirect) connection to European states or nationals. However, it would be exceptionally problematic if multiple states or state collections created multiple and potentially conflicting regulations.

Another example highlighting the prospective problems with international law is the case of a Continental Airlines mechanic. Mechanic John Taylor, who lived and worked in Texas in the United States [20] was tried in absentia, along with Continental Airlines, for the modification of a Continental DC-10. French prosecutors contended that an improperly attached metal strip, installed by Taylor in the United States, fell off of the aircraft and was left on a Paris runway [8] where it subsequently damaged the tire of the Concorde sending tire debris towards the wing and damaging the fuel tanks [5]. This led to its catastrophic crash [8]. While this verdict was subsequently overturned on appeal [18], the reason for the reversal was due to the improper criminalization of a professional mistake instead of a question of jurisdiction, particularly in regards to John Taylor.

A question here is of fundamental importance: when Taylor made the modification to the aircraft, did he have any indication that this plane would be going to France? If not, how could he be expected to apply the standards of French law to his conduct? What if the plane was going to go to other countries, in addition to France? Do all of their laws apply to his conduct? While, arguably, an airline mechanic would realize that the airline is in an inherently international business, the mechanic himself is performing services as an employee in a particular country and it would be unreasonable to expect him to fully evaluate the international legal context of each action.

Similarly, in the realm of computer civil liability and crime, an individual who intentionally commits a crime or engages in commerce in a jurisdiction, albeit remotely, may be choosing to subject him or herself to that jurisdiction. However, an individual who undertakes an action in a jurisdiction without a specific intent to impact another specific jurisdiction is a very different matter. Application of extrajudicial laws to conduct is particularly problematic when the action would not give rise to a civil or criminal liability in the jurisdiction that it was conducted in.

4 The Current Status

Given the foregoing, the current state of legal regulation for cyberspace is hodge-podge and generally inconsistent. What regulation does exist, particularly in determining what law may govern a transaction, mistake or attack is lacking and, in some cases, contradictory.

Under current regulations, individuals can inadvertently commit crimes against or tortuous act under a sovereignty on the other side of the world and may inadvertently fall under the law of numerous states and nations. Actions that are legal, and perhaps even required, in one jurisdiction may subject an individual or firm to criminal penalty or civil judgement in another.

Numerous factors, including where the individual is located, choice of law provisions in ‘click through’ text, where consequences of an action are and most problematically the politics of countries can determine what law applies. Even the connection (or lack thereof) to a government entity may have bearing, as certain laws treat foreign individuals different from foreign government workers or those with government connections. These laws, though, don’t deal with the complexity of unrecognized governments, contractors, loosely affiliated groups and similar, nor do they anticipate situations where governments may intentionally cause harm to an individual or firm, either as a target or in collateral to another action. As just one example, in the United States, the Foreign Sovereign Immunities Act [25] protects other governments from liability for even domestic acts that deliberately target and cause harm to U.S. nationals and others on U.S. soil.

A system of laws that makes it excruciatingly difficult to determine what is prohibited and does not deter proscribed behavior. Further, a system that allows cases to be re-litigated over and over between jurisdictions gives an insuperable benefit to the party with the largest legal budget. While every major new technology may introduce issues of law and policy that take time to identify and work out, the current system of regulations

for cybercrimes and torts is untenable and in need of rapid rectification.

5 Towards International Regulations

This section considers the characteristics that national and international regulations would need to have in order to be successful at resolving the issues described in the previous section.

5.1 Form of Regulation

A critical task on the pathway to the implementation of regulations to resolve the aforementioned issues is to determine what form or forms of regulation would be suitable. There are a limited number of options available.

For the domestic (United States) issue, there are principally two different legislative approaches. The first is a federal law (or potentially constitutional amendment, if a law is insufficient due to a lack of authority or conflicting constitutional language). The second is an agreement between the states, known as an inter-state compact [35].

The federal law (or potentially constitutional amendment) would be a preferable form of regulation as it would create consistency across the entire country. This law or amendment could be debated and enacted through standard processes.

If a federal regulation is unattainable, potentially due to an inability to arrive at political consensus or for any other reason, an inter-state compact would be another possible approach. Inter-state compacts are negotiated between the state members [35]. Then they must be approved by all participating states' legislatures. Finally, in compacts related to some subject matters, approval by the U.S. Congress is also required [35].

A third though significantly more problematic approach also exists. Because of the issue of double jeopardy [6] (an issue of U.S. Constitution interpretation), it is possible that the U.S. Supreme Court could create a procedure for determining jurisdiction to preclude double jeopardy situations from occurring (or to resolve them when they do occur). This sort of ruling could create a judicial regulation with a similar effect to a legislatively enacted one. Problematically, this precludes the significant debate that the legislative process would entail and may result in a regulation without the necessary rigor and nuance, as it would be created in a ruling in response to a specific case and may only narrowly apply. The court has previously caused some confusion with apparently contradictory rulings on double jeopardy [1], and it is possible that this trend could continue if the court ventured into this area. It is also critical to note that this sort of a judicial procedure would require the court to reverse its current position on prosecution being allowable by each sovereignty (each state and federal) under its applicable laws [23].

Thus, a federal law (or, if needed, constitutional amendment) would be the most straightforward and consistent across the country. If this cannot be enacted, a widely adopted inter-state compact would be another viable option. If neither of the foregoing occur, the courts may be called upon to resolve this issue with a ruling (or set of rulings).

At the international level, a similar set of challenges exist. However, there is only a single viable solution: a treaty. This treaty could prospectively be developed through the United Nations. This would have logistical and organizational benefits over a collection of bilateral or small group multilateral treaties. Any treaty only applies to its signatories and this may result in some nations and some situations not being covered.

In addition to covering civil and criminal activities occurring within and between participating nation-states, a treaty could also deal with cyber warfighting, cyber terrorism and groups that are loosely affiliated with government entities. Each of these issues presents considerations that are separate from, but related to, civil and criminal matters. Additionally, the treaty could deal with the determination of what category that a particular circumstance falls into and potentially provide a mechanism for seeking civil damages for a nation-state act (including potentially state-sponsored acts and acts by loosely affiliated organizations) against a private individual or firm.

It is important to note that because of language in Article VI of the U.S. Constitution that makes treaties the "supreme law of the land" [3], any treaty that the United States entered into would become binding on the states. Thus, a treaty could potentially represent a partial or even complete solution to the domestic issues, in addition to the international ones that it is primarily designed to solve.

5.2 Required Regulation Characteristics

A set of regulations to resolve the aforementioned issues would need to have a variety of characteristics. In particular, it would need to provide answers to a number of critical questions. These include venue selection, how to combine (if they are combined) cases from multiple jurisdictions, how fact finding should work, what evidentiary standards should be used when these are in conflict and which state pays for incarceration (and where the convict should be incarcerated) or receives fine payments, if someone is found guilty in a criminal matter. Each is now discussed.

Venue selection determines where the trial (either criminal and/or civil) would occur at. Typically, venue is determined by the jurisdiction; however, in a case with numerous concurrent jurisdictions, cases would either need to be consolidated into a single trial at a single venue or the trial process would need to occur across multiple locations. In the case of multiple trials, a question would need to be answered as to whether these should be concurrent or sequential processes. Regulations would need to specify whether trials are to be consolidated and, if so, where and how or if concurrent trials will occur. If these trials will be sequential, an order of precedence would also need to be developed.

If trials are combined, a question would arise as to how to combine them. Procedures exist for civil matters (such as class actions) that may be effective for this. For criminal matters, options include limiting the case to a single jurisdiction's case (perhaps whichever is determined to be the strongest between all of the prospective cases), limiting the case to one charge in

regards to each matter (e.g., choosing particular charges from relevant jurisdictions, potentially due to elements of a crime being unique to a particular jurisdiction or its laws), or combining the cases in some other way.

If cases are combined, questions of how to resolve differences between evidentiary standards (i.e., what can be entered into evidence) between jurisdictions and how fact finding occurs would need to be answered. Presumably, for a combined case to be effective, there would either need to be a method for resolving evidentiary questions and producing a single set of evidence or a mechanism that limits access to evidence to fact finders for each jurisdiction in accordance with jurisdictional standards. Similarly, a question arises as to whether a single fact finder should be used or whether it is better to have multiple fact finders. In many cases, a fact finder can either be a judge or a jury, at the defendant's option.

Additionally, in combined criminal matters, if a defendant is convicted there is a question of which jurisdiction (or jurisdictions) should pay the cost of the incarceration of the convict, if the individual is sentenced to a term of incarceration. A policy for determining location and cost assignment or sharing would need to be arrived at. If the defendant is ordered to pay a fine, the opposite question would arise as to what jurisdictions receive the funds and how they are divided (if they are divided).

Finally, an additional consideration is how cases with multiple defendants, potentially involved in the incident from multiple locations, should be carried out. The consolidation of the trials of multiple defendants may have economic and expediency benefits; however, it further complexifies each of the aforementioned considerations. A question of how strongly tethered defendants' actions should be to trigger consideration of consolidation (if consolidation is to be adopted as a general principal) is also raised, particularly if one side or the other derives particular benefit from the consolidation. How to deal with chains of defendants (where defendant one's actions are tethered to defendant two's actions which are tethered to defendant three's actions, but defendant one and three would not meet the tethering standard independently) must also be addressed.

5.3 Coverage of Proposed Regulations

Generally, the proposed regulations should be designed to cover the implementation and interaction between criminal statutes related to multi-jurisdictional and cross-jurisdictional issues. Cyberattacks would be one form of conduct that would be covered by these laws; however, a well-defined framework could also cover other related issues such as remote control of robots or unmanned aerial vehicles (UAVs) where the robot or UAV commits a crime in one jurisdiction, while being operated from another.

It is important to note that this framework could focus on the interactions between existing laws and would not necessarily need, in its most minimal form, to create new laws. The framework would handle interactions under cybersecurity-specific laws such as the Computer Fraud and Abuse Act as well as cybersecurity crimes committed under other laws (for example, in the United States, state-level theft, murder and assault laws). In many cases new laws would not be needed, as existing laws cover the criminal conduct whether it is conducted by a human directly or via a computer system. A more robust framework might establish shared definitions of certain types of criminal activities and some statute standards. These shared definitions and statute standards would be particularly helpful for the international treaty approach, as conduct expectations may differ significantly across national borders. The European Union's Data Protection Directive, for example, used the model of providing statute standards that union members were expected to implement in their local laws [4].

