COLUMBIA | SIPA
School of International and Public Affairs

Tech & Policy Initiative, Working Paper Series 1

COLUMBIA | SIPA
School of International and Public Affairs

It is with great pleasure that I invite you to read this multi-disciplinary and forward-looking Working Paper Series.

Over the past two years, Columbia University's School of International and Public Affairs (SIPA) supported the research of numerous experts and next-generation scholars that is reflected in this Working Paper Series.

These papers engage topics fundamental to understanding today's and tomorrow's world, and they tackle complex subjects that range from who should govern the Internet, to what the rules of engagement for cyber conflict are likely to be, to how privacy should be addressed in this age of Big Data, to how digital technology can be used to reshape traditional economic sectors and business models, and many more.

This academic work was undertaken with the vital support of the Carnegie Corporation of New York as part of SIPA's Tech & Policy Initiative, an ambitious effort to explore the intersection of the digital world and SIPA's core fields of study.

The goal of this Initiative is to bridge the gap between policymakers, academics and practitioners in cybersecurity, internet governance and the digital economy and to have a powerful impact on government policies and the behavior of the private sector. As an institution, SIPA is becoming a global hub for policy-relevant, multidisciplinary training, research and engagement on the important issues around technology and public policy. The Tech & Policy Initiative draws on many disciplines and talented researchers within SIPA, in other parts of Columbia University, and outside entities to develop insights that will translate into better and more effective policies.

This volume also includes papers prepared for SIPA's 2016 Global Digital Futures Policy Forum, an annual conference that brought together more than 200 scholars, private sector leaders, legal experts, entrepreneurs, technologists, and others to discuss the domestic and international dimensions of data governance in the context of technological change and globalization.

We hope you will find these papers insightful and an illustration of the many opportunities and challenges associated with tackling this complex and ever-evolving field.

Merit E. Janow
Dean, School of International and Public Affairs
Professor of Practice, International Economic Law and International Affairs

TABLE OF CONTENTS

Section 1: Cybersecurity and Cyber Conflict

Section 2: Global Internet Governance

Section 3: Economic Issues in a Digital World

Section 4: Activism, Rights and Civic Tech

Section 1:
Cybersecurity and Cyber Conflict

Susan E. McGregor*, Franziska Roesner, and Kelly Caine

Individual versus Organizational Computer Security and Privacy Concerns in Journalism

Abstract: A free and open press is a critical piece of the civil-society infrastructure that supports both established and emerging democracies. However, as the professional activities of reporting and publishing are increasingly conducted by digital means, computer security and privacy risks threaten free and independent journalism around the globe. Through interviews with 15 practicing journalists and 14 organizational stakeholders (supervising editors and technologists), we reveal the distinct—and sometimes conflicting—computer security concerns and priorities of different stakeholder groups within journalistic institutions, as well as unique issues in journalism compared to other types of organizations. As these concerns have not been deeply studied by those designing computer security practices or technologies that may benefit journalism, this research offers insight into some of the practical and cultural constraints that can limit the computer security and privacy practices of the journalism community as a whole. Based on these findings, we suggest paths for future research and development that can bridge these gaps through new tools and practices.

Keywords: Journalism, Usable Security, Usable Privacy, Organizational Practices

DOI 10.1515/popets-2016-0048
Received 2016-02-29; revised 2016-06-02; accepted 2016-06-02.

1 Introduction

A free and open press is a central characteristic of successful democracies and those societies moving toward democracy. Technologies can facilitate a free and open press by involving more people in the journalistic process (e.g., [1]) and reducing barriers to communication. However, technologies can also curtail these freedoms by creating computer security vulnerabilities—enabling, among other risks, leak prosecutions (e.g., [2, 3]) and cyberattacks targeted at news organizations (e.g., [4–6]). These security issues directly impact privacy and confidentiality goals for journalist-source communications. They contribute to "chilling effects" in which sources become reluctant to communicate with journalists about potentially sensitive issues [7], and they functionally abridge legal protections afforded to journalists in countries like the U.S. to protect the identities of sources [8]. In short, they limit the free operation of the press.

On the Need to Study Journalistic Organizations. Despite both the pressing need for—and increasing threats against—free and independent journalism around the world, the computer security and privacy community does not have sufficiently robust answers to scientific questions about how to design and implement usable and effective security- and privacy-enhancing tools for journalists and journalistic organizations. Though journalists are a community of interest to privacy and security scholars—in 2014 alone, multiple researchers (e.g., [9, 10]) argued that journalists are likely surveillance targets, and therefore a primary user group for proposed and/or evaluated digital security-related technologies—the scholarship on their actual needs and practices is quite limited within the computer security and privacy community.

Though recent work [11] examined the practices of *individual* journalists, this research left unanswered many questions about the role of journalistic *organizations* in the security and privacy choices of the journalists they employ. And while journalistic organizations share many features with other types organizations, our findings indicate that journalistic organizations have unique characteristics that affect their computer privacy and security risks and outcomes.

Our Study and Findings. To bridge this knowledge gap, our work considers the computer security and privacy practices, attitudes, needs, and challenges specifically for journalistic organizations as a whole.

Through interviews with 14 organizational stakeholders (supervising editors and technologists) and 15 practicing journalists at well-respected media organi-

***Corresponding Author: Susan E. McGregor:** Columbia Journalism School, E-mail: sem2196@columbia.edu
Franziska Roesner: University of Washington, E-mail: franzi@cs.washington.edu
Kelly Caine: Clemson University, E-mail: caine@clemson.edu

zations, we find that journalistic organizations and individual journalists share certain motivations towards computer security, particularly with respect to source protection and the reputational risks of a computer security breach. However, we find important differences in how these motivations translate to day-to-day security concerns and behaviors: for example, individual journalists rarely or never reported phishing, password strength, or the exposure of data to third-party cloud service providers as security concerns, though these were among the top concerns for organizational stakeholders.

We find that these differences lead to broader computer security challenges in the journalism community. For example, as organizational stakeholders struggle to balance various priorities in the face of limited resources, security and privacy concerns that have only a rare—if catastrophic—effect on their news "product" are pushed down the list. Individual journalists, meanwhile, must collect their "raw materials" from human sources and so are hesitant to introduce any barriers to those communications.

Critically, sources receive no direct goods, services, or compensation in return for the information they provide, and journalists are treated more as autonomous peers than subordinates in journalistic organizations. Both of these characteristics differ from norms in other fields where individuals share sensitive information with employees, such as retail, medicine or law. As a result, neither journalists nor their organizations have sufficient leverage to simply mandate that more secure tools or protocols be used by *either* journalists or their sources.

Our findings demonstrate that these structural and cultural features of journalistic practice have concrete implications for the design of secure, usable communication systems for this community. For example, the above issues make any single, centralized portal for all journalist-source communication impractical. Moreover, our findings reveal that journalists are unlikely to use a solution that they do not fully understand. We discuss further recommendations for computer security tools and practices within journalistic organizations, as well as opportunities for future work, in Section 6.

Contributions. Unlike prior work that studied the computer security and privacy attitudes, practices, and needs of individual journalists, we take a step back and consider the broader journalistic ecosystem. We make several contributions:

1. We identify key differences in the computer security priorities and concerns of individual journalists and organizational stakeholders (Section 4.1).
2. We surface broader challenges to robust computer security and privacy practices that arise within journalistic organizations (Section 4.2).
3. We highlight unique features of journalistic organizations, compared to other types of organizations, that have implications for security- and privacy-enhancing technologies intended for journalists (Section 5).
4. We provide lessons and recommendations from our findings, including paths for future research and development (Section 6).

2 Context, Related Work, and Motivation

We provide context and overview related work, identifying a need to study computer security and privacy specific to the journalistic context, with a comprehensive focus on both journalists and journalistic organizations.

2.1 Security Risks in Journalism

In recent years, the security of journalist-source communications has received increased attention, in part due to concerns about government surveillance [7, 12, 13] as well as legal attacks against sensitive sources [3, 13] in the U.S. and Britain. A number of high-profile technical attacks in recent years have also targeted journalistic and related organizations [4–6, 9, 10, 14].

These attacks have highlighted a need for secure communication and data management within journalistic organizations, and have helped spur the development of secure communication tools designed specifically for journalists (e.g., SecureDrop [15] and Dispatch [16]). The journalism community, meanwhile, has responded by developing digital security guides and trainings centered around existing technologies (e.g., [17, 18]).

Unfortunately, computer security practices within journalistic organizations suffer from both the usability limitations of existing computer security tools, and insufficient resources to robustly address or prioritize security issues. For example, over the last decade, many journalistic organizations have transitioned to third-party services like Gmail for their corporate email, and many new ones rely on such services from the start [19, 20]. These decisions have largely been driven by the need for lower costs and better usability [21]. Cost concerns and competitive pressures also drive news

organizations to rely increasingly on journalists' use of personal devices for work, especially mobile phones. As confirmed in our interviews, news organizations thus rely on a heterogeneous and generally unmanaged range of devices and communications systems, creating an environment of increased computer security risks.

2.2 Security, Usability, and Journalism

In addition to tools developed specifically for journalists mentioned above (e.g., [15, 16]), the technical computer security community has built many secure communications tools over the years, including OTR for encrypted chat [22], PGP for encrypted email [23], Tor for anonymous web browsing [24], and many others [25].

Yet these tools rarely see widespread adoption among either journalists (e.g., [26–28])—despite the significant risks they face—or the broader population (e.g., [29–31]). Moreover, scholarship on the actual computer security needs and practices of journalists and their organizations is limited. For example, no papers published at PETS in the last five years address the specific needs of journalists or journalistic organizations.

One recent study [11] focused on individual journalists, and revealed that limited usage of existing tools results not only from standard usability challenges but because these tools are difficult to integrate into the working processes of journalists (e.g., communicating with long-term sources). This work did not, however, evaluate journalists' practices in the context of their organizations. We bridge this gap by considering organizational stakeholders beyond individual journalists. We also surface unique aspects of journalistic culture that may influence the adoption or use of security- and privacy-enhancing tools in journalistic organizations.

From an HCI perspective, others have studied journalism more broadly than security. For example, Garbett et al. [1] studied the role of citizen journalism; Diakopoulos et al. [32] investigated methods for journalists to identify useful social media sources; and Taylor et al. [33] discuss the potential for citizen journalism to help communities take a role in a technological design process that takes into account their community's specific needs ("insight journalism"). These investigations highlight that the complexities of the journalistic process go beyond the level of individual journalists.

2.3 Usable Security for Individuals and Organizations

A large body of work exists on the interaction between individuals and organizations and its impact on security (e.g., [34]). While usability is a major issue in the adoption of secure technologies (e.g., [31]), organizational culture also plays an important role (e.g., [35]). Our work therefore seeks to provide a deeper understanding of both the task-specific usability issues that journalists face when using secure communication tools, and the ways that the unique culture of journalism and journalistic organizations affects the security approaches they employ. For example, in line with findings around other user groups (e.g., [36]), we find that journalists' level of understanding about secure communications plays a role in their use of certain tools. As we discuss in Section 5, we also identify important differences between journalistic institutions and other types of organizations that have implications for their computer security challenges, attitudes, and practices.

3 Methods

To study the computer security and privacy needs and practices among different stakeholders within journalistic organizations, we conducted semi-structured interviews with 29 participants: 14 organizational stakeholders (seven editors and seven technologists) and 15 individual journalists. All participants were current employees at media organizations, including print, online, broadcast and wire services, ranging in size from small, new, U.S.-focused media organizations to large, established, international media organizations.

We recruited participants through our existing professional network within the journalism community. Editors and technologists were recruited through person-to-person conversations with organizational leaders who then referred us to appropriate individuals. Individual journalists were identified through snowball sampling and were often recommended by a leader within the organization based on expertise and availability. While organizational leaders often first recommended we speak with their most security-conscious or -knowledgeable staffers, we explicitly requested also meeting participants who were non-experts, in order to ensure a broad representation of perspectives.

3.1 Participants

Because editors and information technologists both represent the organizational perspective, we refer to them collectively as organizational stakeholders. We selected these participants according to the following criteria:

- *Editors* are authorized to make editorial decisions for one or more journalists within the news organization who report directly to them. This means that the participant had the ability to approve pitches and stories for publication, as well as make scheduling and other resourcing decisions for coverage.
- *Technologists* are knowledgeable about and have influence on the organizations' information technology and, where applicable, computer security practices (e.g., one participant's title was "head of IT").

Individual journalists were selected according to the following criteria:

- *Journalists* are full-time employees of well-respected media organizations including print, digital and broadcast outlets as well as wire services, who regularly communicate with human sources in the process of reporting and publishing original journalism

Interviews with were conducted between November 2014 and September 2015. Interview length ranged from 15 minutes to one hour, and were conducted either in-person ($n = 23$) or via telephone/online video/voice conference ($n = 6$). The majority of participants were based in the U.S. and were interviewed in English, but eight participants were based in Europe and some of those interviews were conducted in the native language of the interviewee and translated during transcription. Seventeen participants were men (including all of the technologists) and twelve participants were women.

The participants in our study represent a broad range of privacy and security needs. Organizational stakeholders include those with editorial and/or technical responsibility for highly sensitive topics and materials—including those of potential interest to nation-states–as well as less sensitive, general interest coverage. Likewise, some journalist participants dealt regularly with highly sensitive topics and materials and had firsthand surveillance experience, while others described their work as non-sensitive and routine.

3.2 Ethical Considerations

Our entire protocol was IRB approved. Furthermore, we considered ethical principles such as beneficence, minimal risk, voluntary consent, and respect for privacy. Specifically, because of the potentially sensitive nature of some of our inquiries, we made explicit efforts not to leave a digital trail that could later identify the participants we interviewed. When organizing interviews, we avoided corresponding directly with interview subjects via email in advance of the interview. Instead, the interviewer typically corresponded with an organizational leader who then suggested potential interviewees. Those who met the criteria and were available participated.