Civil law actions can suffer from similar considerations as criminal ones. While the most basic framework might cover only criminal matters, civil matters could be covered by the same or a closely related framework. Having the two unified would be beneficial for understanding, because civil actions for damages may also arise from the same conduct as that which causes prospective criminal liability. Given this, the most robust framework would cover both criminal matters as well as civil matters arising under contract, tort and other laws.

6 Impediments to Regulation

Given the benefits prospectively produced, it would be ideal to presume that this problem could be expediently solved without significant disagreement. However, given conflicting needs, laws and desires, this seems unlikely. By considering the process required to produce regulations, the potential pitfalls can be identified.

There are three key steps to implementing any sort of regulations in this area. The first is the need to identify one or multiple solutions that can be implemented as federal legislation, an inter-state compact or a treaty. The second is a need to generate consensus around one or multiple solutions. The third is to implement the legislation, compact or treaty itself. Each of these, of course, is a significant undertaking and presents a number of prospective impediments to regulation enactment.

The identification of possible solutions to fill the presented regulatory need is a clear area of critically needed future work. Specifically, this process will entail the identification of candidate solutions, which effectively resolve the problems discussed, and then their comparison to the different existing laws and political will of the prospective implementing states (and/or nation-states, in the case of an international treaty). Solutions that conflict with numerous existing regulations, however ideal or elegant, may find their pathway to implementation intractable. Alternately, solutions which fail to consider the politics of each prospective adopter may be similarly unable to find success in the second step of this process. There are also key technical considerations, as some prospective policies may require certainty regarding elements of a crime or tortuous act which are not technically feasible, or which may be problematic to collect or draw sound conclusions from, in particular scenarios.

Next, some sort of consensus needs to be reached regarding

which prospective solution will be implemented. Of course, it would be ideal for all states (for a domestic implementation) or nation-states (for an international implementation) to agree on a common approach to solving this problem; however, that seems unlikely to happen.

For a treaty, the process commonly used for multi-lateral treaties could prospectively be used. This process allows a treaty to be negotiated between a group of willing states and signed (typically ad referendum or subject to ratification, approval or acceptance) and subsequently ratified by states' legislative bodies [33]. If allowed for by the treaty (or failing that, agreed by existing treaty members), other states can later join the treaty by accession and, through this, incur the obligations and enjoy the benefits provided by the treaty [33]. This approach would, after the consensus-building required to create an initial group of agreeing states, facilitate both the consensus-building and implementation processes for an international agreement.

For domestic implementation, a similar process of creating an initial group of concurring states and allowing other states to later join could be used for an inter-state compact. Of course, the process of creating a federal law, in the United States, or amending the U.S. Constitution is well defined.

7 Conclusions and Future Work

The ability to police the internet effectively is paramount. Given the level of commerce that occurs using it and the myriad of extremely beneficial uses for it, public access to the internet must be assured. For the public to feel comfortable with internet use and attain these benefits, the internet must also be reasonably safe so that its use doesn't present any greater risk than going to a shopping mall or town hall discussion in person. Key to this safety is providing a mechanism for deterring and punishing those who commit crimes online and seeking damages from those who commit tortuous acts online.

This paper has discussed the need for reform of jurisdiction for civil and criminal cases arising from internet use and, in particular, cybersecurity incidents that occur across jurisdictions. It has shown that the current hodge-podge of laws and procedures can result in an individual prospectively being criminally charged for conduct in one jurisdiction that wasn't proscribed in the jurisdiction that he or she was in at the time that it was conducted. It has also discussed the problem that is created when an individual can be charged in numerous places for a single event or series of events which occur in a single location but have impact in multiple jurisdictions. The challenge of incidents with multiple prospective defendants in multiple prospective jurisdictions has also been discussed.

From this analysis, the challenges that would need to be addressed by a prospective legislative, treaty or inter-state compact solution to this problem have been identified. Further analysis has identified and discussed a variety of issues that may impair adoption of these regulations that are key to consider during their creation.

The immediate future work in this area is the creation of one or more draft legislative, multi-state compact or treaty proposals which feature particular answers to the questions posed herein. From these, further activities related to a given plan's adoption can be undertaken.

References

[1] A. R. Amar, "Double Jeopardy Law Made Simple," *Yale Law J.* 106, 1996. https://heinonline.org/HOL/Page?handle=hein.journals/ylr106&id=1825&div=58&collection=journals (accessed September 22, 2019).

[2] T. Armerding, "The 18 Biggest Data Breaches of the 21st Century," CSO Mag., 2018. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (accessed September 2, 2019).

[3] "Article VI of the U.S. Constitution," Cornell Law School Legal Information Institute, 2019. https://www.law.cornell.edu/constitution/articlevi (accessed September 22, 2019).

[4] M. D. Birnhack, "The EU Data Protection Directive: An Engine of a Global Regime," *Comput. Law Secur. Rev.* 24:508-520, 2008. http://law.bepress.com/taulwps/art95 (accessed November 29, 2019).

[5] Bureau d'Enquetes et d'Analyses, "Accident on 25 July 2000 at La Patte d'Oie in Gonesse (95) to the Concorde Registered F-BTSC Operated by Air France," 2000. https://www.bea.aero/docspa/2000/f-sc000725a/pdf/f-sc000725a.pdf (accessed December 2, 2019).

[6] D. E. Burton, "A Closer Look at the Supreme Court and the Double Jeopardy Clause," *Ohio State Law J.* 49, 1988. https://heinonline.org/HOL/Page?handle=hein.journals/ohslj49&id=811&div=37&collection=journals (accessed September 22, 2019).

[7] "Chapter 9. Assault and Battery", Statute, "The Penal Code of California," 1872. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?chapter=9.&part=1.&lawCode=PEN&title=8. (accessed September 19, 2019).

[8] N. Clark, "Continental Airlines Found Guilty in French Concorde Disaster," New York Times, 2010. https://www.nytimes.com/2010/12/07/world/europe/07concorde.html (accessed September 18, 2019).

[9] P. Collier and P.C. Vicente, "Votes and Violence: Evidence from a Field Experiment in Nigeria," *Econ. J.* 124:F327-F355, 2014. doi:10.1111/ecoj.12109.

[10] M. Copeland, "The 20 | The Cost of IT Downtime," 20, 2018. https://www.the20.com/blog/the-cost-of-it-downtime/ (accessed September 18, 2019).

[11] R. V. Duizend, D.C. Steelman, and L. Suskin, "Model Time Standards for State Trial Courts," 2011. https://www.ncsc.org/Services-and-Experts/Technology-tools/~/media/Files/PDF/CourtMD/Model-Time-Standards-for-State-Trial-Courts.ashx (accessed September 19, 2019).

[12] B. A. Foodman and H. W. Foodman, "Internet Based Security, Fire and Emergency Identification and Communication System," US6975220B1, 2005. https://patents.google.com/patent/US6975220B1/en

(accessed September 18, 2019).

[13] M. V. Garoutte, "System for Automated Screening of Security Cameras," US6940998B2, 2005. https://patents.google.com/patent/US6940998B2/en (accessed September 18, 2019).

[14] S. Guerra, "Myth of Dual Sovereignty: Multijuris dictional Drug Law Enforcement and Double Jeopardy," *North Carolina Law Rev.* 73, 1994. https://heinonline.org/HOL/Page?handle=hein.journals/nclr73&id=1171&div=27&collection=journals (accessed September 19, 2019).

[15] G. Hill and K. Hill, "Legal Dictionary - Jurisdiction," People's Law Dictionary, 2019. https://dictionary.law.com/Default.aspx?selected=1070 (accessed September 19, 2019).

[16] R. C. Hollinger and L. Lanza-Kaduce, "The Process of Criminalization: The Case of Computer Crime Laws*," *Criminology*. 26:101-126, 1988. doi:10.1111/j.1745-9125.1988.tb00834.x.

[17] "Human Rights - Convention on the Prevention and Punishment of the Crime of Genocide," United Nations Website, 2019. https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-1&chapter=4&clang=_en (accessed September 21, 2019).

[18] B. Jansen, "French Court Overturns Concorde Crash Conviction," *USA Today*, 2012. https://www.usatoday.com/story/travel/flights/2012/11/29/continental-airlines-air-france-concorde-crash/1734417/ (accessed September 21, 2019).

[19] S. Jeong and C. McSwiggen, "Hackers! The Myth that Warped an Industry," XRDS Crossroads, ACM Mag. Students. 20:38-42, 2014. doi:10.1145/2604998.

[20] D. Lauter, "Continental, Mechanic Guilty of Manslaughter in Concorde Crash," *Los Angeles Times*, 2010. https://www.latimes.com/archives/la-xpm-2010-dec-07-la-fg-concorde-crash-ruling-20101207-story.html.

[21] "Law of the Sea - Convention on the High Seas," United Nations Website, 2019. https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXI-2&chapter=21&clang=_en#EndDec (accessed September 21, 2019).

[22] C. Y. Liu and H.-B. Chen, "Wireless Internet Camera," USD555692S1, 2007. https://patents.google.com/patent/USD555692S1/en (accessed September 18, 2019).

[23] R. Matz, "Dual Sovereignty and the Double Jeopardy Clause: If at First You Don't Convict, Try, Try, Again," *Fordham Urban Law J.* 24:353, 1997. https://heinonline.org/HOL/Page?handle=hein.journals/frdurb24&div=18&g_sent=1&casa_token=&collection=journals (accessed September 22, 2019).

[24] "Number of Social Media Users Worldwide 2010-2021," *Statista*, 2019. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (accessed September 18, 2019).

[25] M. A. Powell, "A Call to Congress: The Urgent Need for Cyberattack Amendments to the Foreign Sovereign Immunities Act," *J. Law Cyber Warf.* 7:117-148, 2018. https://heinonline.org/HOL/Page?handle=hein.journals/jlacybrwa7&id=121&div=7&collection=journals (accessed September 21, 2019).

[26] "Retail E-Commerce Sales Worldwide from 2014 to 2023," *Statista*, 2019. https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/ (accessed September 18, 2019).

[27] Shouse California Law Group, "Penal Code 240 PC - California 'Assault' Law," Shouse Calif. Law Gr. Web Site, 2019. https://www.shouselaw.com/assault.html (accessed September 19, 2019).

[28] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System," *Proc. 2014 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS '14*, ACM Press, New York, NY, USA, 703-715, 2014. doi:10.1145/2660267.2660315.

[29] C. Tankard, "What the GDPR Means for Businesses," *Netw. Secur*. 2016:5-8, 2016. doi:10.1016/S1353-4858(16)30056-3.

[30] The World Bank, "World Development Indicators - People," World Bank Website, 2019. http://datatopics.worldbank.org/world-development-indicators/themes/people.html (accessed September 18, 2019).

[31] "Traffic in Persons - Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others," United Nations Website, 2019. https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VII-11-a&chapter=7&clang=_en (accessed September 21, 2019).

[32] United Nations, "Uphold International Law," United Nations Website, (n.d.). https://www.un.org/en/sections/what-we-do/uphold-international-law/ (accessed September 21, 2019).

[33] "What is the Difference between Signing, Ratification and Accession of UN Treaties?," United Nations Website, 2018. http://ask.un.org/faq/14594 (accessed September 22, 2019).

[34] D. Winder, "Data Breaches Expose 4.1 Billion Records in First Six Months of 2019," Forbes, 2019. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#2c8f09c6bd54 (accessed September 8, 2019).

[35] A. Winston, "Interstate Compacts in the United States," Libr. Congr. Website, 2018. https://www.loc.gov/law/help/interstate-compacts/us.php (accessed September 22, 2019).

Jeremy Straub is an Assistant Professor in the Department of Computer Science and the Associate Director of the Institute for Cyber Security Education and Research at the North Dakota State University. He holds a Ph.D. in Scientific Computing from the University of North Dakota, an M.S. degree from Jacksonville State University, an M.B.A. from Mississippi State University as well as two B.S degrees. He has published over 40 journal articles and over 120 full conference papers, in addition to making numerous other conference presentations. Dr. Straub's research spans many areas between technology, commercialization and technology policy. In particular, his research has recently focused on cybersecurity technology and policy, robotic command and control, aerospace command and 3D printing quality assurance. Dr. Straub is a member of the AIAA, ASEE, SPIE and several other technical societies, he has also served as a track or session chair for numerous conferences.

A Human-Understandable, Behavior-based Trust Management Approach for IoT/CPS at Scale

Farah Kandah, Amani Altarawneh, Brennan Huber, Anthony Skjellum*, Sai Medury
University of Tennessee at Chattanooga, Chattanooga, TN, USA

Abstract

Massive deployment of the Internet of Things (IoT) is driving adoption in many application areas. The privacy, reliability, and integrity of communications must be ensured so that actions based on information provided in IoT contexts are valid, sufficiently accurate and precise, and able to be implemented promptly upon receipt. IoT systems striving to make policy based on information sharing will inevitably face impacts of byzantine and malicious entities/actors. A tunable, understandable means for defining and updating trust of entities based on their on-going behavior is essential to reducing the impact of such actors. What is more, the algorithm(s) used to establish, maintain, and adjust trust must be human understandable and auditable in order for users of the system to trust the system for every day, high-value, as well as mission-critical use cases. The main contributions of this work are as follows: We define a behavioral trust algorithm incorporating four adjustable parameters that are easily human understandable, a mechanism by which entities in a system receive updated trust values, and a metric of goodness (utility) of the system in terms of how well the trust algorithm reduces the trust of entities producing bad (non-consensus) messages over time. We identify trust of an entity as the probability of a message it produces being used by another system entity, which is a logical interpretation for device trust and the means by which we evaluate the utility of our algorithm with respect to a baseline threat model for IoT devices. Four use cases keyed to this threat model are presented together with simulation results, as well as measures of utility of the algorithm and indication of how adjusting the trust algorithm's parameters impacts the achieved utility under simulation.

Key Words: IoT, behavioral model, trust management, breakout fraud, byzantine fault tolerance, human-understandable.

1 Introduction

The integration of wireless communications into embedded devices to create IoT has facilitated ubiquity of IoT devices and increased the ease with which such devices have been integrated into daily life. Although IoT provides users with easy control-at-a-distance over such things as lights, thermostats, and doors, IoT infrastructure is not without vulnerabilities. Three such vulnerabilities are that (1) approximately 70% of IoT devices employ weak or no encryption [14], (2) IoT devices often use commercially available and open source wireless communications standards, and (3) wireless access points remain a key point through which attacks occur [1]. Thus, there remains a need for effective approaches capable of bolstering IoT security before there can be trustworthy systems at scale that incorporate IoT.

IoT systems are based on a collective organization in which devices collaborate to provide better and more accurate decisions. It is important to ensure that the information being shared is legitimate to avoid any significant degradation in system performance due to false or inaccurate information. Building trust— the "assurance" between two devices that the information being shared can be used with confidence that it is accurate—will create a trustworthy, secure system in which all devices are identified, and no information is accepted from any unauthorized device. This supports a dynamic layer of security that better fits realtime systems and thus will help advance secure IoT implementations in future smart applications such as smart cities (see Figure 1).

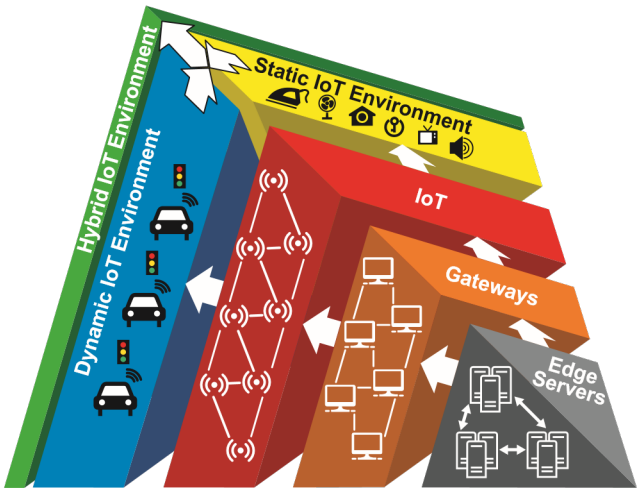


Figure 1: IoT integration towards advancing future smart applications

The key outcome is the trust algorithm that adjusts a scalar trust value for each entity in the system over time (IoT device).

* Computer Science and Engineering, SimCenter.

ISCA Copyright© 2019

From the point of view of system integrity and utility, entity trust is defined as the probability that information it produces is used in decision making. Algorithmically, trust depends on quality and level of participation, quality of messages, lifetime of a given entity in the system, and the number of known "bad" (non-consensus) messages sent by that entity. Based on this approach, we are able to adjust trust as a function of current and past behavior, providing other participants with a trust value upon which to judge information and interactions of the given entity. As shown through our simulation results, this approach reduces the potential for system manipulation by bad or byzantine actors under the reasonable assumption that low-trust entities impact a system less than high-trust entities.

The approach taken here provides an adjustable trust algorithm with four parameters that govern trust updates based on open, high-level behaviors of the devices. Trust itself is identified simply as the probability of use of a given entity's information for the purpose of evaluating the trust algorithm and as a baseline for how applications could choose to use or ignore a given entity's messages. Applications could, of course, pose more lax or stringent requirements. The trust-algorithm parameters themselves can be weighted to meet a system's overall performance (based on a utility function, such as that proposed here) or based on policies and guidelines that are chosen to achieve meta-goals of a system's designers and/or users. We, in this work, combine entity trust with its production of good and/or bad messages to assess its utility contribution to system operation; more complex utility metrics could also be posed in the future based on the details of IoT context and design goals. Importantly, our approach shows that black-box decision-making is not needed to provide rational trust value that can be used and interpreted as needed by designers and users at face value. And, our approach can be extended to vector-trust (scenario-based trust) per device straightforwardly.

The remainder of the paper is organized as follows: We discuss related work in Section 2, followed by our motivations and contributions in Section 3. We present the threat model in Section 4. Our Approach to behavioral trust management is given in Section 5. T hen follows our experimentation and evaluation in Section 6. We discuss the transparency, auditability and human oversight impacts of our model in Section 7. Finally, we conclude and discuss future directions in Section 8.

2 Related Work

Related work presented in this section covers trust management, and behavioral trust.

2.1 Trust Management

Trust is based on the history of interactions and the validity of the information exchanged between network entities (e.g., [3, 16-17]). Recently, the idea of managing trust in the network has received significant attention since it adds an additional security layer designed to ensure that the data being exchanged in the network is valid and originates from a trustworthy source [10, 12]. Several trust management schemes have been proposed, including entity-based, data-based, and hybrid trust models [18]. One area of interest in cyber-physical systems is connected vehicles. As compared to static networks, the dynamic nature of connected vehicles requires a distributed system that allows vehicles to gather and share information toward building trust in the network as they move from one place to another (this trust building can be achieved through collaboration between the connected vehicles and fixed roadside units (RSUs)).

Previous work has proposed solutions for trust management implementation in Vehicle Ad Hoc Network— Intelligent Transportation Systems (VANET-ITS) (e.g., [4, 6, 8-9, 15, 18-19]). Specifically, in our previous study, the team has implemented "BLAST: Blockchain-based Trust Management in Smart Cities and Connected Vehicles Setup [8]." While BLAST primarily concerns itself with VANET-ITS, the principles can be applicable to most any IoT space. This paper proposed the usage of three critical aspects on the handling of trust management. First, platoon formation and validation are performed. Vehicles will send beacons to roadside units (RSUs), such that the RSU will place a small number of vehicles into a cell denoted as platoon. Upon platoon formation, the RSU will find the global trust values of the vehicles and send the genesis block of what will become a platoon blockchain that contains the trust factors for all members of the platoon. As the platoon's vehicles interact through transmission of information, these trust values will be updated to more accurately reflect the trustworthiness of the vehicles. The method by which evaluating the message accuracy is based upon the overall consensus that other vehicles in the platoon have had with the transmitted information. Lastly, as the trust factors of the vehicles are updated, they would be placed onto the blockchain such that the immutability characteristic of blockchain would prevent any malicious actors from modifying the factors of any vehicle in the system.