During the interviews, we were careful not to elicit any protected information which journalists would normally not share, such as details about specific stories or sources. In accordance with concerns expressed to us during recruitment, we agreed not to publish organizations' specific security protocols so as not to compromise the effectiveness of those practices.

All participants agreed to being audio recorded during the interview and all participants answered all of the questions in the interview script. We stored and transmitted audio recordings and de-identified transcripts only in encrypted and/or password-protected form.

3.3 Interview Script

We varied our interview script by the type of participant: journalist, information technologist, or editor.

Organizational Stakeholders. Interview questions for editors and technologists were divided into three general sections: questions about strategies and policies, questions about tools and software, and questions about organizational culture and challenges.

For editors, the first section focused on what kind of trainings were provided to newsroom staff, whether the organization made specific recommendations to journalists about how to manage information related to stories, and how information security did or might factor into decision-making about publication decisions (e.g., when to publish a story). This section also assessed the editorial participant's awareness of information security resources or personnel within the organization.

For technologists, the first section addressed similar questions, but focused on whether information-security specific trainings and/or recommendations were made to journalists by the participant's department,

and whether information security for journalists was an explicit mandate for someone within the department.

The tools and software portion of the interview for both groups focused on security and privacy software that was available to or in use by journalists. Editors were asked about any software they or their team had attempted to use—with or without success—as well as unaddressed technology needs related to security. They were also polled about non-technological security challenges and what would be required to address them.

Technologists were queried more specifically about the tools, technologies, and computer administrative rights to which typical journalist users in their organization would have access. We specifically asked about whether any security or privacy software (specifically OTR and GPG) was part of users' default computer profiles, and whether individuals had administrator rights to install new software. We also asked about third-party and cloud-based services licensed by the company, as well as what digital storage and communication services the organization provided directly (e.g., a virtual private network, shared network drives, etc.).

The final portion of the interview addressed organizational culture and challenges. Participants were asked to assess the most serious information security issue faced by the organization, and to characterize the outcome should that issue arise (e.g., if the website was hacked). Editorial participants were then asked about challenges they had encountered or anticipated in implementing stronger security or source protection policies in the newsroom. Technologists were asked about both technical and non-technical challenges to implementing stronger information security, and were asked prioritize two journalist behaviors as the top of their "wish list" for improving information security in their organization.

Journalists. Interview questions for journalists focused on their communication with sources, computer security needs, and data management practices. These were elicited in two parts: the first asked participants to answer questions about source communications by calling to mind their actual interactions with a specific source from a recently published story. The second focused on general questions about data management and sharing, as well as the journalist's own computer and information security concerns and resources, including those in their personal network.

	Concern	Journalists	Organizations
Shared (Sec. 4.1.1)	Source Protection in Communication	6	8
	Reputational Risks	5	7
	Competitive Value of Risk of Infosec	3	4
Differing (Sec. 4.1.2)	Sources Drive Comm. Method	7	3
	Phishing	0	8
	Password Sharing	0	10
	Weak Passwords	1	4
	Third-Party or Cloud Apps	1	7
	Limited Resources	0	12
	Liability / Libel	0	4
	Protecting Journalists Abroad	1	3

Fig. 1. Table 1. Journalist ($n = 15$) versus Organizational ($n = 14$) Stakeholder Concerns Related to Computer Security.

3.4 Data Preparation and Analysis

Once all interviews were complete, we transcribed the audio recordings and coded the resulting transcripts using an iterative inductive process [37]. We then identified themes based on the coded transcripts.

4 Results

We organize our results around two overarching themes: (1) specific shared and differing security concerns between organizational stakeholders and individual journalists, and (2) broader challenges to organizational computer security in journalism. Together, these results reveal opportunities for improving the collective security practices of journalists and journalistic organizations.

4.1 Journalist versus Organizational Computer Security Concerns

Overall, we found that while individual journalists and organizational stakeholders share similar security motivations (e.g., protecting source identities), the way each group prioritizes computer security and privacy threats and concerns can differ drastically in practice. Table 1 summarizes these results, and this section discusses these findings in detail.

4.1.1 Shared Priorities

We begin by highlighting two areas of shared priority that drive computer security choices for both journalists and organizational stakeholders: the need to protect source identities and the reputation of the organization.

Source Protection. Both individual journalists and organizational stakeholders described the protection of sources as a critical information security concern. For example, one journalist said:

> My sources trust me to keep their information. It would be a problem for my news organization, to not be able to protect my sources, to protect the files or documents. (J5)

Organizational stakeholders expressed their concerns about source protection in particularly urgent terms. For example, while one journalist acknowledged that exposure of a source's information "would probably not be great" (J11), organizational stakeholders tended to describe source protection as "vital", "crucial," and "critical." As one editor put it:

> [Source protection is] terribly important. It's important in the U.S. because there are laws about that, but it is particularly important overseas where governments can intimidate those who talk to Western reporters and/or take reprisals against our local staff in those countries. (E5)

Organizational stakeholders also expressed a sense of responsibility for the security practices of journalists affiliated with their organization. For example:

> If [a journalist is] texting from a personal account and I didn't know about that or didn't strive to prevent that and then that somehow gets into the hands of the public when we promised anonymity—and causes whatever results the person was trying to prevent by asking for anonymity and we agreed were reasonable by granting it—that's a grievous journalistic error. (E3)

While these findings suggest that it is the responsibility of both individual journalists *and* the journalistic organization to protect sources, only one organization in our sample included secure communication tools by default, as we discuss in Section 4.2.1.

Reputation Protection. Like source protection, reputational concerns were also prevalent in both groups of participants (five of 15 individuals and seven of 14 organizational stakeholders). For journalists, however, reputational concerns primarily revolved around the worry that the failure to protect a source would affect the ability to attract future sources.

Organizations' concerns about reduced access to sources, however, was overshadowed by the possibility that failure to protect a source would compromise the credibility and integrity of the brand; both the importance and fragility of the organization's reputation was mentioned by multiple stakeholders:

> [We] have, I think, a pretty good reputation. But it could get blown away in an instant, so we have to make sure that we protect everyone, because if that gets out, then we'll never live it down. (E2)

> [One of the] really serious problems is the brand image, the damage to the brand. If you're not deemed trustworthy. . . . Trust and reliability are indispensable to us. (E1)

So, while both individual journalists and organizational stakeholders are concerned about protecting sources, their motivations for doing so diverge: individual journalists worry about *their own* ability to attract future sources, while organizational stakeholders worry about brand image, and the ability of *all* their journalists to attract future sources. Nevertheless, both individual journalists and organizational stakeholders are strongly and similarly motivated to protect sources. This motivation may lead to journalistic users being willing to adopt new technologies, spend more time using technologies, and otherwise sacrifice some amount of ease of use and convenience [38]. As we discuss in Section 5, however, even motivation cannot compensate for missing functionality.

4.1.2 Differing Concerns

Though both individual journalists and organizational stakeholders identified source protection and reputation management as substantial motivators of better computer security practices, the way priorities manifest in practice can differ dramatically. For example, several of the most pressing concerns for organizational stakeholders—such as libel, phishing, and manageable computer security practices—were not mentioned by even a single individual journalist.

Sources Drive Communication Method. Since one goal of individual journalists is to gather information from sources, their concerns include their *sources'* technical abilities and access to technology. Echoing previous work [11], we find that lowering the barrier to communication is critical. As one journalist put it:

> In my experience, taking down barriers is the most important thing to source communication for 99% of the people you need to access as a journalist. (J14)

As a result, the communication methods used by journalists are driven largely by the preferences of sources; even journalists who understand the risks of insecure communication methods may choose those tools over secure ones, if that is what the source prefers. In general, journalists expressed deference to time, availability, and convenience of sources over security. When asked if they would feel comfortable asking a source to use a specific form of communication, journalists agreed:

> Absolutely not. I would never impose any kind of burden on a source to communicate in a way that they're not used to. You're taking their time. (J14)

> There are few sources that I've had that I would feel comfortable asking them to use, like, hyper-specific technologies to talk to me through, like a different app, or a funky encryption service, or something. (J13)

While some of these concerns were acknowledged by organizational stakeholders, they generally expressed less concern about the repercussions of losing a particular source. For example:

> I mean, my fear for the secure communication with sources is definitely like, I don't want [a source] to not want to wait for someone [e.g., a reporter] to figure something out and so they go somewhere else. But that's not, like, an existential fear, because if we lose a story, then I have plenty of ways to communicate with a new one. (E2)

While organizational stakeholders' focus is on the security and practices of the organization's employees as a whole, perhaps because they worry primarily about organizational reputation, individual journalists "on the ground," are more focused on ensuring a source is comfortable and willing to talk. Whereas an organizational stakeholder may be willing to lose a source in a case where they would not use secure communication, individual journalists may not be.

Phishing. Unlike source protection and reputational concerns, computer security issues not directly connected to newsgathering—such as phishing and password practices—were articulated only by organizational stakeholders. Eight of 14 organizational stakeholders expressed concern about phishing attacks—a concern that was shared equally between editors and technologists. By comparison, none of the 15 journalists interviewed mentioned phishing as a computer security concern.

Concern about phishing among organizational stakeholders stemmed from two distinct characteristics of this type of attack: the pervasiveness of the tactic and the potential severity of its consequences. Asked to characterize the organization's biggest security risk, one technologist said simply:

> Phishing, and DDOS. Because they're cheap and they're effective. (T2)

In terms of potential severity of the consequences, several recent academic studies discussed targeted phishing as a primary cause of compromise for politically-involved organizations (such as NGOs, activist organizations, and journalistic organizations) [9, 10]. Compromising the account of one of an organization's employees may provide access to significant sensitive information, including source identities and unpublished stories. For example, one technologist commented:

> We had a targeted phishing attack against us, that, after doing some analysis, we determined it was probably SEA [the Syrian Electronic Army]. . . . We had a couple of people whose email accounts were compromised. (T3)

In other organizations, the consequences have been much more severe (e.g., [39]).

One editor interviewed also highlighted an incident where a phishing attack resulted in significant downtime within the organization, a serious business and credibility issue for journalistic outlets where, unlike banks, for example, 24-7 operations are viewed as a requirement:

> The company was attacked by an international group. . . . Suddenly at 10pm everyone is getting a phone call [from IT] saying you've got to change your password now. We've had other phishing things but this one took the whole server system down, the whole nine yards. (E5)

The always-on business cycle of journalism also means that recovering from a phishing attack may be particularly challenging, as the timeliness and currency of information are of significant competitive value. Interrupting the publication flow and/or reverting to backup data even a few hours old can be commercially damaging.

The disparity between the individual and organizational perspectives here is notable. While many organizational stakeholders expressed concern about phishing, no individual journalists mentioned this risk. It is not clear why journalists seem unconcerned, or at least less concerned, about phishing. One possibility is that journalists are aware of the risk, but may not consider it their responsibility. As one technologist put it:

> Some people have the attitude, I don't wanna be bothered by this stuff, can't IT just fix it, don't you have something that can keep everything secure, that doesn't require me to do anything different at all. (T1)

Another possibility is that journalists are simply unaware of the risk. If so, then why are journalists unaware when the organization is keenly aware? Do journalistic organizations offer training that includes information about phishing, and if so, why it is ineffective? One possible answer may be suggested by the resource limitations we discuss in Section 4.2 below: that the attention paid to computer security by all parties must be balanced with other competing concerns.

Password Security. Password security was also mentioned by all technologists interviewed and three of seven editors as a top computer security concern, both in terms of password sharing/reuse and password strength. Several organizational technologists put improving password security and practices at the top of their "wish list." As one described it:

> One of [the items on my wish list] would be to improve password security. . . . I think that there's probably a lot of people who aren't actually using password databases and who are probably reusing passwords sometimes, and who are using weaker passwords than they need to and things like that. (T6)

This desire also extended to personal accounts and devices, congruent with the fact that all organizations where interviews were conducted had "bring your own device" practices. As another technologist mentioned:

> I guess the first would be just better personal password policies. (T3)

By contrast, only one individual journalist mentioned password sharing, but as a positive means of information management (to collaborate with colleagues), rather than a security risk. Again, the disparity here is worth considering. Why do organizational stakeholders—but not individual journalists—consider password security to be such a high priority? Perhaps editors and technologists are (as a result of their positions in the organization) more aware of incidents involving password security, and/or are trained to be attuned to this risk. If either of these is the case, why is this information not making its way to end users (journalists)?

Third-Party and Cloud Applications. Finally, while seven of 14 organizational stakeholders expressed concerns about the computer security risks of using third-party and cloud applications, these issues did not appear to occupy the attention of individual journalists.

For example, prior work [11] indicated that individual journalists did not report computer security concerns associated with third-party applications or the remote syncing of data. Yet technologists we interviewed expressed concerns about both USB drives and third-party services, a concern shared by savvy editors as well. As one said:

> Sometimes I'm just walking through the organization and I'll see someone with an Evernote open—and it's like, just making sure that you're not putting your source phone numbers in there! If you want to keep your recipes in there that's fine, but be careful. (E1)

Likewise, while technologists saw benefits in cloud infrastructure, they also appreciated its risks:

> We wanna take advantage of all the good benefits you get from being in the cloud. Scalability, higher performance, bigger global footprint, etc. But as we've learned, these parties can get subpoenaed and they can be gagged, and so we definitely first and foremost think about what is the data that we think about possibly migrating to the cloud, and from an infosec perspective is it even a candidate? (T1)

At some smaller organizations—where budgets were not always sufficient to support an in-house information technology department—concerns about third-party services also extended to physical computer and networking infrastructure, which was sometimes maintained by third parties, rather than direct employees.