Another work by the team has been conducted for trust management in "A Hardware-Software Codesign Approach to Identity, Trust, and Resilience for IoT/CPS at Scale [7]." Trust in this study was evaluated based on two metrics: A Trust Mechanism and RF-DNA Fingerprinting. The trust mechanism seeks to analyze the accuracy of messages that are generated by IoT devices transmitting; the goal is to establish metrics that can be used in an equation to output the overall trust value of said device. The equation developed considers four factors including the past and current behavior of the device, the quality and quantity of the messages during its lifetime, the ratio of bad messages, and frequency that the devices has had this behavior (an approach we continue in this paper). Preliminary simulations were done, and the study found that these variables were able to accurately assign trust values to vehicles even when malicious devices were present.

By way of contrast, the RF-DNA Fingerprinting is a method for capturing and verifying the identity of a specific transmitter through the exploitation of the unique coloration that a waveform generated by the IoT transmitter during its formation and transmission. This was implemented to serve two purposes; first was verification of the identity of an authorized IoT

transmitter such that it would be granted access to the network, as well as the ability to reject a rogue IoT transmitter from having access to the network. The study found that through the SVM-based ID Verification process, threat models such as counterfeiting, and impersonation were strongly mitigated. Lastly, the study implemented a blockchain structure that was used to store the trust values such that each and every trust values of devices is readily available while also providing immutability of those values.

2.2 Behavioral Trust

The concept of trust management has been studied in humans including rule-based trust and history-based trust. Trust management has also been applied in different IoT setups focusing on entity-based, databased, and hybrid trust models. A study by Jarvenpaa et al. in [5] shows how humans evaluate a situational form of trust, in which trust is based on the current environment that the person is experiencing. This study examines how an individual's trust will change in what is called global virtual teams (where team members are not co-located) in the information systems field. It shows that a person's initial trustworthiness or perception of trustworthiness of the team members has a greater impact and the "team member's willingness to exert effort for the collective benefit." It was generally found that a higher trust between team members lead to more frequent communications (because it helps assure everyone is completing the necessary tasks).

Previous studies regarding human based trust in relation to organizations shows that humans base trust primarily on historical contexts, which is named History-Based Trust which means the "willingness to engage in trusting behavior" [11]. However there also exists what is known as Rule-Based trust, which shows that following rules whether social or contractual generally lead to higher trust in an organization. Between rules that are generally followed and the historical context of a person on whether they have been trustworthy in the past, one can accurately represent the overall trustworthiness of a person. Lastly the research goes on to state that the trust-destroying acts have a much greater impact on trust than trust building. This is important an aspect in human application of trust because it is easier to lose trust than it is to gain trust [11].

One study has demonstrated that a behavioral analysis on IoT devices can be implemented through a master node which is used to monitor the data that devices will send and extract features from this data [2]. Features such as the source IP address, the destination IP address, the MAC address, and the port number, are extracted and the master nodes store the data or transactions on the behavioral monitor blockchain. Then using this data and associated feature, a machine learning model can be built in order to build an accurate representation of the behavior of the device. This machine learning model can be used to analyze similar to an anomaly detection method to determine which devices are currently acting maliciously [2].

It is worthwhile to note that aspects of anthropomorphic trust can be introduced into the trust algorithms used to enhance device trust; this is the approach taken here.

3 Motivation and Contributions

Our work is motivated by the need for more security in massive IoT deployments, and by related work described above. We are also motivated by the need for the algorithmics and mechanisms defined to be human-understandable and auditable.

The main contributions of this work are as follows:

- Definition of a baseline set of threats that IoT systems will face involving their collective interactions.
- Introduction of a behavioral trust management approach between the devices that include hysteresis.
- Simulation of four use-case scenarios that are driven by the threat model in which device trust is updated periodically to reflect behavior
- Evaluation of the trust management approach and how it impacts metrics for total net in a given scenario (system utility).
- Discussion how trust mechanism can provide human trust of system behavior and measures of transparency and auditability.
- Identification of meaningful opportunities to extend, enhance, and expand this work in future.

4 Threat Model

We present a number of threats that target IoT devices:

Threat 1. Systems with Bad and Byzantine Actors: Devices may misbehave because of faults or through malicious takeover. This general category of threat is pervasive in all distributed systems.

Threat 2. Breakout Fraud: Devices in the network can participate and exchange messages collaboratively. Decisions will be made based on these interactions. Devices can attack the system by maintaining a period of (or initial) good behavior that yields a high level of trust, then start injecting the network with invalid information. In [7], we consider these and additional threats in a threat model for large-scale IoT systems as well.

5 Behavioral-Based Trust Management

Our trust management approach focused on how trust between devices will be realized and dynamically managed by taking device behavior in the system into consideration; trust is evaluated based on interactions with peers and the quantity and quality of those interactions as compared to its peers. In the live system, group consensus defines which delivered messages were good and which were not, providing a basis to grade the behavior of devices. For the purposes of evaluation, in simulations, we can control which messages are reported faithfully and which are not without running a consensus algorithm, either deterministically or probabilistically, depending on the use case; that approach helps identify the quality of the trust algorithm under threats caused by a misbehaving device. When running the simulations as well as

in the live system, a device's trust will be used by other devices as an assurance with which to form a level of confidence used by recipient devices to identify a given device either as legitimate or not in its response regarding a specific reported event. That is, this trust value will be used as a weight for decision-making purposes by other devices. We consider an approach to realizing a group consensus mechanism in [8], but further discussion is beyond the scope of this paper.

5.1 Overview

Previous trust-based schemes of which we are aware have been based solely on the history of communications [4, 6, 7, 15, 19]. While message validation is an essential component in such systems, it is critical for system entities to know whom to trust; therefore, in our design, we consider three types of trust:

a) Direct trust ($D_t(u, v)$) is established between device u and device v that are within each other's direct transmission range.
b) Indirect trust ($I_t(u, w)$) is established between device u and device w based on neighbor-of-neighbor connection.
c) Reputational trust ($R_t(u, v, w)$) can be formed between device u and its directly connected device v based on the information gathered from device w.

Along with the aforementioned levels of trust, we will use an approach with finite memory to manage and build the trust between devices. Within its peer group of devices, a device's trust is based on the quality and quantity of interactions, as well as the lifetime of the device in the system.

Four major factors drive trust:

1) **Relativity:** measures participation of the device and its current trust compared to its peers in the system;
2) **Participation:** measures the device's behavior in the system, which is monitored by the number of messages it generates (quantity) and has shared in the system during its lifetime, and the criticality (rank) of the messages (quality) being shared by the device during its lifetime;
3) **Lifetime:** measures the time it took a device to build its trust based on the shared messages compared to the total uptime of the system since the last update.
4) **Truthfulness:** measures how truthful the device is based on its behavior as being good or bad, which is calculated as a fraction of the truthfulness of the messages being shared by the device in the system.

In the model that follows below, we capture these four factors through the following, adjustable weights: θ for relativity as the current behavior and participation in which the device will be rewarded for participation based on its behavior among other devices; χ for participation (the rank (criticality) and number of messages at each rank), φ for the lifetime (total uptime of the device being active to share their messages); and, τ for the truthfulness as a fraction of bad messages to total messages shared by the device. We normalize the weights in the range [0, ... ,1], and, by convention, assign

$$\tau = 1 - \theta - \chi - \varphi \quad (1)$$

5.2 Trust Model Design

The trust mechanism includes the four factors ($\theta, \chi, \varphi, \tau$) that merit/demerit the current and past behavior for devices in a way that we hypothesize will reduce the potential for threats. Following is the approach to updating the trust for each device in detail.

The first function below represents the devices' participation and their current behaviors vis a vis other device. $F(C_{i,t})$ is defined by the following algorithm for each device i (see Figure 2):

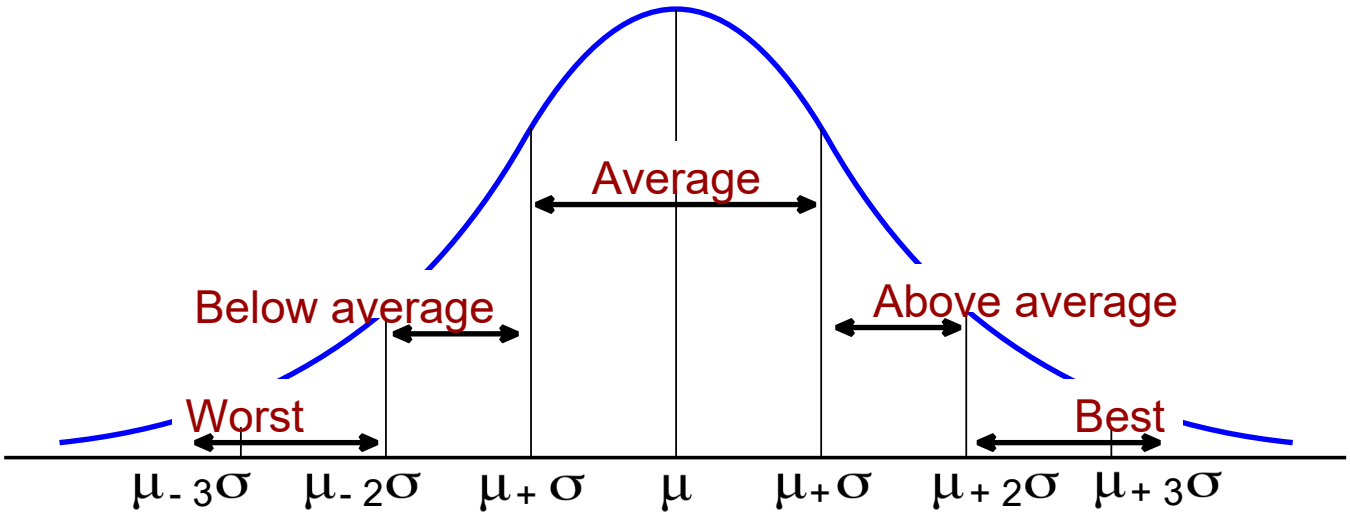


Figure 2: Calculating the interval that covers at a maximum 99.7% of the devices and builds the categories

a) Find the mean (μ) value for all the trust values and the standard deviation (σ).
b) Using the empirical rule [13] to calculate the interval that covers at a maximum 99.7% of the devices and builds the categories (and hence $C_{i,t}$); for instance: $\mu \pm \sigma$ is approximately 68% of the measurements, $\mu \pm 2\sigma$ is approximately 95%, and $\mu \pm 3\sigma$ is approximately 99.7% of the measurements, which will lead us to create five categories around the mean to measure the current behavior among other peers. Thus, the $C_{i,\,t}$ value is computed thusly:

- The "Average" category has an impact factor of 0.05; values within the interval $[\mu \pm \sigma]$ are in the majority, which represents 68% of the devices in the system.
- The "Above-average" category has impact factor of 0.07; values are within the interval $((\mu + \sigma), (\mu + 2\sigma)]$.
- The "Best" category has impact factor equal to 0.09; values are greater than $(\mu + 2\sigma)$.
- The "Below-average" category has impact factor of 0.03; values are within the interval $[(\mu - 2\sigma), (\mu - \sigma)]$.
- The "Worst" category has impact factor of 0.01; values are less than $(\mu - 2\sigma)$.

c) Determine the device category $C_{i,t}$ for each device i based on the five categories above and calculate the corresponding equation of that category with the device's current trust value using the following function:

$$F(C_{i,t}) = \begin{cases} C_{i,t} \times 1.09, & C_{i,t} \geq (\mu + 2\sigma) \\ C_{i,t} \times 1.07, & (\mu + \sigma) \leq C_{i,t} < (\mu + 2\sigma) \\ C_{i,t} \times 1.05, & (\mu - \sigma) < C_{i,t} < (\mu + \sigma) \\ C_{i,t} \times 1.03, & (\mu - 2\sigma) < C_{i,t} \leq (\mu - \sigma) \\ C_{i,t} \times 1.01, & C_{i,t} \leq (\mu - 2\sigma) \end{cases} \quad (2)$$

The second factor is based on the history of the device. In our system, the messages are ranked from one to ten[1], which reflects how critical the messages being shared by this specific device during its lifetime are. So, the number of messages of each rank are stored as a list for each device, which enables calculating the number of points $M_{i,points}$ as follows:

$$M_{i,points} = \sum_{j=1}^{10} \left(\mathrm{Freq_{i,j}} \times j\right) \quad (3)$$

This value will be calculated and later will be compared to the maximum value achieved among all devices using $g(M_{i,points})$:

$$g(M_{i,points}) = \frac{M_{i,points}}{max\,(_{k,points})} \quad (4)$$

[1] Rankings other than linear 1...10 are substitutable without loss of generality (e.g., one could use exponential rankings of criticality). Then $j \rightarrow rank(j)$ as the multiplicand of frequencies in Equations 3, 8, and 9, and the number 10 is replaced by the number of ranks in the model.

The third factor, which is the time it took device i to build the messages, is evaluated using $L(lt_i)$, which is the ratio of the time that a device spent to build its message history to the amount of time on the system since the last update (uptime):

$$L(lt_i) = \frac{lt_i}{Total\ time} \quad (5)$$

The fourth factor is computed based on the following function, where B_i is the fraction of bad messages, which reflects the truth ratio based on the messages being sent by these devices compared to the events being reported, which is calculated as

$$P(B_i) = 1 - \frac{B_i}{Total\ messages} \quad (6)$$

The final trust value will be the sum of all four factors, where each contribution is multiplied with its corresponding weight; thus, the updated value for each device in the system participating in that round will be calculated as:

$$\begin{aligned} T\,i(new) &= \theta \times F(Ci,\,t) + \chi \times g(Mi,\,points) \\ &\quad + \varphi \times L(lt_i) + \tau \times P(B_i) \\ &= \theta \times F(Ci,\,t) + \chi \times g(Mi,\,points) + \\ &\quad + \varphi \times L(lt_i) + (1 - \theta - \chi - \varphi) \times P(B_i). \end{aligned} \quad (7)$$

This final formula reflects the punishment and reward in the new trust based on the current and the past behavior of the device, considering the quality and the quantity of messages during its lifetime, the fraction of bad messages, and how many times the device repeated that behavior. The trust value does not increase or decrease independently for each device; rather, the formula rebuilds the new trust for each device based on its behavior in comparison with other devices' behaviors (current and past).

6 System Evaluation and Experimentation

We establish a metric of system utility; that is, how well does trust impact the system performance under threats. We describe four experimental scenarios and evaluate their successfulness with the utility formalism while varying the trust-algorithm parameters θ, χ, φ, and τ over the 3D parameter space (τ depends on θ, χ, φ, as noted above in Equation 1).

6.1 Trust Effectiveness Metrics

Tacitly, we recognize that high-trust entities produce messages that are more likely to be used than those produced by low-trust devices. As noted above, we identify trust of a given device, in the context of evaluating the utility of our algorithm, as the probability that a message generated by that device—whether good or bad—will be utilized by applications (cooperating groups devices delivering an IoT service). Applications could apply more-lax, more stringent, or even case-based or situational rationales[2] for determining whether to

decide based on a given message from a given device at a current trust level, but that is beyond the scope of this study.

We define a utility function for the performance of our trust algorithm as follows: For each device *i* in the field, we calculate $G_{i,(hourly)}$, which is the quality of its good behavior, $G_{i,(hourly)}$ is given in Equation (8) below, which is the rank of the good messages times that message rank's frequency. This also applies for device *i*'s bad behavior, as denoted by $B_{(hourly)}$ and given in the Equation (9), following:

$$G_{i,(hourly)} = \sum_{j=1}^{10} \left(\text{GoodMessageFreq}_{\text{i,j}} \times j\right) \quad (8)$$

and

$$B_{i,(hourly)} = \sum_{j=1}^{10} \left(\text{BadMessageFreq}_{\text{i,j}} \times j\right) \quad (9)$$

The utility value is calculated hourly for all *n* participating devices as follows:

$$U_{\theta,\chi,\phi,\tau(hourly)} \sum_{i=1}^{n} \left(Ti(new)\ (G_{i,(hourly)}\, B_{i,(hourly)})\right) \quad (10)$$

We calculate the average utility value for the same combination of (θ, χ, φ) for number of hours simulated in equation 11:

$$U'_{i,(\theta,\chi,\phi,\tau)} = \sum_{h=1}^{H} \left(U_{\theta,\chi,\phi,\tau(h)}\right) / H \quad (11)$$

where *H* is the number of hours simulated in a single run with a single use case and fixed θ, χ, φ, τ. In the following experiments, we denote *U''* as the mean utility of a single configuration over multiple reruns and s_U'' as its standard deviation of that mean.

6.2 Experimentation

All devices start their trust at zero. Thus, each device's trust in the next update will be nearly the same if they were active to the same degree and communicated honestly with the same number of messages and no bad messages. The weight for participation and current behavior in comparison with one another in the formula is the same for all given their common initial trust. Differences arise from other factors such as the active uptime for each, the number of generated messages, and the fraction of bad messages produced by each.

To evaluate the performance of the trust mechanism presented in this work, an event-based simulation was designed, such that, devices will report incidents represented by events. Later, each device will be categorized as begin good if their report matches the incidents and bad if there is a mismatch between the messages being generated by the device compared to the events. The simulation was configured to include 25 devices all transmitting messages between one another to build trust naturally in the system. As the simulation progresses and devices are transmitting several messages between each other, the trust values of each device are updated every 360 seconds in simulation time. Trust values are carried forward from the beginning of the simulation. Each device's behavior (consider our four factors of behavior) will be used to update its trust periodically. As we consider IoT devices, we chose a one-hour duration as a monitoring period during which device behavior can be measured. This duration was selected to make sure any negative behavior can be captured before its effect on the system becomes unacceptably high; nonetheless, shorter monitoring periods could also have been chosen[3].

Trust values are updated 24 times during the simulation meaning that the trust value at the end of the simulation would be the trust value of the devices after a period of 1 day. In order to obtain a more accurate evaluation of our utility function, we run the simulation for 200 times. Across these runs, the utility function is calculated per run and the average is calculate for all the runs to provide insight into the performance of each run to determine which combination of coefficients (θ, χ, φ, and τ) in the formula enhances the system better than other combinations so that entity trusts are adjusted, thereby yielding the largest net number of accurate messages vs. false messages.

We used (θ = 0.25, χ = 0.25, φ = 0.25, τ = 0.25) as an initial configuration. We fixed τ and generated 106 different configurations using various margins such as 1.0, 0.5, and 0.25 for the other coefficients. We ran the simulation for each of 106 combinations[4] and found the average utility value as in equations (10) and (11) for each. This procedure was applied for the following cases, where we were able to find the best combination that yielded the maximum average utility value.

6.3 Use Cases

As described above in Section 4, we are considering two high-level classes of threats to the IoT system to be mitigated with our trust model. Consequently, the first three use cases below explore the case with bad and byzantine actors throughout a given simulation scenario. These cases were designed to measure the ability of the system to handle byzantine actors. We considered different percentages of failing (34%, 5%, and the most chaotic one with 50% failure ratio). However, the fourth use case considers the threat of breakout fraud.

Use Case 1: This use case is designed to reflect the situation where 66% of the devices are deemed to be good devices, while the rest (34%) are malicious (byzantine actors). 66% of the devices reach consensus based on a given event being reported as compared to the rest of the devices. This case was designed to target bad and byzantine actors' threat (Section 4 - Threat 1).

[2]A selective parameter study was performed to demonstrate the utility of this approach. An exhaustive study of the parameter space may result in even better results. This is left for future work.

[3] In [8], we consider maximum frequencies of trust updates based on the ability to form consensuses and promulgate trust updates.

[4] We chose 106 as greater than 100 but without any other particular rationale for this precise value.

Our experimental results and the system utility evaluation of this case are presented in Table 1. Our results reflect the best[5] representation of the U''s along with their corresponding error estimates, s_U''. This table shows the level of confidence in the selection of the coefficient values for this case. The best coefficients combination achieved for this case were picked based on the maximum U'' value among other combinations for this sample (highlighted in blue in the table). Note that these combinations were selected to reflect the best representation where there is no overlap in $U'' \pm s_U$'' with other combinations' values.

As shown in Table 1, the best combination found has high values of relativity factor and low values of lifetime and participation factors. This combination enables the system to achieve 34% fault tolerance. Assigning a higher weight for the relativity factor will evidently keep trust values from being influenced by the percentage of bad messages in the system.

The observations in Table 1 show optimized weights for the trust factors and depict the corresponding system evaluation in Figure. 3.