While better-resourced organizations in industries like retail and law may have purpose-built (if less than usable) systems that satisfy unique needs, for both budgetary and efficiency reasons, journalistic organizations increasingly use "off-the-shelf" software for communication and coordination. One side effect of this is that secure communications tools compare particularly unfavorably with these large-scale solutions. For example, one participant described the challenge of encouraging the use of secure tools on a distributed project:

> I had to call the editor running the story to say, let's just make sure we're being careful here, because Google will turn this stuff over to the feds in a heartbeat. . . . The problem with Google Docs is it's awesome – I mean it's so seamless and intuitive. Much more so than some of the more secure solutions. (E1)

4.2 Challenges to Organizational Computer Security in Journalism

Stepping back, our interviews with organizational stakeholders also surfaced several broader themes directly related to the systemic challenges to organizational computer security in journalistic organizations, in part due to the disparities in day-to-day concerns and priorities among different members of the organization. While many of these challenges echo issues present in other types of organizations, we discuss further in Section 5, there exist important ways in which these issues are particularly challenging in the journalistic context.

4.2.1 Supporting Software

An organization's technical staff is tasked with supporting a variety of hardware and software for the employees of that organization. This task is simplified when the necessary tools are standardized across organizational users, when those tools come with sufficient external support and/or can be sufficiently controlled by the IT department. As a result, for example, un- or semi-supported projects like GPG, or externally-managed cloud services like Google Docs can be more challenging to adopt than explicit enterprise solutions like Microsoft Outlook. For example, one technologist interviewed discussed Google Docs:

> It's a case of: Who owns this? Who's going to pay for it? Who's going to pay for the licenses? And then it becomes an issue around: is this a strategic imperative? Who controls it? (T5)

As a result of the difficulty of supporting one-off tools, technical staff members may be hesitant to support specific computer security tools used by only a small number of individual journalists. For example, one technologist mentioned learning about new security tools from journalists themselves, but admits some reluctance about supporting such tools:

> If you come to me and tell me that you need to be able to encrypt the email that you're writing to a source, we're at the point now where we're going to tell you that the tool that you are going use is GPG 4.0. We're not going to go use some other tool. We find some tool and standardize on it, until we find some reason that it's no longer going to serve our standard. (T1)

The challenges of supporting software also extended to what users were provided with by default; only one organization in our study provided computer security software by default on regular user profiles. Moreover, only 6 of 15 journalists had the admin privileges required to install additional software. For technologists, this was in part a support issue:

> Historically, [users] had too many administrative rights on the PCs and it got them into trouble. They would just install something that would conflict with something else on their machine. (T1)

One potential side effect of this approach is that newer tools—which necessarily have lower adoption rates—may never be practically available to institutional journalists even if they are more usable or more secure than more established alternatives.

4.2.2 Distributed and Collaborative Culture

The inherently distributed and collaborative nature of journalism presents specific challenges to communicating securely. As one journalist put it:

> We try to use the most secure tools possible. And I think the problem was that at first we were only two or three . . . and now we are maybe a dozen. And as most of my colleagues are not really good with technology we have to lower our expectations in security. (J9)

Another participant expressed a similar difficulty: the most trusted secure chat solution (OTR) doesn't support multi-party chat.

> I use CryptoCat for stuff that is for someone that I know I'm not going to be able to figure out how to get OTR on—it's so much simpler. . . . It's also nice because it has a group function, and I haven't really found. . . I don't know how secure it is, so I wouldn't necessarily use it for the most sensitive of things, but for something that is sensitive and I need to have a group conversation about, I would go for that because it's simple. (E2)

This finding has implications for the design of secure systems for journalistic practice: targeted solutions should consider all stakeholders and communication partners, not just individual journalists and their sources. The ability to communicate securely with colleagues is a critical part of the journalistic process.

4.2.3 "Us-vs.-them" Mentalities

Though the pressure to adopt certain computer security tools may come from individual journalists, as noted above, organizational stakeholders must typically manage the computer security of an entire media organization. As a result, an "us-vs.-them" mentality can sometimes begin to characterize the attitudes of organizational stakeholders towards individual journalists, or of editorial staff towards IT department staff. For example, one editor described enforcing better computer security practices among journalists as a problem of "herding cats" (E4) while another expressed frustration with his organization's IT department:

> It's the journalists dragging the IT people kicking and screaming and saying, you need to think about China, you need to think about Russia, because we have people there. They think of it very much in hardware terms. (E5)

We also found evidence that the culture of journalism—despite the presence of official hierarchies—functions in a largely egalitarian, peer-oriented way. When speaking about security, it was clear that institutional actors were uncomfortable with simply imposing requirements:

> Occasionally reporters will ask or start using services that we're a little less comfortable with that are maybe a little more convenient . . . and there's no prohibition but we sit down with them and say, "We need for you to understand the risks associated with this." (E1)

There was also the sense that imposing requirements would be ineffective:

> [Security] has to be enforced in some way. Not necessarily with punitive repercussions, but something that doesn't allow people to work around it. Journalists, what they are good at, is overcoming an obstacle that they don't choose to deal with. (E5)

4.2.4 Limited Resources: Secure Journalism Comes with a Cost

Maintaining strong information security and data management practices at a journalistic organization requires devoting significant resources exclusively to this purpose. These resources must be gleaned from an existing pool of limited people, money, skills, and attention otherwise focused on journalistic and business tasks.

Uncertain priorities. Devoting resources, in terms of people or infrastructure, to computer security costs money—money that may otherwise be put to other uses within the organization. While downtime in the organization cost credibility, it was often unclear what "uptime" was worth. In the words of one technologist:

> I sort of ran the numbers. . . . That would cost us anywhere from $25-50K, just in infrastructure costs alone, right? And like, we can scale up. The way that we've architected our environment, we can scale up to—whatever we need. But, it costs money. . . . I can't make those decisions, about whether or not we take down content because it costs us 100 grand over a two-day period, right? That's something that [the editorial leaders] will have to decide. So, I want their input on that kind of stuff. I mean, if we're coming out with a new application tomorrow, we could spend a lot of money securing it. We can make it a hardened target. But do we need to do that? (T2)

Limited Time. One of the most compelling and frequently cited issues our interviews revealed was the broader opportunity cost of computer security. This was particularly true for editors and technologists, who often referred to managing competing priorities when asked about the role of newsroom source protection and information security. As one participant put it:

> There are lots of other fires to put out every day, so I think it's probably an issue that doesn't get the priority in our newsroom that it deserves. (E3)

The cost of computer security was also felt as a limitation on executing journalism itself. As one editor said:

> There's a kind of like an encryption tax on the work of journalists these days. . . . We have to spend time doing things that we otherwise wouldn't do in order to communicate securely with sources and with each other and to responsibly use documents that we have. And it takes time. It means that we have less time to talk to people, to go and travel, etc. We still do all those things, but there's a chunk of our time that's spent on security, and not on other forms of reporting. (E6)

Limited Attention. Even when computer security interventions were taken, however, editors and technologists alike expressed the need to carefully manage the limited attention they felt journalists had for these issues. As one technologist said:

> We always feel like we're vying for part of a limited attention span. If you want to communicate something, you want to be sure you have their attention. . . . If you throw too much at them, none of it gets attention. . . . If you tell somebody come to this workshop, we're going to tell you how to not get phished, or how to keep your phone call encrypted—

> unless you have cookies, two people are going to show up. (T1)

Limited Expertise. Another frequently cited limitation on better computer security was insufficient expertise within the organization. At times, this limitation prohibited the adoption of very specific tools or protocols, as one technologist noted:

> I would love to force people to use a password manager, but that's not realistic at this point—frankly because I'd probably be the one who'd end up doing desktop support on that and I don't have the time for that. (T3)

Indeed, prior work [11] found that individual journalists often did not feel that they had someone with technical expertise within their organization to whom they could go for help with computer security related issues.

In other cases, insufficient staff expertise simply creates an imbalance of work:

> It ends up being that that one person has way too much work to do to support everyone in the office. And then there's only so much that you can do remotely to support people. (T6)

Limited Understanding. Expert staff in the strictest sense, however, was not the only way in which expertise limitations were felt. Multiple participants indicated the importance of their own need to understand how computer security tools work:

> Having people that are journalists and actually want to know everything, they're like: "Wait, I don't understand. I need to understand how this functions before I start to use it." Which is also a thing of "I need to understand how it functions so I feel comfortable using it." And so it's not that hard in abstract to think like, "Great, you're basically putting everything into a cipher and then you're sending that cipher to someone else and you have two different keys." Like, it's not that crazy, but when you start to actually execute it you're like, "Wait, I have to have this key, and if this key gets out then I'm in trouble, but this is also called a key but this is something I share with everyone?" (E2)

In other words, individually understanding the how and why behind computer security practices and tools was an important factor in being willing to use them. This attitude highlights an opportunity to engage with individuals on these issues and change their behaviors:

> My initial response to being prompted to set up two factor authentication on my personal accounts—like on my Gmail account or my Facebook or wherever—was deep skepticism, because it just felt like another corporation asking for my phone number. . . . It was only really after . . . the whole tech team gave kind of a broader and clearer explanation of why it matters, and it didn't just seem like some kind of fishy thing from a faceless corporation, but more like, you know—here's a person I trust who's looking out for my company telling me why this matters for us as a company. And shortly after we went to two factor for the company, you know, I sort of acquiesced to all of the various two-factor requests in the rest of my life as well. (E3)

As we discuss in Section 6, clear communication by organizational stakeholders with journalists about computer security goals and consequences is thus important. This observation also holds implications for the designs of computer security tools for journalists, which may see more adoption if their benefits are clearly explained.

4.3 Summary of Findings

Our findings suggest that individual journalists and organization stakeholders within journalistic institutions consider and prioritize different computer security and privacy concerns. Though both groups take very seriously their professional duties to protect sources and manage the organization's reputation, organizational stakeholders are focused more inward, concerned with the computer security practices of their employees (e.g., resilience to phishing attacks) and the tradeoffs in how to allocate resources. Individual journalists are tasked with collecting information from sources, and so their use of secure communication technologies is often influenced by the abilities and attitudes of sources; their concerns surrounding computer security lie more in whether and how to protect those communications, and less on their own individual behavior within the organization (e.g., password practices). As a result of these differing viewpoints and priorities, different organizational stakeholders in our interviews sometimes expressed frustration with other groups' failures to properly understand or support their priorities. Our interviews also surface additional important challenges to journalistic organizational computer security, including the challenges of supporting a variety of software across the organization and the need to balance computer security practices with other priorities in the face of limited resources (time, money, and expertise). These challenges expand on those previously identified in the context of individual journalists, such as the importance of a source's comfort level with computer security technologies [11].

5 Discussion: Journalistic versus Other Organizations

Naturally, some of the computer security challenges experienced by journalists and their organizations are also faced by other users and organizations. There are, however, many ways in which the resources, needs and culture of journalism differ significantly from other communities of practice, suggesting the need for additional research, tool, and strategy development to be focused specifically on journalists and their organizations.

5.1 Similarities to Other Organizations

At face value, many of the concerns expressed by journalistic organizations are similar to concerns of other organizations. For example, like many organizations, journalistic organizations must balance security concerns with other priorities in the face of limited resources of time, attention, expertise and money.

Phishing is also a common concern: phishing as a form of cyberattack is increasingly common, growing over 90% in 2014 [40]. Proposed solutions for phishing, such as training email recipients, have been unsuccessful [41]. Successful anti-phishing strategies that address either organizational practices in general and/or recipient practices can improve all organizations' information security, including journalistic organizations.

Similarly, insecure password practices are a pervasive problem across different organization types [35]. For example, people across organizational domains reuse passwords [42], indicating that journalists and journalistic organizations are not alone in their concerns about and less than optimal practices around passwords. In the case of journalists, there may be opportunities to use journalists' dedication to the protection of their sources as motivation to change their behaviors.

5.2 Unique Features of Journalistic Organizations

Beyond these basic similarities, our findings highlight several important cultural and functional *differences* between journalistic institutions and other types of organizations with comparable security needs. Thus, while on the surface it may seem that journalistic organizations could simply implement the types of organizational security practices in place at medical, legal, or retail organizations, solutions must consider the nature of journalistic organizations specifically.

5.2.1 Journalists as Atypical "Users"

As prior work indicates [11], journalists often select communication tools based on the preferences of their sources. In this sense, individual journalists may share some computer security needs and habits with other types of of "consumer-facing" industries, like retail and medicine. At the same time, however, individual journalists have both greater autonomy and responsibility in their work with sources. For example, while a retail clerk at a major chain store cannot independently choose to accept barter as a form of payment, individual journalists can (and do) accept as many forms of communication "currency" as possible. From an organizational standpoint, then, journalists are more like independent contractors than direct employees: they are responsible for delivering a content "product" to their organization, but they are individually responsible for how it is produced. As a result, journalists prioritize communicating with sources over security concerns, as this is the core "business" of journalism. As one editor put it:

> The effective [security] tools that are out there are pretty kludgey. And then because they're kludgey they get in the way of people being able to do their jobs. And I think given the choice of being information aware and secure and getting your story done, most journalists are gonna get their story done. It's about that simple. (E4)

Though an apparently simple solution would appear to be centralizing and mandating particular protocols or software, our research suggests that this approach would be a poor fit for the distributed and heterogeneous nature of journalistic organizations, as we discuss below.

5.2.2 Sources as Atypical "Clients"

Journalistic organizations are relatively unique in their desire to protect the privacy of an entire class of . . . organizational participant: sources. These participants are unpaid and unaffiliated with the organization itself, but are still a critical component of the journalistic product. While the cost and stress around legal concerns are substantial, the primary driver for journalistic organizations' desire to protect the security and privacy of sources is reputational, and ultimately existential: if

the organization does not protect the privacy of their sources, other sources will not work with them.

This observation supports existing research on privacy-enhancing behaviors suggesting that people avoid technologies or organizations that do not meet their privacy needs [43]. If journalistic organizations do not support sources in both revealing information *and* remaining private and/or anonymous, sources will be more reluctant to share information. Thus, the implementation and perception of more secure communications practices by journalists may also reduce source "chilling effects" that inhibit newsgathering [7]. Unlike organizations where "clients" directly benefit from their interactions with that organization (e.g., law firms), these issues are particularly existential for journalism.

5.2.3 Peer-Oriented Culture

One important feature of journalistic culture that we noted throughout our interviews was the dominance of peer-oriented attitudes despite formally hierarchical organizational structures. In journalistic organizations, for example, editors wield significant influence over individual journalists' work, including the ability to approve (and "kill") stories, and allocate time and financial resources for projects. That said, as discussed in Section 4.2.3, we noted a consistent reluctance on the part of editors we interviewed to mandate particular security practices for journalists in their organizations—or skepticism that such mandates would be effective.

5.2.4 Decentralized Control: De facto and by Design

Congruent with the reluctance on the part of organizational stakeholders to mandate particular systems or punish non-compliant journalist, our findings also reveal significant decentralization—both de facto and by design—in journalistic organizations' information security practices. This decentralization again differs from other, more top-down organizations where computer security practices can be more easily mandated.

De Facto Decentralization. Much of the decentralization of journalistic systems was attributable to the interaction between the wide range of populations and jurisdictions that media organizations touched, as well as to their limited resources.

> Our IT department is very reluctant to have a "one size fits all" approach. As a result they have no size that fits anyone. There is no good intersection between IT and the core of the business, which is news gathering. . . . It's like, here's an iPhone, good luck. (E5)

Decentralization by Design. Interestingly, however, there were instances in which the decentralization of information was treated as a security measure in itself, in a form of "security through obscurity."

> There's a case that we're working on about a sensitive topic, and I don't know the person's name . . . And I'm sure I could ask for the person's name, but there's no reason to know the person's name. . . . What you don't know you can't leak, you can't get in trouble with it, you can't get in trouble for having it. (E7)

A similar sentiment was expressed by one technologist:

> From a user support perspective, it would be good to store . . . passphrases, but our legal folks don't want to do that, because then *we* can be compelled to turn over passphrases by subpoena. Better that we not know them. (T1)

In this case, the very decentralization of information was perceived to help minimize its potential exposure points. This sentiment was echoed by another organizational leader, who commented:

> I feel like it's something that, even if [messaging service] is not—even if it was theoretically not super secure, it would be so hard to figure out what we were doing and where that is. . . . You're like, using something that's not the most popular is maybe the way to go. (E2)

Thus, the decentralization within journalistic organizations may have (possibly unintentional) security benefits, but it also limits the effectiveness of top-down mandates of computer security practices that may be effective in other types of organizations.

6 Lessons and Recommendations

Existing research on individual journalists' information security practices [11] recommends further work around issues of first contact, authentication, metadata protection and knowledge management. While valuable, these recommendations do not take into account the role of journalists' organizations in shaping their information security abilities and choices.

Additionally, though at first the security challenges of journalistic institutions resemble those of organiza-

tions in other industries, we identified functional and cultural aspects of journalistic organizations that set their needs apart. As a consequence, security solutions relying on conventionally opaque, tightly-coupled systems are unlikely to be useful in journalistic settings.

We therefore recommend that protocols and technologies designed for organizational journalists leverage well-known protocols, support multi-party collaboration, and clearly indicate the security processes and protections at work in a given tool. We close with reflections on opportunities for future work.

6.1 Rally Around Known Protocols/Tools

Recall from Section 4.2.1 that supporting a diverse range of software is a particular challenge for organizational participants. As a consequence, interoperability and adherence to known standards is viewed as critical:

> Probably the best tool, by far, is OTR, because everyone has a Gmail account, everyone has some sort of chat account, and since it's so seamless with Adium, and it's like once you have that open it's so simple, and it's great. (E2)

> ... We're gonna tell you that the tool that you *are* gonna use is GPG 4.0. We're not gonna go use some other tool. We find some tool and standardize on it. (T1)

Thus, we recommend that members of the technical computer security community wishing to develop tools for journalists work closely with organizational stakeholders to understand organizational needs and constraints, and to help support the deployment and maintenance of these tools. Without such support, the limited resources of journalistic organizations will greatly limit the adoption potential of new, and particularly of experimental, tools.

6.2 Support Multi-Party Collaboration

As we noted in Section 4.2.2, the production of journalism is inherently distributed and collaborative; privacy- and security-enhancing tools designed for the journalism community must support these functions. Our interviews suggest that efficiency and seamlessness of collaboration were high priorities for organizational stakeholders, and several journalists described using third-party services (like Google Docs) specifically to share information with others or between devices (e.g., with a home computer). In fact, our findings suggest that support for collaborative functionality is important enough that even security-conscious users will choose less secure tools that support these activities. Thus, while journalists are highly motivated to use security- and privacy-enhancing technologies, our broader findings suggest that these motivations will not overcome missing functionality. We therefore recommend that computer security tools seeking wide adoption consider implementations that support collaboration.

6.3 Clearly Communicate Security Goals and Consequences

Organizational concerns are often not visible or tangible to individual journalists, while these concerns are highly visible to organizational stakeholders. For example, organizational security concerns like password sharing and phishing rarely produce immediate or highly visible consequences at the individual level. This leads to an informational asymmetry between journalists and organizational stakeholders, who are often responsible for managing the consequences and identifying the security breach. As one technologist put it:

> If a user falls for a phishing attack, and they don't report it, and they don't even realize what happened—then, you know, what can you do at that point? It's only a problem when it becomes troublesome when it actually manifests into a security incident. And by that time it's too late. (T2)

Thus, helping journalists appreciate the impact of their individual behaviors on the organization may be a useful strategy for increasing secure computing behaviors. In one recent study, researchers demonstrated that employee attitudes toward organizational password policies affect password behaviors [35]. Similarly, we propose that properly explaining and contextualizing computer security practices for all journalists in an organization may help shift attitudes, priorities, and practices.

Better communication among the different stakeholders within organizations may also help overcome some of the gaps we observed. In the words of one technologist:

> My second biggest wish actually would be more communication and less whining. When something goes wrong, that they communicate it immediately, and not try to find a workaround. ... We don't have all the answers here. (T5)

In the other direction, clear communication from technologists is equally important:

> Having a technology team that can speak in fluid, persuasive non-jargon-ridden sentences is just like, an insane asset to any company. Because there's many ways to roll out security tweaks, and doing them where you make a clear and lucid case for what you're doing and why—there was just no pushback whatsoever. Everyone was just like, "OK, great. We'll do that." (E3)

When asked what pushback could be anticipated to efforts to impose further security in the newsroom, another editor commented:

> I think if explained, not really any. ...I think if it were presented as, this protects your sources—we are in the information business, we know that this is a contemporary issue in society, and in the industry. I don't think you're going to get any resistance from the journalists. (E5)

Thus, we recommend that journalistic organizations focus on clear communication channels among all stakeholders surrounding computer security issues. Building on the observation in Section 4.2.4 that journalists do change their security-related behaviors when they understand the issues, we also recommend that tool designers consider these issues within tools themselves—for example, providing clear user interfaces and explanations for the risks addressed and the benefits provided by security- or privacy-enhancing features.

6.4 Opportunities for Future Work

While our work clearly demonstrates that there are differences in computer security concerns between journalists and organizational stakeholders, as well as unique features of journalistic organizations compared to other types of organizations, a number of questions remain, presenting opportunities for future work.

Designing Tools and Practices. Our findings raised questions for the design of general organizational practices and specific computer security tools that can mitigate the challenges we observed. For example, organizational stakeholders devote significant effort to computer security issues not specifically related to journalism, like phishing and password practices. How can practices or tools better mitigate these issues so that organizational stakeholders may devote their computer security resources elsewhere?

Awareness and Education. We observed that journalists are willing to use computer security tools when they understand the risks they address and how they work. This finding suggests that education and awareness efforts can be successful in this space, particularly if they situate security in terms of other priorities and experiences. For example, training could focus on helping journalists understand that their computer security behaviors impact the safety of their colleagues and the reputation of the organization. Building on successful prior work in the area of anti-phishing education e.g., [44]) and lessons learned from industry (e.g. [45]), we believe that educating users about the security and privacy risks—and meaningful ways to mitigate them—has potential for significant impact in this space.

Considering all Stakeholders. Even when appropriate practices or tools exist, their adoption may fail in several ways: because sources are unable to use them and thus journalists avoid them; because organizational stakeholders are unwilling or unable to support them at the organizational level; or because information security priorities from organizational stakeholders don't reach or resonate with individual journalists. An important lesson from our findings for those developing computer security technologies for journalists is thus that it is not sufficient to make those solutions easy to use, or even to design them specifically for the journalistic process. Those seeking to develop computer security tools for journalists should include all organizational stakeholders in their design process. We must also understand the motivations and practices of sources, another set of primary stakeholders in the journalistic process, who have thus far not been studied in this context.

Other Journalistic Organizations. By interviewing people at major journalistic organizations that have staff members we could classify as technologists, our interviews could not provide a view of other organizations without even those resources. How can stronger computer security practices be best supported in such organizations? Our sample also included only participants from the U.S. and Europe (though many organizations had reporters working abroad). Western societies often afford journalism leeway that may not be granted in other locations. Therefore, our results may differ if we replicated this study with journalists who live in countries with weaker press and speech protections. However, because of Internet technology and the globalization of the media (e.g., [46]) we expect that some of our findings would translate.

Beyond Journalism. Finally, the journalism community has an existing framework and vocabulary for protecting the privacy of its members. This framework may be useful in other organizational settings, and it is possible

that other communities that maintain privileged relationships with a diverse range of constituents will benefit from further research on journalistic organizations. Lawyers, for example, arguably share many of the same responsibilities and concerns and challenges:

> The lack of universal use of [security technology] and the scariness of it for all kinds of reasons is problematic for journalists as well as others. And it just goes across the board. I mean it's like even emailing with lawyers, you know, who should know better. You know, they just have these little things that say, "This is confidential" and like, are you kidding? I had one experience with a prominent lawyer and he said, "Yeah, I've heard about this PGP stuff, I'd like to use it," but he was working for a big firm and his IT department basically said, "No, we just don't support that." (E6)

Thus, future work should investigate whether and how our findings apply in other domains.

7 Conclusion

A free and open press is a central characteristic of successful democracies and those societies moving toward democracy. Technologies can facilitate a free and open press, or restrain it. We argue that it is critical for the computer security and privacy community to systematically study security and privacy practices, attitudes, needs, and challenges in the journalistic context. We take a substantial step in this paper, focusing holistically on journalistic organizations. Our findings reveal important differences between individual journalists and organizational stakeholders (supervising editors and technologists), as well as broader organizational challenges to computer security and privacy. These challenges—many complicated by unique features of journalistic organizations compared to other types of organizations—have implications for the designs of security- and privacy-enhancing technologies and practices that will succeed in the journalistic context. We see supporting the computer security practices and needs of these organizations as critical to preserving a free press and all the societal benefits that come with it.

Acknowledgements

We thank our shepherd, Lorrie Faith Cranor, as well as our anonymous reviewers, for valuable feedback on an earlier version of this paper. We are also extremely grateful to our interview subjects for their participation. This work is supported in part by the National Science Foundation under Awards CNS-1513575, CNS-1513875, and CNS-1513663.

References

[1] A. T. Garbett, R. Comber, P. Egglestone, M. Glancy, and P. Olivier, "Finding real people: trust and diversity in the interface between professional and citizen journalists," in *32nd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 3015–3024.

[2] U.S. Supreme Court, "Risen v. United States," *SCOTUSblog*, Retrieved: June 5, 2014.

[3] A. E. Marimow, "Justice Department's scrutiny of Fox News reporter James Rosen in leak case draws fire," *The Washington Post*, May 2013. [Online]. Available: http://www.washingtonpost.com/local/justice-departments-scrutiny-of-fox-news-reporter-james-rosen-in-leak-case-draws-fire/2013/05/20/c6289eba-c162-11e2-8bd8-2788030e6b44_story.html

[4] N. Perlroth, "Hackers in China Attacked The Times for Last 4 Months," *The New York Times*, January 2013. [Online]. Available: http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=2&_r=0

[5] N. Perloth, "Washington Post Joins List of News Media Hacked by the Chinese," *The New York Times*, February 2013. [Online]. Available: http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html?_r=0

[6] ——, "Wall Street Journal Announces That It, Too, Was Hacked by the Chinese," *The New York Times*, January 2013. [Online]. Available: http://www.nytimes.com/2013/02/01/technology/wall-street-journal-reports-attack-by-china-hackers.html?ref=technology

[7] Human Rights Watch, "With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy," Jul. 2014, http://www.hrw.org/node/127364.

[8] K. A. Ruane, "Journalists' Privilege: Overview of the Law and Legislation in Recent Congresses," 2011. [Online]. Available: http://www.fas.org/sgp/crs/secrecy/RL34193.pdf

[9] S. Hardy, M. Crete-Nishihata, K. Kleemola, A. Senft, B. Sonne, G. Wiseman, P. Gill, and R. J. Deibert, "Targeted threat index: Characterizing and quantifying politically-motivated targeted malware," in *Proceedings of the 23rd USENIX Security Symposium*, 2014.

[10] W. R. Marczak, J. Scott-Railton, M. Marquis-Boire, and V. Paxson, "When governments hack opponents: A look at actors and technology," in *23rd USENIX Security Symposium*, 2014.

[11] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner, "Investigating the computer security practices and needs of journalists," in *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, 2015.

[12] G. Greenwald, *No Place To Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books, 2014.

[13] C. Savage and L. Kaufman, "Phone Records of Journalists Seized by U.S." *The New York Times*, May 2013. [Online]. Available: http://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html

[14] S. Huntley and M. Marquis-Boire, "Tomorrow's News is Today's Intel: Journalists as Targets and Compromise Vectors," BlackHat Asia, Mar. 2014, https://www.blackhat.com/docs/asia-14/materials/Huntley/BH_Asia_2014_Boire_Huntley.pdf.