Figure 3 shows the results for a sample points of the analysis (four devices) to demonstrate how the proposed algorithm manages trust in the system. According to this use case, 66% of devices are considered to be good devices with corresponding good (truthful) behavior while 34% of the devices are considered as bad devices based on their behavior in the system. In this use case, we have introduced at least two devices from each category to yield a reasonable comparison of the behavior and how the trust is being handled in the system. The trust can be observed as increasing for devices #1 and #2, based on their good behavior; it is more noticeable when compared with the trust of devices #3 and #4, whose trust decreases because of their bad behavior.

The selected combinations demonstrate that the system was able to distinguish good behavior from bad behavior. As a result, devices #1 and #2 with good behavior were able to build their trust rapidly over time, while other devices failed to achieve high trust values in the system as a result of their bad behavior.

Table 1: The average Utility values with 66% good devices

θ	χ	φ	τ	$U''_{(\theta,\chi,\phi,\tau)} \pm S_{U''}$
0.43	0.16	0.16	0.25	9,961 ± 1,024
0.44	0.155	0.155	0.25	10,104 ± 916
0.6	0.075	0.075	0.25	12,225 ± 955
0.25	0.25	0.25	0.25	8,752 ± 903
0.075	0.6	0.075	0.25	10,045 ± 1,385

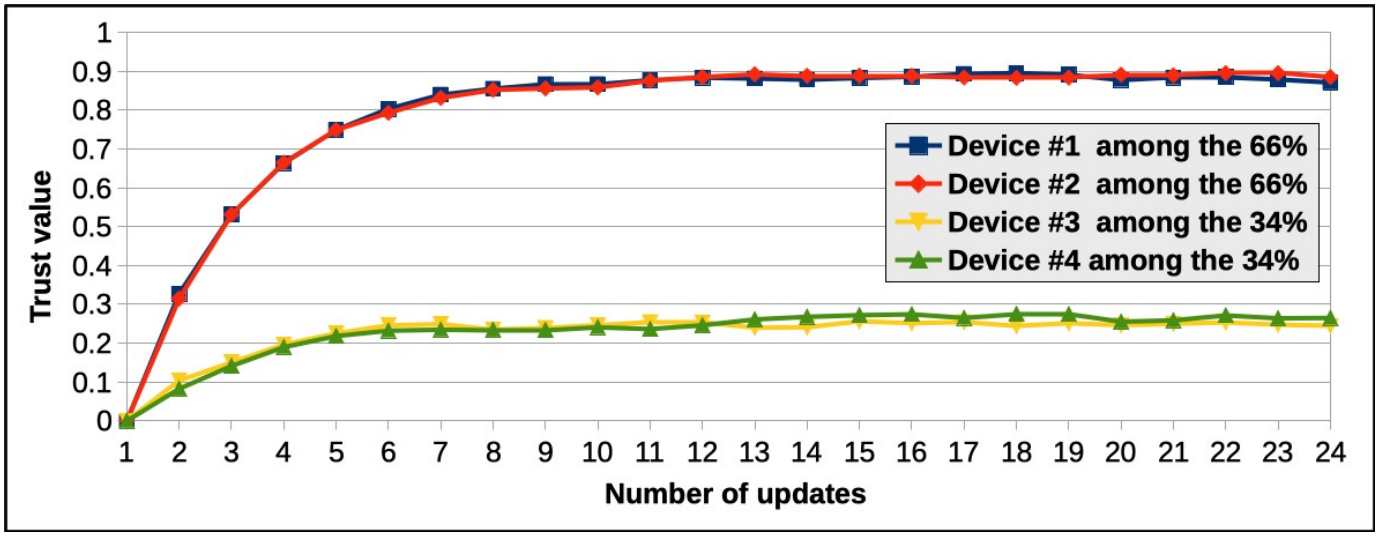


Figure 3: Trust updates values for the 66% good actors with best utility value

[5] A selective parameter study was performed to demonstrate the utility of this approach. An exhaustive study of the parameter space may result in even better results. This is left for future work.

Use Case 2: With 95% of devices sending truthful (accurate) messages, and the remaining 5% sending false messages, this case was designed to target the threat of bad and byzantine actors (Section 4 - Threat 1). The results of simulation and the values generated by the utility function observed in this case are presented in Table 2. In this case, 95% of the messages being shared in the system are good messages; that justifies that the highest weight being given to the participation factor. To achieve the highest utility value (highlighted in blue in the table), the other three factors were assigned a comparatively lower weight.

In Table 2, we identified the highest utility weights for the trust factors and depicted the corresponding system evaluation in Figure. 4.

As shown in Figure. 4, we plot the same number of devices as in use case 1 for uniformity, where devices #1 and #2 are among the 95% of the system devices with good behavior while devices #3 and #4 are among the remaining 5% of the devices with bad behavior.

Based on the selected combinations, it can be seen in Figure. 4 that the system was able to successfully distinguish good behavior from the bad behavior, where devices #1 and #2 with their good behavior were able to reach topmost trust values in a short period of time similar to what was observed with good devices in case 1, which reflects the system's ability to perform well with minimum byzantine behaviors.

Despite the fact that the system has 95% of its devices as behaving good, the bad devices could not advance their trust beyond the second trust update, which is considered lower than the ones with the good behaviors.

Use Case 3: In this case, we set the number of devices sending accurate messages to be precisely the same as the number of devices sending inaccurate messages (both to 50%). This use case is meant to show the ability of the system to tolerate the scenario with 50% of devices failing while targeting bad and byzantine actors' threats (Section 4 - Threat 1).

Our experimental results and the system utility evaluation of this case is presented in Table 3. This case is close in its results to Case 1, where the best combination is that with the highest weight assigned to the relativity factor, while the other factors are set to lower weights, which is for the same reason as was addressed in Case 1.

Table 2: The average Utility values with 95% good devices

θ	χ	φ	τ	$U''_{(\theta,\chi,\phi,\tau)} \pm S_{U''}$
0.23	0.29	0.23	0.25	16,634 ± 1,177
0.08	0.59	0.08	0.25	20,389 ± 1560
0.09	0.09	0.57	0.25	10,561 ± 738
0.085	0.085	0.58	0.25	10,489 ± 744
0.08	0.08	0.59	0.25	10,289 ± 659

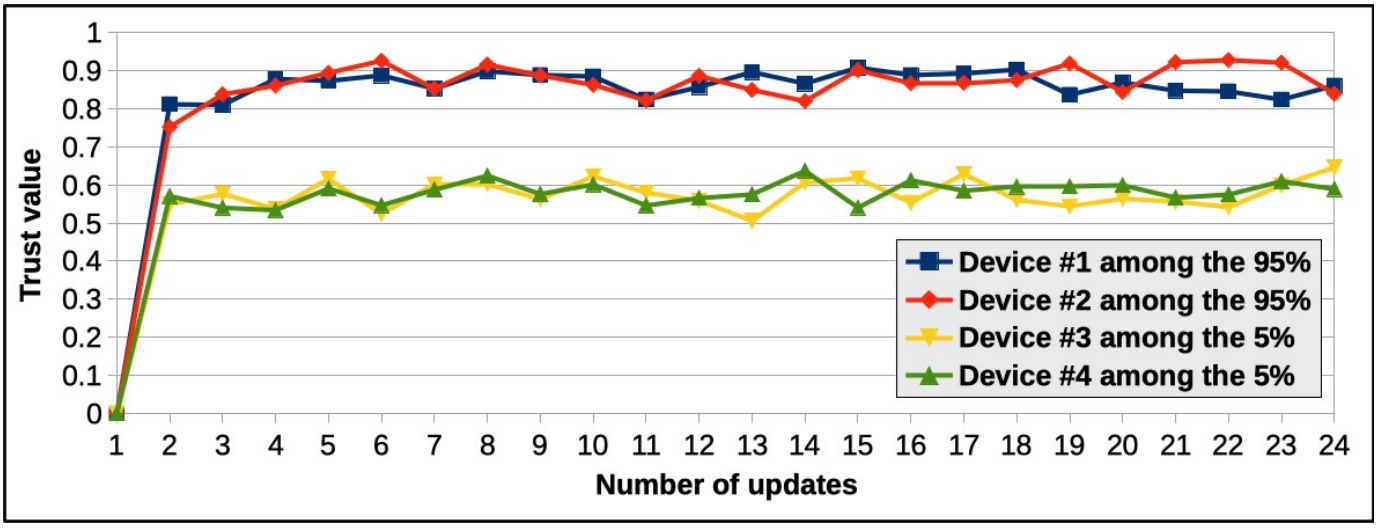


Figure 4: Trust updates values for the 95% good actors with best utility value

Table 3: The average Utility values with 50% good devices

θ	χ	φ	τ	$U''_{(\theta,\chi,\phi,\tau)} \pm S_{U''}$
0.03	0.03	0.59	0.35	4,616 ± 323
0.135	0.38	0.135	0.35	5,326 ± 809
0.5	0.075	0.075	0.35	8922 ± 511
0.49	0.08	0.08	0.35	8,316 ± 910
0.58	0.035	0.035	0.035	10,650 ± 777

In Figure 5, we plot the trust of five devices with 50% of the devices behaving well. Here devices #1 and #2 are among the good ones and devices #3, #4, and #5 are among the bad ones.

The combinations selected are shown in Table 3 (highlighted in blue). It can also be observed in Figure 5 that devices with good behavior were able to build up their trust faster than those behaving maliciously.

Since the relativity in the system is considered to be the one with the highest weight, the system was able to successfully separate the bad behavior from good behavior, and trust of all devices with bad behavior was isolated farther apart from the ones with good behavior. This behavior is made more evident by the large gap in the figure between the trust values of the devices with good behavior vs. those with bad behavior.

Use Case 4: Devices in the network can participate and exchange messages collaboratively, and decisions will be made based on these interactions. Devices can perform a *breakout fraud* behavior, where they can attack the system by maintaining a period of (or initial) good behavior that yields a high level of trust, then start injecting the network with invalid information. To address this behavior, we designed this use case with the focus on this type of behavior to determine how our approach mitigates such behavior. This case was designed to target bad and byzantine actors' threat (Section 4 - Threat 2). All devices begin the simulation with an equal 50% trust then the simulation runs for half of the time as the other simulations in order to give each of the devices an opportunity to build their trust as it would naturally occur. Then at the halfway point in the simulation, 10% of the devices would systematically begin sending bad messages. The outcome of this simulation can be used to determine how quickly the system reacts to degrade the trust value of a previously trustworthy device.