[15] Freedom of the Press Foundation, "SecureDrop (formerly known as DeadDrop, originally developed by Aaron Swartz)," 2013. [Online]. Available: https://pressfreedomfoundation.org/securedrop

[16] K. Biscuitwala, W. Bult, T. J. P. Mathias Lecuyer, M. K. B. Ross, A. Chaintreau, C. Haseman, M. S. Lam, and S. E. McGregor, "Secure, Resilient Mobile Reporting," in *Proceedings of ACM SIGCOMM*, 2013.

[17] S. Carlo and A. Kamphuis, "Information Security for Journalists," The Centre for Investigative Journalism, Jul. 2014. [Online]. Available: http://www.tcij.org/resources/handbooks/infosec

[18] S. E. McGregor, "Digital Security and Source Protection for Journalists," Tow Center for Digital Journalism, Jul. 2014. [Online]. Available: http://towcenter.org/blog/digital-security-and-source-protection-for-journalists/

[19] M. Keys, "Google experts reveal how top organizations are in danger," The Blot, 2014, https://www.theblot.com/google-experts-reveal-top-organizations-danger-7717511.

[20] A. Soltani, "12 of the top 25 news sites (incl. @washingtonpost) rely on Microsoft or Google for hosted email services," Twitter, 2014, https://twitter.com/ashk4n/status/448105177439285248.

[21] P. Thornton, "Outlook/Exchange vs. GMAIL," The Journalism Iconoclast, May 2008. [Online]. Available: http://patthorntonfiles.com/blog/2008/05/26/outlookexchange-vs-gmail/

[22] N. Borisov, I. Goldberg, and E. Brewer, "Off-the-record communication, or, why not to use PGP," in *ACM Workshop on Privacy in the Electronic Society*, 2004.

[23] P. R. Zimmermann, *The Official PGP User's Guide*. Cambridge, MA, USA: MIT Press, 1995.

[24] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, 2004.

[25] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith, "SoK: Secure Messaging," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2015.

[26] M. Brennan, K. Metzroth, and R. Stafford, "Building Effective Internet Freedom Tools: Needfinding with the Tibetan Exile Community," in *7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs)*, 2014.

[27] Internews Center for Innovation & Learning, "Digital Security and Journalists: A SnapShot of Awareness and Practices in Pakistan," 2012, https://www.fes.de/themen/menschenrechtspreis/pdf/mrp2012/Internews.pdf.

[28] J. L. Sierra, "Digital and Mobile Security for Mexican Journalists and Bloggers," Freedom House, 2013. [Online]. Available: http://www.freedomhouse.org/report/special-reports/digital-and-mobile-security-mexican-journalists-and-bloggers

[29] S. Gaw, E. W. Felten, and P. Fernandez-Kelly, "Secrecy, flagging, and paranoia: adoption criteria in encrypted email," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2006, pp. 591–600.

[30] G. Norcie, J. Blythe, K. Caine, and L. J. Camp, "Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems," in *Workshop on Usable Security (USEC)*, 2014.

[31] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *Proceedings of the 8th USENIX Security Symposium*, 1999.

[32] N. Diakopoulos, M. De Choudhury, and M. Naaman, "Finding and assessing social media information sources in the context of journalism," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2012, pp. 2451–2460.

[33] N. Taylor, D. M. Frohlich, P. Egglestone, J. Marshall, J. Rogers, A. Blum-Ross, J. Mills, M. Shorter, and P. Olivier, "Utilising insight journalism for community technology design," in *Proceedings of the 32nd ACM Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2995–3004.

[34] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[35] Y.-Y. Choong and M. Theofanos, *What 4,500+ People Can Tell You - Employees' Attitudes Toward Organizational Password Policy Do Matter*, ser. Lecture Notes in Computer Science. Springer International Publishing, 2015, vol. 9190, ch. 27, pp. 299–310.

[36] K. Renaud, M. Volkamer, and A. Renkema-Padmos, "Why Doesn't Jane Protect Her Privacy?" in *Proceedings of the 2014 Privacy Enhancing Technology Symposium*, 2014.

[37] J. Corbin and A. Strauss, *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

[38] V. Venkatesh and H. Bala, "Technology Acceptance Model 3 and a Research Agenda on Interventions," *Decision Sciences*, vol. 39, no. 2, pp. 273–315, 2008.

[39] A. Greenberg, "How the Syrian electronic army hacked us: A detailed timeline," *Forbes*, February 2014. [Online]. Available: http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/

[40] Symantec, "Internet security threat report 2014," 2014. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[41] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness," *Security & Privacy, IEEE*, vol. 12, no. 1, pp. 28–38, 2014.

[42] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse," in *Symposium on Network and Distributed System Security (NDSS)*, 2014.

[43] K. E. Caine, "Supporting privacy by preventing misclosure," in *CHI'09 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2009, pp. 3145–3148.

[44] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny Not to Fall for Phish," *ACM Transactions on Internet Technology*, vol. 10, no. 2, pp. 7:1–7:31, Jun. 2010.

[45] PhishMe, http://phishme.com/.

[46] K. Niknejad, A. Kaphle, A. A. Omran, B. Baykurt, and J. Graham, "The New Global Journalism: Foreign Correspondence in Transition," Tow Center for Digital Journalism, Sep. 2014. [Online]. Available: http://towcenter.org/wp-content/uploads/2014/09/The-New-Global-Journalism-1.pdf

"Security by Obscurity": Journalists' Mental Models of Information Security

Susan E. McGregor and Elizabeth Anne Watkins

Despite wide-ranging threats and tangible risks, journalists have not done much to change their information or communications security practices in recent years. Through in-depth interviews, we provide insight into how journalists conceptualize security risk. By applying a mental models framework, we identify a model of "security by obscurity"—one that persists across participants despite varying levels of investigative experience, information security expertise and job responsibilities. We find that the prevalence of this model is attributable at least in part to poor understandings of technological communication systems, and recommend future research directions in developing educational materials focused on these concepts.

Introduction

Among the first and most shocking of the Snowden revelations of 2013 was the public disclosure of the U.S. government's large-scale collection of communications metadata, including the information of U.S. citizens (Greenwald, 2013). While there was nothing to suggest that journalists were particular targets of this effort, the revelations were nonetheless a shock to the U.S. journalism community in particular, which for decades had operated with the understanding that their communications with sources were effectively protected from government interference by the network of so-called "shield laws" that prevented law enforcement from using the legal system to compel journalists to reveal their sources. That the Snowden documents also implied government infiltration of the systems of companies (such as Google) (Greenwald & MacAskill, 2013) to which many journalistic organizations had recently turned over their own email services, was even more unsettling (Wagstaff, 2014).

Moreover, the Snowden revelations came at a time when the journalism industry was feeling particularly sensitive about the government's collection and use of metadata: only several weeks prior, the U.S. Department of Justice had notified the Associated Press that it had been secretly monitoring both the office and mobile phone lines of several AP journalists as part of a leak investigation (Horowitz, 2013). Though outcry from the industry over this activity eventually resulted in promises from the attorney general that orders for journalists' information would be reviewed more closely (Savage, 2013), these were only good-faith assurances. Should they be contravened, a news organization

could not, as Senior Vice President and General Counsel of Hearst Corporation Eve Burton put it, “march into court and sue the DOJ” (McGregor, 2013, para. 7).

At the same time, the U.S. government’s willingness to treat metadata as legally dispositive was playing a role in multiple high-profile journalistic leak investigations. Though another 18 months remained in the standoff between the Department of Justice and *The New York Times* reporter James Risen over Risen’s refusal to identify the source of classified information included in his 2006 book State of War, District Judge Leonie Brinkema had quashed the subpoena for Risen’s testimony, on the basis that the “numerous telephone records, e-mail messages, computer files and testimony that strongly indicates that Sterling was Risen’s source” (Brinkema, 2011, p.23). In 2015, Jeffrey Sterling was convicted and sentenced under the Espionage Act, though Risen never testified (Maass, 2015). Similarly, just a few weeks before the Snowden revelations *The Washington Post* reported on the DOJ’s use of Fox News reporter James Rosen’s telephone and other metadata to build a case against Stephen Jin-Woo Kim in 2010 (Marimow, 2013).

The security risks to journalists and journalistic organizations in recent years have not been confined to legal mechanisms and leak prosecutions, however. During 2013 alone a host of major news organizations—including *The New York Times*, *The Wall Street Journal*, *Bloomberg*, and *The Washington Post*—revealed that their digital communications systems had been the target of state-sponsored digital attacks (Perlroth, 2013), a pattern that was corroborated by independent security researchers in the spring of 2014 (Marquis-Boire & Huntley, 2014). In at least some cases, the objective of the attacks seemed to be the identification of journalists’ sources. In the case of The New York Times, for example, the timing and pattern of the attack suggested that the motivation was to uncover the identities of sources for a range of embarrassing stories about Chinese government officials (Perlroth, 2013). In other cases, hacking efforts appeared more ad-hoc and retaliatory, as when the Syrian Electronic Army (SEA) defaced the VICE website following a story that allegedly revealed the real identity of SEA member “Th3 Pr0” (Greenberg, 2013), or when the Associated Press’ Twitter account was hacked, leading to false reports of a bomb detonating near the White House (Blake, 2013).

Despite the wide range of threats and tangible consequences of these events (for example, both Sterling and Kim were convicted and sentenced to prison time as a result of their implication as journalistic sources), research shows that in the roughly 30 months since the Snowden revelations, even investigative journalists have not done much to change their practices with respect to information or communications security. For example, a Pew Research Survey of investigative journalists conducted in late 2014 found that fully half of these practitioners did not report using information security tools in their work, and less than 40% reported changing their methods of communicating with sources since the Snowden revelations (Mitchell, Holcomb & Purcell, 2015a). Yet the same research indicates that the majority of investigative journalists believe that the government has collected data about their communications (Mitchell, Holcomb & Purcell, 2015a). And while the Pew survey found that fully 88% of respondents reported

"decreasing resources in newsrooms" as the top challenge facing journalists today, more than half (56%) named legal action against journalists as the second.

On its surface, these results offer an apparent contradiction: roughly the same majority proportion of investigative journalists (62%) had not changed the way they communicate with sources in the 18-months after the Snowden revelations, despite the belief that the government is collecting data about their communications (Mitchell, Holcomb & Purcell, 2015a), and that legal action against journalists is the second-biggest challenge faced in the profession today. And, as noted above, these concerns are well founded given the significant reliance by law enforcement on communications' metadata to prosecute journalistic sources.

Literature Review

Mental Models and Journalists' Security Practices

Discrepancies between belief and practice are hardly unique to journalists, and a range of frameworks is used in the behavioral sciences to both describe and these gaps and design mechanisms for change (Gastin & Gerjo, 1996; Festinger, 1962). Of these, however, only a mental models framework captures both the systemic and technological nature of journalists' information security space.

While there are many definitions of the term mental model across fields (Doyle & Ford, 1998), one useful definition comes from Norman, who characterizes a mental model as a construct that a person or group uses to represent a system and make decisions about it (1983, p. 7). Based on our research and the fact that journalists' security understandings and practices exist at the intersection of multiple technological and human systems of which journalists themselves may have varying levels of understanding (Mitchell, Holcomb & Purcell, 2015a), we find that exploring and characterizing journalists' mental models of information security helps illuminate how and why journalists make the information security choices that they do.

Growing Digital Risk

The majority of both legal and technological security risks to journalists and sources in recent years have centered on digital communications technology. In the United States, the most high-profile of these were leak prosecutions that relied on digital communications metadata (Horowitz, 2013; Brinkema, 2011), and technical attacks by state actors on U.S. news organizations (Perlroth, 2013a; 2013b).

While such incidents are becoming unsettlingly common, however, this does not mean that they constitute an appropriate proxy for the breadth of security risk actually faced by journalists and journalistic organizations, even in a solely U.S. context. While by 2013 the Obama administration had brought a total of seven cases against journalists' source under the Espionage Act (Currier, 2013) more than twice that of all previous administrations combined—this record is not of a particular policy decision or a greater

absolute number of leaks, but also of more general policies and the greater feasibility of tracking disclosures (Shane & Savage, 2012). As one department official put it:

> As a general matter, prosecutions of those who leaked classified information to reporters have been rare, due, in part, to the inherent challenges involved in identifying the person responsible for the illegal disclosure and in compiling the evidence necessary to prove it beyond a reasonable doubt (Liptak, 2012, p.1)

In other words the recent flurry of leak prosecutions is not the result of the administration working harder, but because the process is getting easier, including "a proliferation of e-mail and computer audit trails that increasingly can pinpoint reporters' sources" (Shane and Savage, 2012, para. 3).

Similarly, while sophisticated technical attacks by nation-states like China (Perlroth, 2013a) and North Korea (Grisham, 2015) have been prominently reported, more commonplace attacks have also become more frequent. For example, more generalized phishing attacks (Greenberg, 2014) and exploitation attacks (Mattise, 2014) have also been on the rise.

Thus, while the industry consciousness has been focused on leak prosecutions and technical attacks relating to national-security beats, the reality is that the general security risk for journalists has been growing in recent years across the board. From SEC investigations (Coronel, 2014; Hurtado, 2014) to phishing attacks (Associated Press, 2013; Greenberg, 2014), evidence suggests that while thus far the consequences of national-security related threats have been more severe, the risks faced by journalists are more general across the board.

Despite both the severity and pervasiveness of these attacks, however, research indicates that journalists believe that information security is "as a serious concern mainly for journalists who cover national security, foreign affairs or the federal government" (Mitchell, Holcomb & Purcell, 2015a, 13). Reflecting this attitude, more than 60% of investigative journalists had never participated in any type of information security training (Mitchell, Holcomb & Purcell, 2015a).