Our experimental results and the system utility evaluation of this case is presented in Table 4. It can be seen that the best combination based on the highest utility value was realized with the highest weight again given to the relativity factor (highlighted in blue in the table). Because the breakout-fraud situation occurs after malicious devices gain their highest trust in the system, assigning the highest weight to the relativity

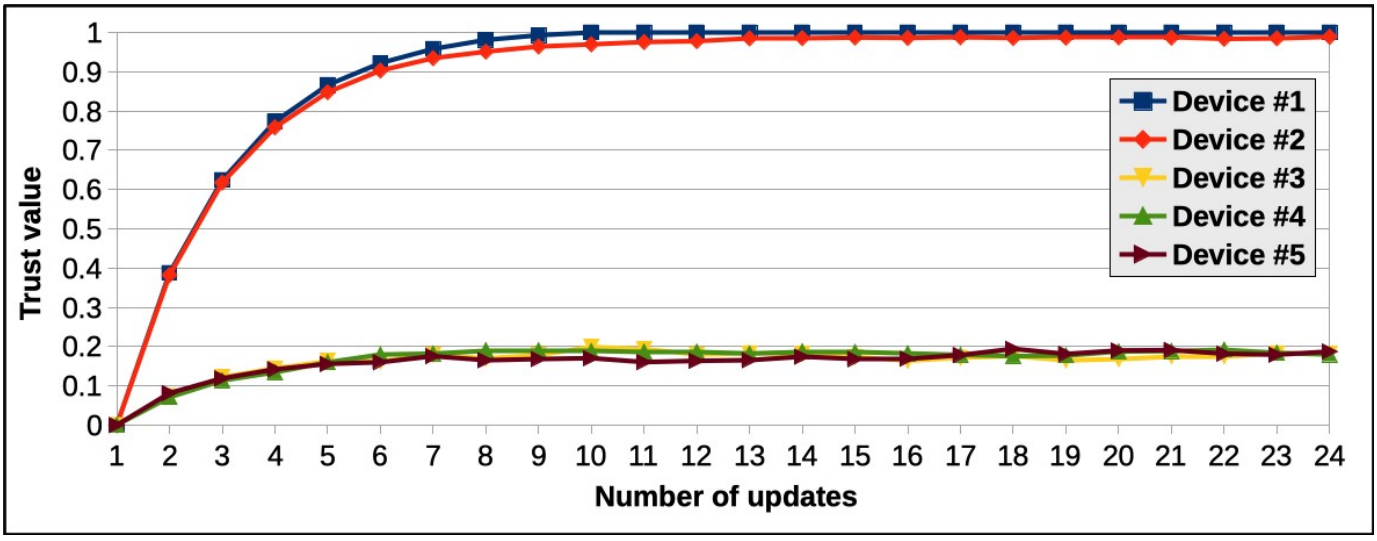


Figure 5: Trust updates values for the 50% good actors with best utility value

Table 4: The average Utility values with devices engaging in *breakout fraud* behavior

θ	χ	φ	τ	$U''_{(\theta,\chi,\phi,\tau)} \pm S_{U''}$
0.08	0.08	0.59	0.25	9,935 ± 610
0.075	0.075	0.6	0.25	9,776 ± 616
0.105	0.105	0.54	0.25	10,709 ± 690
0.25	0.25	0.25	0.25	8,316 ± 1,149
0.6	0.075	0.075	0.25	19,946 ± 1,312

factor evidently will degrade the trust update values for these devices faster. This fast action will work to reduce the impact of bad behavior on the system as a whole.

Based on the results presented in Table 4, we identified the highest utility weights for the trust factors and depicted the corresponding system evaluation in Figure 6. It can be seen that devices start building their trust rapidly. And, as soon as the system detects bad behavior carried through the breakout fraud, their trust values will rapidly degrade as they continue with their bad behavior.

Based on the chosen utility function, we were able to determine quality combinations of factors given the different use cases presented in this section.

7 Transparency, Audibility, and Human Oversight

Our basic conclusion of this work is that our trust model incorporates human-understandable reactions to good and bad behavior. The weights on various behavior are explicit in the model, so that designers, auditors, and users can understand why certain devices gain and lose trust over time in an operational system. These properties enable human-centric control of the outcomes of trust-related decisions in terms of non-biasing of certain actors and participants, as well as making explicit what good and bad behavior are of both human and machine actors in such a system. While considering this qualitative measurement via the four factors of our behavioral model, we assert that it is superior to black-box decision-making insofar as it is explainable at or immediately after trusts are adjusted based on behavior. What is more, the simple connection of trust as the probability that data produced by a given device will be used provides a baseline to consider the impact of good and bad behavior in a large-scale IoT system. Certainly, more sophisticated scalar and vector (per scenario) trusts can be extrapolated from these without losing the aspect of human understandability, which is a key prerequisite for keeping humans in (supervisory) control of the system.

8 Conclusion and Future Work

Our trust algorithm and approach provide a human-understandable concept for trust, and an understandable

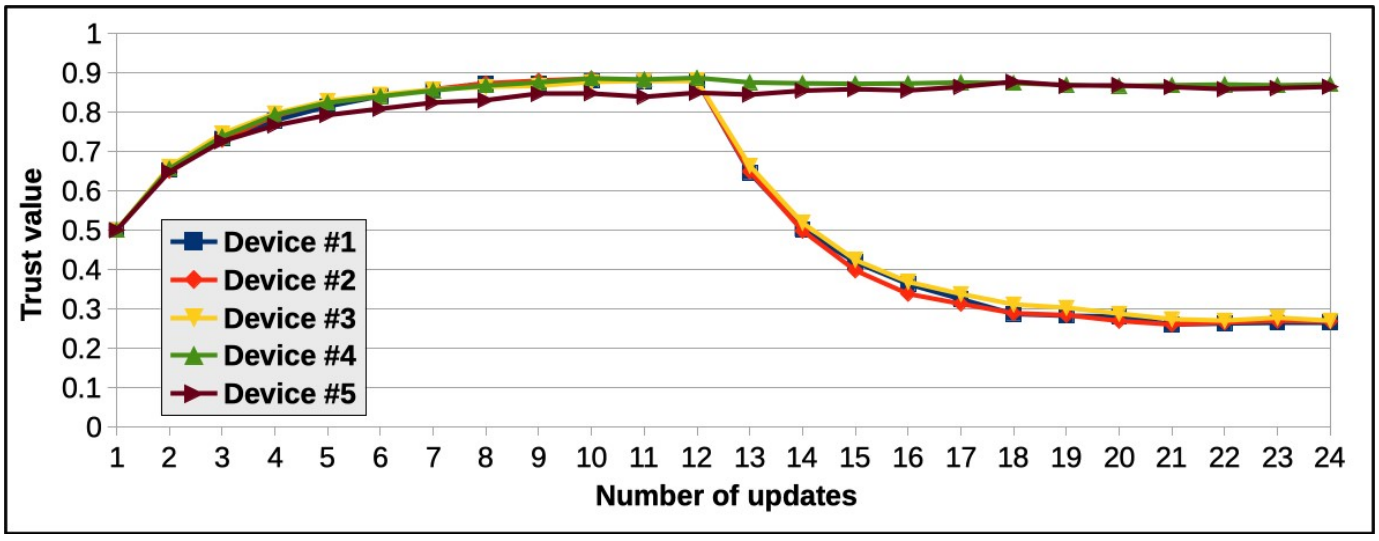


Figure 6: Trust updates values for the break fraud attack with best utility value

mechanism for trust updating based on device (entity) behavior in a large-scale IoT system. We identify trust for a device as a scalar probability that this device's messages will be used by others in the system; this provides a basis for indicating contribution or degradation that is caused by a given device. Vector (or scenario-based) trust for each device, as well as more complex application-based decisions of how to interpret that trust remain as future extensions to this work.

Our baseline threat model addresses bad and byzantine actors as well as breakout fraud but leaves open experimentation with additional dimensions of threat. Our use cases are keyed to the threat model, and our outcomes are rated against a logical utility metric of system utility (ability to favor good behavior over bad, and downrate badly behaving actors). Three of these use cases examine difficult scenarios in which overall behavior (good vs. bad) is a percentage of total membership and random...practical systems will often be much less demanding that these scenarios. The fourth case involves breakout fraud among a subset of devices after initial good behavior, which means that trust has grown for such ultimately bad actors due to initial performance.

In conclusion, with our optimization procedure we were able to use adjustable parameters guided by a utility function to find the approximate optimal performance based on the test cases. We determined for each case the behavioral model's factors with the highest beneficial impact on trust updates, thus led to better system behavior for the test cases, as measured by the utility function, vs. random choices of these parameters.

Based on the use case results, the highest weight was assigned to the relativity factor in order to achieve better performance. This holds for all cases except for the case where the system tolerate is 5% byzantine behavior, in which the highest weight was assigned to the participation factor. As the majority of the devices are behaving legitimately (good behavior), and because of the relativity factor, most devices will be categorized as distinct from those devices behaving maliciously. Bad behavior will mainly be captured by the participation factor (in which malicious devices are sending false reports considering the reported events). Since the bad behavior in the system is measured through the use of the participation and lifetime factors, it is still hard to determine their best weights given the cases presented in this work. Nevertheless, in use Cases 1-3 and through our behavior-based trust model with the assigned weights, we were able to mitigate bad devices' behavior in the system, as well as to mitigate the breakout fraud behavior in use Case 4.

While our model is understandable and auditable, it currently lacks the ability to over-penalize bad behavior. What this means is that an actor whose trust is substantially reduced by a scenario of bad behavior can ultimately reaccumulate trust in equal measure to another device that has never acted badly, despite a degree of memory of that bad behavior. These is no "parole" or period of strong negative bias once bad behavior has been detected, and trust lowered. Therefore, cyclical good and bad behavior is not fully captured and could be used as a countermeasure by bad and colluding actors in the system. Furthermore, we need to explore the frequency of trust change (which is hourly as currently implemented) vs. the frequency and content of bad messages that can be transmitted (with concomitant damage potential) during a period. In fact, a period of no less than three hours is needed to establish a trust trend definitively. As such, the threat models will have to be extended to look not only at cyclical good vs. bad behavior, but also frequency effects that will motivate trust updates that are more frequent. In this regard, there will be a maximum rate at which trust can be transmitted broadly as a function of system size and performance in order to maintain scalability. For this reason, exploration of random frequency of trust updates, and asynchronous trust values, as well as trust hierarchies will evidently be needed. These considerations also remain for future work.