Mental Models

Journalists' failure to engage with information security topics and tools can be explained in a number of ways; indeed, failure to adopt information secure tools and practices has been the subject of substantial research within the security community, especially since Alma Whitten and J. D. Tygar's seminal paper on the topic, "Why Johnny can't encrypt" (1999). Like Whitten and Tygar, computer security researchers have tended to focus on either the usability of the security tools available (Renaud, Volkamer & Renkema-Padmos, 2014), or to uncritically label information security failures as user errors (as discussed in Sasse et al., 2001). Even if accurate, however, these explanations do little to explain why journalists may not see information security practices as essential in the first place.

By contrast, understanding journalists' mental models of information security can provide valuable insight into how they interact with security-related systems and processes. Because mental models comprise "what people really have in their heads and guide their use of things" (Norman, 1983, p. 12), they can offer both "explanatory and predictive power" (Rook & Donnell, 1993, p. 1650) for journalists' decisions about systems and situations like digital communications and information security.

A complete mental model is usually comprised of one or more system models along with related knowledge and concepts about how that system behaves in particular domains (Brandt & Uden, 2003). For example, a mental model of using a search engine to locate information on the Internet might be comprised of a system model of how the search engine retrieves and ranks information, along with conceptual models about what types of search terms will yield the preferred results. Taken together, these models would constitute the particular users mental model of Internet searching.

Importantly, however, the system models that help make up a given model are not always complete or accurate; while this may reduce the efficacy of the mental model, it does not necessarily render it completely useless. For example, many of us are able to employ sufficiently useful mental models of searching with Google that we can use it to find the Web information we are looking for; given that their search algorithm is both complex and proprietary, however, we do not have a complete system model of how the search engine actually functions. As such, it is possible for users to have mental models based upon inaccurate or missing system models that are still sufficient for use.

Moreover, experience with a system does not necessarily translate to an accurate system *or* mental model of it. For example, early research on users' mental models of the Internet found that only a small number of the users surveyed—many of whom used it quite extensively and effectively for their desired purposes—possessed a complete and detailed mental model of how the Internet functioned. This led the researchers to conclude that "frequent use of the Internet appears to be more of a necessary than a sufficient condition for detailed and complete mental models of the Internet" (Thatcher & Greyling, 1998, 304). This finding has been echoed in related findings about users' mental models of search engines (Brandt & Uden, 2003), email (Renaud et al., 2014) and credential management (Wastlund, Angulo, & Fischer-Hubner, 2012). In the case of encrypted email in particular, even a computer-science background-which might presumably affect participants' understandings of technical systems-had no apparent impact on the completeness or accuracy of participants' mental models of email communication (Renaud et al., 2014). These smaller experimental results are also supported by broader, more recent findings. For example, a significant percentage of global social network users are unaware that services like Facebook are on the Internet (Mirani, 2015).

Methods

In order to learn more about how journalists' mental models of information security might be influencing their related attitudes and behaviors, we conducted in-depth,

semi-structured interviews with journalists (N = 15) and editors (N = 7) about their security preferences, practices and concerns. Although there is no single methodology for working with or identifying mental models (Stevens & Gentner, 1983; Renaud et al., 2014), we determined that in-depth interviews would offer us the most comprehensive view of "what people really have in their heads and guide their use of things" (Norman, 1983, 12). To help understand how the interplay between journalists' individual work with sources and other professional responsibilities—such as editing for and organizing other reporters—shaped their needs and practices with respect to information security, the interview script varied according to each participant's primary role as a reporter or editor. Thus, while both sets of interview questions focused on security attitudes and behaviors, the "reporter" script focused on questions around individual attitudes and practices while the "editor" script included broader policy questions. We made this distinction based on our understanding of the differing scope of responsibility and awareness between these two roles in journalistic organizations, differences that had some impact on our findings, as discussed below.

Participants

All of the interview subjects were full-time employees at well-respected media organizations, ranging in size and focus from small, U.S.- or issue-focused news outlets to large, international media services with bureaus around the world. While the majority of the participants was located in the United States, some of the participants were located based in Europe (n = 8) and were interviewed in their native language, with the interview responses translated to English during transcription. Ten participants were men and 12 were women.

Ethical Considerations

The entire protocol for this research was conducted under the auspices of the Columbia University IRB, and special care was taken to limit the creation or exposure of any sensitive information during the course of the research process. To this end, participants were often recruited through existing professional networks via person-to-person conversations; as such, the identity of particular interview subjects was often unknown to the researcher prior to the interview itself.

Similarly, we were careful during the interviews to discourage participants from sharing identifying information or sensitive details about particular sources, stories or incidents, in order to limit the risk of compromising any individuals or the efficacy of particular practices.

Participants were also given the option to decline recording of the interview, and to decline to answer any individual questions, though all participants agreed to recording and responded fully. All audio recordings were kept encrypted and labeled only in coded form, both in storage and in transit.

Grounded-theory

Once all interviews were complete, the audio recordings were translated, if necessary, and then transcribed in English, and coded by the researchers using a grounded theory approach (Glaser & Strauss, 1967). The grounded theory method is designed to help identify authentic themes from qualitative interview material through successive iterations of coding and synthesis. By beginning with an initial coding process that relies heavily on the actual language used by participants, a grounded theory method helps minimize the influence of researcher expectation and bias when evaluative qualitative results by drawing topic classifications directly from the participants' interview material, rather than by bucketing responses according to a predetermined rubric. Once a set of themes is identified via the initial coding, these are then synthesized and refined—a process known as "focused coding"—for application across the wider data set.

Participant roles and expertise

In addition to the themes identified through our grounded theory analysis, we also evaluated our results in the context of users' primary role as a reporter or editor, and on our own analysis of their emergent expertise in information security. As we discuss below, however, none of these factors had a significant interaction with participants' mental models of security.

Results

Overall, our results indicate that journalists' mental model of information security can best be characterized as a type of "security by obscurity": the belief one need not take particular security precautions unless one is involved in work that is sensitive enough to attract the attention of government actors. While we are intentionally using this term in a way that deviates from the typical computer-security definition (Anderson, 2001; Mercuri & Neumann, 2003) we do so in part to acknowledge the tangible security benefits that obscure solutions can offer to organizations in terms of slowing down or reducing the severity of an attack. As we discuss below, however, we find that there is little actual "obscurity" available to journalists, making this conceptually attractive characterization of security risk of little practical value.

"Sensitivity" as a proxy for risk exposure

In line with previous findings (Mitchell, Holcomb & Purcell, 2015a), a recurring theme in our work was participants' use of the "sensitivity" of particular stories, subjects, sources, or geography as a proxy for security risk exposure, with more than half of our subjects indicating the need for security precautions was dependent on the presence of one of these features. As one participant put it:

> It depends on the sector, but not everyone has sensitive information. We have many open sources that don't require any particular protection...It's just in certain cases that one really needs to be careful.

This characterization of security risk applied to participants on both sides of the issue, i.e. both journalists on, for example, national-security beats and those on other beats suggested that the need for security was dependent on one's coverage area. As another participant commented:

> If you were on the national security beat [security technology] would be really useful. But I write about domestic social problems, education, crime, poverty.

When asked about the need for specifically information security-related practices, one participant put it even more simply:

> I feel like it depends on how much you think someone is actively spying on you.

Overall, these comments indicate that participants perceived security risk to be primarily related to how sensitive or visible one's subject of reporting may be to powerful actors, rather than the particular vulnerabilities of the collaboration, sharing, recording and transcribing mechanisms through which that reporting is done. Participants who did not consider their coverage areas controversial, then, tended to minimize or dismiss the existence of information security risks to themselves and their sources. Participants who did cover "sensitive" beats, likewise, distinguished their own needs from those of other colleagues who did not do this type of work.

This pattern was pervasive across both reporters and editors, despite the fact that editors knew details of specific security incidents that did not necessarily support a relationship between particular beats and security risk. While both groups adhered to this model of security risk, our research suggests that the two groups rationalized it differently. Many reporters expressed a lack of first-hand experience with security incidents or concerns. As one reporter described it:

> I haven't really dealt with something that was life or death. An extra level of security just didn't seem necessary.

For editors, however, information security was beat-dependent enough that other, more universal newsroom concerns were a higher priority. As one editor said:

> [Information security is] handled kind of on an ad-hoc basis by different reporters and teams depending on the sensitivity of the kind of stories they're working on…it's just not a big enough priority for the kind of journalism we do for it to be anywhere near the top of my tech wish list.

In addition to the above, the researchers also evaluated results for an interaction between information-security expertise, investigative experience, and the use of subject "sensitivity" as a proxy for security risk, but found no effect for these characteristics. In other words, participants described security risk in terms of subject sensitivity regardless of their information-security expertise or investigative experience.

Face-to-face conversation as risk mitigation

In keeping with their view of security risk as contingent on the sensitivity of coverage, our participants reported using a wide variety of security-enhancing tools and techniques in particular situations, some of which will be discussed below. One security strategy referenced by the vast majority of participants, however, was the use of face-to-face conversation as a security strategy. One participant described this in the context of working with a sensitive source:

> If something is sensitive, I say to that person, I'll come and see you.

However, this strategy also extended to communications with colleagues when dealing with sensitive sources or topics. As another participant explained:

> We don't put anonymous sources in the emails, we don't memorialize them in the reporter's notes—it's all done verbally.

This strategy of avoiding the use of technology as a privacy or security measure has been previously categorized as a privacy-enhancing avoidance behavior (Caine, 2009, 3146). In this framework, individuals make behavioral choices explicitly intended to avoid situations where privacy could be compromised or violated.

As in previous research (Mitchell, Holcomb & Purcell, 2015a), the majority of our participants spoke of in-person conversations as a go-to security strategy. This was true irrespective of participants' role, information-security expertise, or experience with investigative journalism. As we will discuss in more detail below, this may at least be in part because this method is guaranteed to be understood by and accessible to all parties. As one editor described it:

> I tried to send an encrypted email to a manager, and she doesn't have [encrypted] email. So, it's available to our company…but it hasn't been a priority for that manager. So I sent a note to her reporter…who was encrypted but was not in the office. So I said, "I'll walk over and have a conversation with you, because I can't send you what I would like to send you. I don't want to put this in writing."

Discussion

Though technically a misappropriation of the computer-science term, we describe journalists' mental models of information security as "security by obscurity" to reflect the two most salient and common features of journalists' thinking about security risk and avoidance in relation to digital communications technology. Specifically, this mental model treats as "secure" any type of journalism that is sufficiently "obscure" to not be of interest to powerful actors, such as nation-states. We also note, however, that while "security by obscurity" is largely dismissed in the computer science community as a false promise (Anderson, Neumann & Mercuri, 2003), it has been argued that in real-world

applications, “obscure” solutions can help delay the onset or mitigate the severity of an actual attack (Stuttard, 2005). Given the large proportion of our participants and those in previous studies whose mental model of security appears to fit with this characterization, we examine the ways in which this mental model both fits and fails journalists’ actual information-security needs.

The appropriateness of “security by obscurity” as a mental model for journalists’ information-security risk lies in its ability to reflect or predict actual information security risk. Accepting this model as accurate would require two things: first, an indication that being “obscure” as a journalist or journalistic organization is possible, and second, that being lower profile in this way offers a measure of security. If this is so, then it may be that “security by obscurity” is a sensible, if imperfect, mental model of journalists’ information-security risk.

If not, however, it is worth looking deeper into the possible reasons why journalists continue to use this mental model, to appreciate what might replace it, and how.

Are journalists “obscure”?

While research confirms that large news organizations are under regular attack (Marquis-Boire & Huntley, 2014), it is difficult to ascertain the extent to which smaller news organizations may face similar threats. That said, there are certain types of attacks known to affect media organizations in general: third-party malvertising attacks. Small and large news organizations alike tend to rely on third-party platforms to serve ads, and the organizations affected when an ad platform is breached often number in the hundreds (Brandom, 2014; Cox, 2015; Whitwam, 2016). Since employees of a news organization are also likely to constitute its “readers,” the potential for exposure to such risks is arguably higher than the average reader.

Are “obscure” journalists more secure?

Given that all of our participants came from well-recognized media organizations, their assessment of security risk tended to relate to individual topics, beats, regions or stories, rather than applying to the media organization as a whole. As noted above, the vast majority of our participants felt that security was a concern primarily for reporters covering national security-related beats, rather than those covering local or social topics. Under this rubric, do non-national security journalists face fewer security risks?

In this case, the evidence is less equivocal: because many high-profile breaches and hacks are actually perpetrated through spearphishing campaigns, in which “targets” receive emails written to look like they came from a friend or colleague, often addressed directly to the target’s name with a personal-sounding salutation. Virtually anyone with an organizational email address is an equally likely “target”; one need not even be a journalist. Such campaigns have been a documented or posited part of several high-profile media breaches, including the Associated Press’ Twitter account hack (Oremus, 2013), and hacks of *VICE* (Greenberg, 2013) and *Forbes* (Greenberg, 2014).

Understanding the "security by obscurity" mental model

Given the mechanisms through which security breaches at journalistic institutions have been enacted—as well as the more general targeting of journalistic institutions in general—"security by obscurity" appears to be a poor fit for journalists' actual level of information security risk. Yet while all of the above-cited evidence was publicly reported (much of it before this study began), this mental model of information security risk still persists across both our study population and that of other researchers. To understand the potential sources of this incongruence, we examined our results for themes that might illuminate why this mental model might persist in the face of such limitations.

Insufficient system models

As we noted above, mental models are typically composed of one or more "system models" along with domain-specific knowledge and concepts (Brandt & Uden, 2003). There is, however, no requirement that a given system model be complete or even accurate in order to serve as part of a useful mental model. Of the 22 participants in this study, only a handful of these demonstrated what could be described as coherent and complete systems models of digital communications (this assessment was reached based on comments made throughout the interview regarding both ownership and operation of various systems, as well as their specific functions).