Acknowledgement

The authors acknowledge support from the University of Tennessee at Chattanooga. Research reported in this publication was supported by the 2019 Center of Excellence for Applied Computational Science and Engineering grant competition (CEACSE). This material is based upon work supported in part by the National Science Foundation (NSF) under Grant No. 1821926. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

References

[1] "Top 10 Network Security Threats," *Government Technology*, Sep 2010.

[2] Jawad Ali, Toqeer Ali, Yazed Alsaawy, Ahmad Shahrafidz Khalid, and Shahrulniza Musa, "BlockChain-Based Smart-IoT Trust Zone Measurement Architecture," *Proceedings of the International Conference on Omni-Layer Intelligent Systems*, ACM, COINS '19, pp. 152-157, New York, NY, USA, 2019.

[3] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," *Proceedings 1996 IEEE Symposium on Security and Privacy*, pp. 164-173, May 1996.

[4] I. Butun, S. D. Morgera, and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," *IEEE Communications Surveys Tutorials*, 16(1):266-282, 2014, First Quarter, https://ieeexplore .ieee.org/document/6517052.

[5] Sirkka Jarvenpaa, Thomas R. Shaw, and D Sandy Staples, "Toward Contextualized Theories of Trust: The Role of Trust in Global Virtual Teams," *Information Systems Research*, 15:250-267, Sept. 2004.

[6] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, 26(5):1228-1237, May 2015.

[7] F. Kandah, J. Cancelleri, D. Reising, A. Altarawneh, and A. Skjellum, "A Hardware-Software Codesign Approach to Identity, Trust, and Resilience for IoT/CPS at Scale," *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and*

Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1125-1134, July 2019.

[8] F. Kandah, B. Huber, A. Altarawneh, S. Medury, and A. Skjellum, "BLAST: Blockchain-Based Trust Management in Smart Cities and Connected Vehicles Setup," *2019 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1-7, Sep. 2019.

[9] F. Kandah, B. Huber, A. Skjellum, and A. Altarawneh, "A Blockchain-Based Trust Management Approach for Connected Autonomous Vehicles in Smart Cities," *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0544-0549, Jan 2019.

[10] C. A. Kerrache, C. T. Calafate, J. Cano, N. Lagraa, and P. Manzoni, "Trust Management for Vehicular Networks: An Adversary-Oriented Overview," *IEEE Access*, 4:9293-9307, 2016.

[11] Roderick M. Kramer, "Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions," PMID: 15012464, *Annual Review of Psychology*, 50(1):569-598, 1999.

[12] W. Li, H. Song, and F. Zeng, "Policy-Based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," *IEEE Internet of Things Journal*, 5(2):716-723, April 2018.

[13] R. Lyman Ott and Micheal T Longnecker, *An Introduction to Statistical Methods and Data Analysis*, Cengage Learning, 2015.

[14] K. Rawlinson, "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," July 2014, https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676.

[15] Jiangwen Wan, Xiang Zhou, Xiaofeng Xu, and Renjian Feng, "A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory," *Sensors* 11:1345-1360, 2011.

[16] Li Xiong and Ling Liu, "Building Trust in Decentralized Peer-to-Peer Electronic Communities," The 5th International Conference on Electronic Commerce Research, (ICECR), 2002.

[17] Li Xiong and Ling Liu. "Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," *IEEE Transactions on Knowledge and Data Engineering*, 16(7):843-857, July 2004.

[18] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," *IEEE Internet of Things Journal*, pp. 1-1, 2018.

[19] G. Zhan, W. Shi, and J. Deng, Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNS," *IEEE Transactions on Dependable and Secure Computing*, 9(2):184-197, March 2012.

Farah Kandah is a UC Foundation Associate Professor in the Computer Science and Engineering (CSE) Department at the University of Tennessee at Chattanooga (UTC). His research interests and expertise span a wide range of topics in cybersecurity and cyber-physical systems. He is currently leading the Network Communication Laboratory (NCL) at UTC, which leverages expertise on smart communications to support real-time communications in wired and wireless networks, threat hunting, Blockchain and trust management with research focuses on urban science, Internet of Things, public safety, smart networking design, smart autonomous/connected vehicle networks, cybersecurity, and Software-Defined Networks. He is a member of ACM and IEEE. During his time at UTC, he received the outstanding Tenured/Tenure-Track Faculty Teaching Computer Science and Engineering Award in 2017, the Faculty/Teacher of the Year Award, Computer Science and Engineering in 2017, and the outstanding Researcher, Computer Science and Engineering in 2016. He has served as a technical committee member, a Co-Chair, and a Session Chair for a number of conferences in the field of cybersecurity, wireless communications and networking such as CHINACOM, IEEE ICNC, and IEEE CCNC. He has also served as a reviewer for several international journals including the Security and Communication Networks, IEEE Sensor Networks, International Journal of Information Processing and Management (IJIPM), and the Journal of Computer Systems, Networks and Communications (JCSNC).

Amani Altarawneh received her BA from Mu'tah University in Computer Science, Alkarak, Jordan and MS in CS from Bridgewater State University in MA, USA. She is currently a PhD candidate in Computer Science and Engineering at The University of Tennessee at Chattanooga (UTC), Tennessee, USA. Her research interests include Cybersecurity, queuing theory, IoT, and smart cities, and distributed systems.

Brennan Huber received his BS in Computer Science: Scientific Application from University of Tennessee at Chattanooga (UTC). He is currently a Master's candidate in Computer Science: Cybersecurity at the University of Tennessee at Chattanooga (UTC). His primary research interests include cybersecurity, trust management, and vehicle ad-hoc networks.

Anthony (Tony) Skjellum studied at Caltech (BS, MS, PhD). His PhD work emphasized portable, parallel software for large-scale dynamic simulation, with a specific emphasis on message-passing systems, parallel nonlinear and linear solvers, and massive parallelism. From 1990-93, he was a computer scientist at LLNL focusing on performance-portable message passing and portable parallel math libraries. From 1993-2003, he was on the faculty in Computer Science at Mississippi State University, where his group co-invented the MPICH implementation of the Message Passing Interface (MPI) together with colleagues at Argonne National Laboratory. From 2003-2013, he was professor and chair at the University of Alabama at Birmingham, Dept. of Computer and Information Sciences. In 2014, he joined Auburn University as Lead Cyber Scientist and led R&D in cyber and High-Performance Computing for over three years. In Summer 2017, he joined the University of Tennessee at Chattanooga as Professor of Computer Science, Chair of Excellence, and Director, SimCenter, where he continues work in HPC and Cybersecurity, with strong emphases on IoT and blockchain technologies. He is a senior member of ACM, IEEE, ASEE, and AIChE, and an Associate Member of the American Academy of Forensic Science (AAFS), Digital & Multimedia Sciences Division.

Sai Medury is a PhD Candidate at University of Tennessee at Chattanooga with research interests related to Cybersecurity, blockchain technology, and X.509 Digital Certificate revocation. He received the Master's degree in Software Engineering from Auburn University in 2017.

Index

Authors

A

B-C

D-G

H-J

K-L

M-O

P-Q

ISCA Copyright© 2019

R-S

T-Z

Key Words

A

B-C

D

E-F

G-H

I-J

K-L

M

Journal Submission

The International Journal of Computers and Their Applications is published four times a year with the purpose of providing a forum for state-of-the-art developments and research in the theory and design of computers, as well as current innovative activities in the applications of computers. In contrast to other journals, this journal focuses on emerging computer technologies with emphasis on the applicability to real world problems. Current areas of particular interest include, but are not limited to: architecture, networks, intelligent systems, parallel and distributed computing, software and information engineering, and computer applications (e.g., engineering, medicine, business, education, etc.). All papers are subject to peer review before selection.

A. Procedure for Submission of a Technical Paper for Consideration

1. Email your manuscript to the Editor-in-Chief, Dr. Ziping Liu at: zliu@semo.edu.
2. Illustrations should be high quality (originals unnecessary).
3. Enclose a separate page (or include in the email message) the preferred author and address for correspondence. Also, please include email, telephone, and fax information should further contact be needed.
4. **Note**: Papers shorter than 10 pages long will be returned.

B. Manuscript Style:

1. The text should be **double-spaced** (12 point or larger), **single column** and **single-sided** on 8.5 X 11 inch pages.
2. An informative abstract of 100-250 words should be provided.
3. At least 5 keywords following the abstract describing the paper topics.
4. References (alphabetized by first author) should appear at the end of the paper, as follows: author(s), first initials followed by last name, title in quotation marks, periodical, volume, inclusive page numbers, month and year.
5. The figures are to be integrated in the text after referenced in the text.

C. Submission of Accepted Manuscripts

1. The final complete paper (with abstract, figures, tables, and keywords) satisfying Section B above in **MS Word format** should be submitted to the Editor-in-Chief. If one wished to use LaTex, please see the corresponding LaTex template.
2. The submission may be on a CD/DVD or as an email attachment(s). **The following electronic files should be included:**
   - Paper text (required).
   - Bios (required for each author).
   - Author Photos (jpeg files are required) or photos can be integrated into the text.
   - Figures, Tables, and Illustrations. These should be integrated into the paper text file.
3. Reminder: The authors photos and short bios should be integrated into the text at the end of the paper. All figures, tables, and illustrations should be integrated into the text.
4. The final paper should be submitted in (a) pdf AND (b) either Word or LaTex. For those authors using LaTex, please follow the guidelines and template.
5. Authors are asked to sign an ISCA copyright form (http://www.isca-hq.org/j-copyright.htm), indicating that they are transferring the copyright to ISCA or declaring the work to be government-sponsored work in the public domain. Also, letters of permission for inclusion of non-original materials are required.

Publication Charges

After a manuscript has been accepted for publication, the contact author will be invoiced a publication charge of **$500.00 USD** to cover part of the cost of publication. For ISCA members, publication charges are **$400.00 USD** publication charges are required.

Revised 2019