Otherwise, even participants who expressed an interest in greater information security were aware of the challenge presented by their own limited understanding of the systems with which they were dealing. As one participant put it:

> I've been trying to reduce my Dropbox usage, and so I've been using just a USB stick or something. Which, I actually have no idea how safe that is. It seems more safe.

Another participant described information security risk as equally predictable (and, presumably, comprehensible) as a natural disaster:

> It's one of those things, like worrying about earthquakes or hurricanes … It's the sort of thing where a terrible incident could be catastrophic, and that's something that you worry about. However, there are lots of other fires to put out every day.

Comments like these also illuminate another aspect of our findings: that the most common security measure mentioned by participants was meeting in person. When contrasted with the opacity and uncertainty of technological systems, meeting face-to-face offers clarity and assurance.

This tendency to rely on security strategies that are well understood was underscored by one participant who shared that where salient explanations for security measures were provided, they were well-accepted and understood:

> There's many ways to roll out security tweaks, and doing them where you make a clear and lucid case for what you're doing and why—there was just no pushback whatsoever. Everyone was just like, "Okay, great. We'll do that."

"Good enough" is good enough

Particularly in complex or ill-defined subject areas, such as information security, it is typical for individuals to build mental models around simple explanations that capture the features of a system or situation that are most readily apparent (Feltovich et al, 1996). While these models can be useful insofar as they provide initial support for reasoning about complex situations, they can also hinder more complete understandings (Feltovich et al, 1996). Once established, moreover, a given mental model is rarely amended. Instead, contradictory evidence is either dismissed or interpreted in such a way that is congruent with the existing mental model.

It is possible, then, to appreciate journalists' "security by obscurity" mental model as a way to reason about information security risk that is congruent with the most salient and accessible features of high-profile security incidents. For example, while there have been repeated reports of aggressive leak investigations by the SEC (Coronel, 2014; Hurtado, 2016) most recent leak prosecutions were related to national security reporting (e.g. Jeffrey Sterling and Stephen Jin-Woo Kim). Moreover, such cases are often reported on in great detail. By contrast, only rarely do news organizations share details of technical or spearphishing attacks, making such events far less memorable. For most journalists, then, there is a naturally dominant association between national security and other "sensitive" beats and security risk, despite the greater frequency and, arguably, greater threat, posed by simple phishing campaigns, for example.

Conclusions

By employing a mental models framework to journalists' information security attitudes and behaviors, we identify an approach to information security risk that can best be described as "security by obscurity": the belief that journalists do not need to concern themselves with information security unless they are working on topics of perceived interest to nation-state actors. Although this model is a demonstrably poor fit for the actual security risk faced by our participants (who are all part of well-recognized media organizations), this "security by obscurity" model may persist because it is congruent with the most high-profile security incidents in recent years, and because journalists have poor systems models of digital communications technology.

At the same time, given that one's actual security risk is more likely to be related to one's work as a journalist no matter the capacity, the question remains of how journalists' mental models of information security risk can be updated to reflect their actual threat landscape. Based on our findings, we recommend further study with a focus on developing training modules and educational interventions designed to improve journalists' systems models of digital communications and understanding of threats.

References

Anderson, R. (2001). Why information security is hard: An economic perspective. *Proceedings of the 17th Annual Computer Security Applications Conference*. 358 doi: http://dl.acm.org/citation.cfm?id=872016.872155

Associated Press (2013, April 23). Hackers compromise AP Twitter account. *Associated Press*. Retrieved from http://bigstory.ap.org/article/hackers-compromise-ap-twitter-account

Blake, A. (2013, April 23). AP Twitter account hacked; hacker tweets of 'explosions in the White House'. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/post-politics/wp/2013/ 04/23/ap-twitter-account-hacked-hacker-tweets-of-explosions -in-the-white-house/

Brandom, R. (2014, September 19). Google's doubleclick ad servers exposed millions of computers to malware. *The Verge*. Retrieved from http://www.theverge.com/2014/9/19/6537511/google-ad-network-exposed-millions-of-computers-to-malware

Brandt, D. S., & Uden, L. (2003, July). Insight into the mental models of novice Internet searchers. *Communciations of the ACM* (7). 133-136.

Brinkema, J. L. (2011). U.S. v. Sterling, Fourth Circuit. Retrieved from http://www.documentcloud.org/documents/229733-judge-leonie-brinkemas-ruling-quashing-subpoena.html

Caine, K. E. (2009). Supporting privacy by preventing misclosure. *Extended abstracts of the ACM conference on human factors in computing systems*. (Doctoral Consortium).

Coronel, S. S. (2014, August 13). SEC aggressively investigates media leaks. *Columbia Journalism Review*. Retrieved from http://www.cjr.org/the_kicker/sec_investigation_media_leaks_reuters.php

Cox, J. (2015, October 13). Malvertising hits 'The Daily Mail,' one of the biggest news sites on the Web. *Motherboard*. Retrieved from http://motherboard.vice.com/read/malvertising-hits-the-daily-mail-one-of-the-biggest-news-sites-on-the-web

Currier, C. (2013, July 30). Charting Obama's crackdown on national security leaks. *ProPublica*. Retrieved from https://www.propublica.org/special/sealing-loose-lips-charting-obamas-crackdown-on-national-security-leaks

Doyle. J. K. & Ford, D.N. (1998). Mental models concepts for system dynamics research. *System Dynamics Review*, 14. 3-29.

Feltovich, P. J., Spiro, R.J., Coulson, R.L. & Feltovich, J. (1996). Collaboration within and among minds: Mastering complexity, within and among groups. In T. Koschmann (Ed.) *CSCL: Theory and Practice of an Emerging Paradigm*. (pp. 27-34). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Festinger, L. (1962). Cognitive dissonance. *Scientific American, 207*(4), 93-107. doi: http://dx.doi.org/10.1038/scientificamerican1062-93

Gaston, G. & Gerjo, K. (1996). The theory of planned behavior: A review of its applications to health-related behaviors. *American Journal of Health Promotion, 11*(2), 87-98 doi: http://dx.doi.org/10.4278/0890-1171-11.2.87

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Chicago, IL: Aldine Publishing Company.

Greenberg, A. (2014, February 20). How the Syrian electronic army hacked us: A detailed timeline. *Forbes*. Retrieved from http://www.forbes.com/ sites/andygreenberg/2014/02/20/how-the-syrian-electronic -army-hacked-us-a-detailed-timeline/

Greenberg, A. (2013, November 11). Vice.com hacked by Syrian Electronic Army. *SCMagazine*. Retrieved from http://www.scmagazine.com/vicecom-hacked-by -syrian-electronic-army/ article/320466/

Greenwald, G. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, G. & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/ us-tech-giants-nsa-data

Grisham, L. (2015, January 5). Timeline: North Korea and the Sony Pictures hack. *USA Today*. Retrieved from http://www.usatoday.com/story/news/nationnow/2014/12/18/sony-hack-timeline-interview-north-korea/ 20601645/

Gross, J. B., & Rosson, M. B. (2007). Looking for trouble: Understanding end-user security management. *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology*. doi: 10.1145/1234772.1234786

Holmes, H., & McGregor, S. E. (2015, February 5). Making online chats really 'off the record'. *Tow Center*. Retrieved from http://towcenter.org/ making-online-chats-really-off-the-record/

Horowitz, S. (2013, May 13). Under sweeping subpoenas, Justice Department obtained AP phone records in leak investigation. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/under-sweeping-subpoenas-justice-department-obtained-ap-phone-records-in-leak-investigation/2013/05/13/11d1bb82-bc11-11e2-89c9-3be8095fe767_story.html

Hurtado, P. (2016, February 23). The London whale. *Bloomberg*. Retrieved from http://www.bloombergview.com/quicktake/the-london-whale

Kerr, J. C. (2013, June 19). AP president Pruitt accuses DOJ of rule violations in phone records case; source intimidation. *The Associated Press*. Retrieved from http://www.ap.org/Content/AP-In-The-News/2013/AP-President-Pruitt-accuses-DOJ-of-rule-violations-in-phone-records-case-source-intimidation

Kulwin, N. (2015). Encrypting your email: What is PGP? Why is it important? And how do I use it? *re/code*. Retrieved from: http://recode.net/2015/05/13/ encrypting-your-email-what-is-pgp-why-is-it-important-and -how-do-i-use-it/

Liptak, A. (2012, February 11). A high-tech war on leaks. *The New York Times*. Retrieved from: http://www.nytimes.com/2012/02/12/sunday-review/a-high-tech-war-on-leaks.html

Marimow, A.E. (2013, May 20). Justice Department's scrutiny of Fox News reporter James Rosen in leak case draws fire. *The Washington Post*. Retrieved from https://www.washingtonpost.com/local/justice-departments-scrutiny-of-fox-news-reporter-james-rosen-in-leak-case-draws-fire/2013/05/20/c6289eba-c162-11e2-8bd8-2788030e6b44_story.html

Marquis-Boire, M., & Huntley, S. (2014, March). Tomorrow's news is today's Intel: Journalists as targets and compromise vectors. *Black Hat Asia 2014*. Retrieved from https://www.blackhat.com/docs/asia-14/materials/Huntley/BH_Asia_2014_Boire_Huntley.pdf

Mass, P. (2015, May 11). CIA's Jeffrey Sterling sentenced to 42 months for leaking to New York Times journalist. *The Intercept*. Retrieved from https://theintercept.com/2015/05/11/sterling-sentenced-for-cia-leak-to-nyt/

Mattise, N. (2014, June 22). Syrian electronic army targets Reuters again but ad network provided the leak. *ArsTechnica*. Retrieved from http://arstechnica.com/ security/2014/06/syrian-electronic-army-targets-reuters -again-but-ad-network-provided-the-leak/

McGregor, S. (2013, May 15). AP phone records seizure reveals telecoms risks for journalists. *Columbia Journalism Review*. Retrieved from http://www.cjr.org/cloud_control/ap_phone_records_seizure_revea.php

McGregor, S. T. H., Charters, P. & Roesner, F. (2015). Investigating the security needs and practices of journalists. *Proceedings of the 24th USENIX Security Symposium*.

Mercuri, R. T. & Neumann, P. G. (2003) Security by obscurity. *Communications of the ACM*, 46(1).

Mirani, L. (2015, February 9). Millions of Facebook users have no idea they're using the Internet. *Quartz*. Retrieved from http://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/

Mitchell, A., Holcomb, J., & Purcell, K. (2015a, February). Investigative journalists and digital security: Perceptions of vulnerability and changes in behavior. *Pew Research Center*. Retrieved from http://www.journalism.org/files/2015/02/PJ_InvestigativeJournalists_0205152.pdf

Mitchell, A., Holcomb, J., & Purcell, K. (2015b, February). Journalist training and knowledge about digital security. *Pew Research Center*. Retrieved from http://www.journalism.org/2015/02/05/journalist-training-and-knowledge-about-digital-security/

Norman, D. A. (1983). Some observations on mental models. In A. L. Stevens & D. Gentner (Eds.), *Mental models* (pp. 7-14). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Oremus, W. (2013, April 23). Would you click the link in this email that apparently tricked the AP? *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2013/04/23/ap_twitter_hack_would_you_click_the_link_in_this _phishing_email.html

Perlroth, N. (2013, January 31). Hackers in China attacked The Times for last 4 months. *The New York Times*. Retrieved from http://www.nytimes.com/2013/ 01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

Perlroth, N. (2013, July 12). Washington Post joins list of news media hacked by the Chinese. *The New York Times*. Retrieved from http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html?_r=0

Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). Why doesn't Jane protect her privacy? *Proceedings of the 2014 Privacy Enhancing Technology Symposium*. (Amsterdam, Netherlands).

Rook, F. W., & Donnell, M. L. (1993). Human cognition and the expert system interface: Mental models and inference explanations. *IEEE Transactions on Systems, Man, and Cybernetics (6)*, 1649-1661.

Ruane, K. A. (2011). Journalists' privilege: Overview of the law and legislation in recent Congresses. *Congressional Research Service*.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link': A human/computer interaction approach to usable and effective security. *B T Technology Journal, 19*(3), 122-131.

Savage, C. (2013, July 12). Holder tightens rules on getting reporters' data. *The New York Times*. Retrieved from http://www.nytimes.com/2013/07/13/us/holder-to-tighten-rules-for-obtaining-reporters-data.html

Shane, S. & Savage, C. (2012, June 19). Administration took accidental path to setting record for leak cases. *The New York Times.* Retrieved from http://www.nytimes.com/2012/06/20/us/politics/accidental-path-to-record-leak-cases-under-obama.html?_r=0

Staggers, N., & Norcio, A. F. (1993). Mental models: Concepts for human-computer interaction research. *International Journal of Man-Machine Studies 38*(4) 587-605. doi:10.1006/imms.1993.1028

Stevens, A. L., & Gentner, D. (1983). Introduction. In A. L. Stevens & D. Gentner (Eds.), *Mental models* (pp. 1-6). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Stuttard, D. (2005). Security & obscurity. *Network Security, 2005* (7), 10-12. doi:10.1016/S1353-4858(05)70259-2

Thatcher, A., & Greyling, M. (1998). Mental models of the Internet. *International Journal of Industrial Ergonomics, 22*(4-5), 299-305. doi:10.1016/S0169-8141(97)00081-4

Wagstaff, J. (2014, March 28). Journalists, media under attack from hackers: Google researchers. Reuters. Retrieved from http://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328

Wastlund, E., Angulo, J., & Fischer-Hubner, S. (2012). Evoking comprehensive mental models of anonymous credentials. *iNetSec 2011*, 1-14. doi: 10.1007/978-3-642-27585-2_1

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium*.

Whitwam, R. (2016, January 10) Forbes forced readers to disable ad-blocking, then served them malware ads. *Geek.com*. Retrieved from http://www.geek.com/news/forbes-forced-readers-to-disable-ad-blocking-then-served-them-malware-ads-1644231/

Susan E. McGregor *is assistant director of the Tow Center for Digital Journalism and assistant professor at Columbia Journalism School, where she helps supervise the dual-degree program in Journalism & Computer Science. She teaches primarily in areas of data journalism & information visualization, with a research interests in information security, knowledge management and alternative forms of digital distribution. McGregor was the Senior Programmer on the News Graphics team at the Wall Street Journal Online for four years before joining Columbia Journalism School in 2011. In 2012, McGregor received a Magic Grant from the Brown Institute for Media Innovation for her work on Dispatch, a mobile app for secure source communication. In June of 2014 she published the Tow/Knight report "Digital Security and Source Protection for Journalists," which explores the legal and technical underpinnings of the challenges journalists face in protecting sources while using digital tools to report. In the fall of 2015, the National Science Foundation funded McGregor and collaborators Drs. Kelly Caine and Franzi Roesner to research and develop secure, usable communications tools for journalists and others. She conducts regular trainings with journalists and academics on practical strategies for protecting sources and research subjects.*

Elizabeth Anne Watkins *is a maker, writer, and researcher interested in the future of collaborative, meaningful work in digital ecosystems. Using a mixed-methods approach, she stitches research in knowledge management and organizational behavior together with insights gleaned from innovative community practices in art-making and storytelling. Her written case studies have been published by Harvard Business School, where she also worked with startups at the Harvard Innovation Lab and the Berkman Center for Internet and Society. She studied video art at the University of California at Irvine and received a Master of Science degree in Art, Culture, and Technology at MIT. She's currently pursuing a PhD in Communications at Columbia University in the city of New York, where she's a Research Assistant affiliated with the Tow Center for Digital Journalism contributing to studies in information security.*

Quieting the Commenters: The Spiral of Silence's Persistent Effect on Online News Forums

Hans K. Meyer and Burton Speakman

The Internet may help overcome the Spiral of Silence because posters can remain anonymous. Forum moderators could alleviate some concerns by imposing group norms, such as moderation, to ensure civility. Through a nationwide survey, this study focuses specifically on comments at the end of news stories to examine the impact journalists can have on the conversation. Despite online advantages, the study finds the spiral of silence persists, but journalists who noticeably moderate comments have an effect. The key to overcoming the spiral of silence is helping commenters feel part of a community with other forum participants.

Introduction

Only a small percentage of readers are willing to comment on news stories online (Chung & Nah, 2009; Larsson, 2011), but online comments represent one way a newsroom can fulfill its democratic mission. Online comments at the end of news stories can serve as a "forum for public criticism and compromise," that Kovach and Rosenstiel (2004, p. 6) call one of the essential elements of journalism. They can also help a newroom increase engagement and build audience as legacy media's audience is shrinking.

Newsrooms need to understand why people do not join conversations publically, and the Spiral of Silence may help. People are unwilling to comment publicly because they want to avoid the isolation their minority opinions can cause (Noelle-Neumann, 1993). A bandwagon effect occurs when one side of an issue is more aggressive and causes their opinion to surge in popularity (Noelle-Neumann, 1993). It does not matter if those who are more aggressive actually represent the majority of the population (Noelle-Neumann, 1993). Journalists will play an important role in applying the democractic principles of the Internet in order to decrease their readers' fears.

This study examines what elements a journalist can control to help overcome the spiral of silence and ensure that comments at the end of news stories create the public forum Kovach and Rosenstiel (2004) envisioned. Through a nationwide survey (N = 1,007) of Internet users that specifically asks them whether they comment at the end of news stories, the study measures participants' experience with the spiral of silence within

The Logic of Coercion in Cyberspace

Erica D. Borghard and Shawn W. Lonergan[1]

Cyberspace has definitively emerged as the latest frontier of militarized interactions between nation-states. Governments, as they are wont to do in an anarchic international system, have already invested considerable resources to develop offensive and defensive military capabilities in cyberspace. It remains to be seen, however, how and to what extent these tools can be employed to achieve desired political objectives. Put simply, what is the logic of coercion in cyberspace? Can governments utilize cyber power to deter state adversaries from taking undesirable actions or compel them to bend to their wills and, if so, how and under what conditions? This paper draws on the large corpus of coercion theory to assess the extent to which existing frameworks can shed light on the dynamics of coercion in cyberspace. The paper proceeds as follows. First, we outline the theoretical logic of coercion theory and identify the factors necessary for successful coercion. Each element of coercion is immediately followed by a discussion of how it applies to the cyber domain and an assessment of how the particularities of the domain reflect on the requirements of successful coercion. We demonstrate that, based on current capabilities, cyber power has limited effectiveness as an independent tool of coercion. Second, we explore the extent to which cyber power could be used as part of a warfighting strategy to target an adversary's ability or willingness to resist and suggest which strategies are likely to be more versus less effective. We assert that, based on current capabilities, attrition, denial, and decapitation strategies are most likely to be effective in cyberspace. Finally, we conclude with recommendations for policymaking and further research.

[1] The authors wish to thank the Carnegie Corporation of New York for the grant that made this research possible, the numerous individuals within the United States Government who agreed to share their candid thoughts on coercion in cyberspace, and insightful comments provided by Robert Jervis, Jack Snyder, and Brian Blankenship. The views expressed in this paper are personal and do not reflect the policy or position of the United States Military Academy at West Point, Department of the Army, Department of Defense, or United States Government.

“When are Cyber Attacks State-sponsored and how can we know?”

Justin Key Canfil[1]

How prevalent is state support for "patriotic hackers"? One account is that states outsource computer network attacks (CNA) to non-state confederates in order to retain plausible deniability for their involvement. While empirical difficulties have confounded researchers' ability to test this proposition directly at the open-source level, this paper uses a combination of legal analysis and decision-theoretic techniques to formally map the conditions under which delegation might be reputationally profitable. The model predicts that although CNA delegation can successfully exploit a variety of international legal lacunae, the set of conditions under which covert delegation is expected to yield political cover is narrow in comparison. Ex ante, suspicions should be directed primarily at the smaller universe of states that meet these permissive conditions, since only in these cases is complicity predicted.

[1] This research was made possible by a grant of the Carnegie Corporation of New York.

What it Takes to Develop a Cyber Weapon[1]

Abstract

Today, policymakers offer various warnings about the ease to conduct a successful cyber operation with major consequences. But is it really that easy? The purpose of this article is to elucidate the main obstacles actors have to overcome to develop a cyber weapon. I distinguish between various type of cyber capabilities, and deploy a new dataset, the Cyber Incident Dataset, to identify the main case studies. I argue that the barriers to develop an unsophisticated cyber weapon are indeed low. These weapons have little material and organizational costs. Being mostly based on 'known-how', the costs of these capabilities are likely to fall in future through learning curve effects like standardization, labour efficiency product redesign, and shared experience effects. Hence, it is likely that unsophisticated capabilities – what I refer to as type I, type II and type III cases – will become more widely available to various actors in the future. The obstacles actors have to overcome to develop sophisticated cyber weapons – what I refer to as type IV cases -, however, are disproportionately higher. In order to gather enough information about the adversary's systems – an activity which often takes place outside cyberspace – direct access to a dedicated intelligence network is required to develop these offensive capabilities. The material demands are also much higher for sophisticated cyber weapons. Not least, the mirroring of an Industrial Control System environment – in order to ensure the effectiveness and precision of a cyber weapon – is an obstacle even well-funded actors find difficult to overcome. Also for sophisticated capabilities, intelligence and military organizations have to work closely together while maintaining a high level of secrecy. These type of cyber weapons are also less perceptible to cost reduction effects in the future.

Key Words: Cyberspace, cyber weapons, Cyber Incident Dataset, Sophistication, learning curve effects

[1] Comments or questions can be sent to: Max.Smeets@politics.ox.ac.uk.

The author would like to thank Columbia University SIPA and the Carnegie Corporation for their generous research support. I am also grateful to Robert Morgus for his valuable comments and suggestions to improve the quality of the paper.

Introduction

"I am informed that within 20 minutes the seven of you could make the internet unusable for the entire nation is that correct?"[2] It was the first question Senator Fred Thompson asked grey-hacker group LOpht when they testified in front of US Congress in May 1998. One of the hackers called Mudge corrected the Congressman from Tennessee, "actually any one of us can do it in 30 minutes". The Congressman soon followed up asking, "what if a foreign government would hire seven individuals like you. What harm could they do to the US? [..] What would the effects be?" Without raising their voices the "hacker think tank from Boston Massachusetts", as the group was officially named, sketched out various scenarios: there is the option to bring down the phone system or the electricity net, take down the financial markets, or jam satellite communication. Overall, the group affirmed that it is pretty "easy to cause major havoc."[3]

Today, policymakers offer remarkably similar warnings about the ease to conduct a successful cyber operation with major consequences. In 2009, when a reporter asked Former director of the NSA and National Intelligence Mike McConnell how easy it was to bring down the power grid, he said that a sophisticated hacker can "sack electric power on the U.S. East Coast, maybe the West Coast, and attempt to cause a cascading effect."[4] The most widely cited statement is from Leon Panetta that the U.S. is facing the possibility of a "cyber-Pearl Harbor", as "a destructive cyber terrorist attack could paralyze the nation."[5] Overall, there is a strong sense that cyber weapons empowers weaker actors; the idea is that just a few hackers with a sufficient supply of Club Mate can wage a cyber war.

But is it really that easy? What obstacles do actors have to overcome to develop a cyber weapon? I argue that the barriers to develop an unsophisticated cyber weapon are indeed low. These weapons have little material and organizational costs. Being mostly based on 'known-how', the costs of these capabilities are likely to fall in future through learning curve effects like standardization, labour efficiency product redesign, and shared experience effects. Hence, it is likely that unsophisticated capabilities – what I refer to as type I, type II and type III cases – will become more widely available to various actors in the future. The obstacles actors have to overcome to develop sophisticated cyber weapons – what I refer to as type IV cases -, however, are disproportionately higher. In order to gather enough information about the adversary's systems – an activity which often takes place outside cyberspace – direct access to a dedicated intelligence network is required to develop these offensive capabilities. The material demands are also much higher for sophisticated cyber weapons. Not least, the mirroring of an Industrial Control System environment – in order to ensure the effectiveness and precision of a cyber weapon – is an obstacle even well-funded actors find difficult to overcome. Also for sophisticated capabilities, intelligence and military organizations have to work closely together while maintaining a high level of secrecy. These type of cyber weapons are also less perceptible to cost reduction effects in the future.

This work is conducted in five phases. The first part lays the conceptual groundwork and discusses the meaning of a cyber weapon. The second part identifies in which (known) cyber campaigns a cyber weapon has been used. I develop a new dataset called the Cyber Incident Dataset which offers information on the date, threat actor, target, intent and sophistication of the main cyber incidents since the Morris Worm. In part III I look at the development costs of the identified cyber weapons on a case-by-case basis. The fourth part brings together the case study results, and contrasts the

---

[2]YouTube, "Hackers Testifying at the United States Senate, May 19, 1998 (L0pht Heavy Industries)," retrieved from: https://www.youtube.com/watch?v=VVJldn_MmMY

[3]Ibid

[4]CBS News, "Cyber War: Sabotaging the System," (6 November 2009), Retrieved from: http://www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/

[5]Steven Musil, "Pre-emptive cyberattack defense possible, Panetta warns," *CNET* (11 October 2012), Retrieved from: http://www.cnet.com/news/pre-emptive-cyberattack-defense-possible-panetta-warns/

obstacles actors have to overcome to develop cyber weapons with the nuclear case. This part also addresses potential areas of cost reduction with respect to cyber weapons. The final part concludes, lists avenues for future research, and sheds light on some of the main implications of this research

I Defining Cyber Weapons

Cyber weapons are defined as a capability designed to access a computer system or network to damage or harm living or material entities. As cyber weapons contain both physical and non-physical elements, it makes more sense to talk about cyber weapons as a *capability* rather than a *tool* or instrument. Cyber weapons tend to cause harm or damage through an indirect path.[6] In that respect, it can be said that cyber weapons are more likely to cause *mediated* destruction rather than *immediate* destruction.

Cyber weapons can exploit different types of vulnerabilities. A common distinction made is between between hardware, software and network infrastructure and protocol vulnerabilities.[7] A *hardware*-based cyber weapon alters the physical elements that comprise a computer system and/or network. The key source of hardware-based cyber weapons is derived from the unauthentic or illegal clones of hardware which can be found on the Internet Technology (IT) market.[8] A *software*-based cyber weapon exploits a certain weakness in the code of a computer program.[9] A *network infrastructure and protocol*- based cyber weapon concerns a capacity which exploit vulnerabilities in the set of rules and conventions that governs the communication between network devices.[10]

There are also differences in the route used by a cyber weapon to access a computer system. Many systems are relatively easy to gain access – including most targets known to be connected to the internet. Air-gapped systems are more difficult to access as they are physically isolated from unsecured networks. In this case, the adversary's computer network has to be accessed through the local installation of hardware or software functionality by friendly or ignorant parties in close proximity to the computer system of interest.

Finally, the *payload* of a cyber weapon can vary widely. The *payload* concerns the part of the weapon designed to execute on a computer system or network and achieve some predefined, malicious goal.[11] As Herr and Rosenzweig point out, the payload is the "*raison d'etre"* of a cyber weapon.[12] Payloads can be programmed to do more than one thing when inserted into an adversary computer system or network. Indeed, like a missile, a cyber weapon can deliver multiple payloads. The timing of these actions can also be varied. And, as Lin states, if a communications channel to the attacker is available, payloads can be remotely updated.[13] In fact, in some cases, the initial delivered payload consists of nothing more than a mechanism for scanning the system to determine its technical characteristics and an update mechanism to retrieve from the attacker the best packages to further its attack. What distinguishes a cyber weapon from a more generic cyber capacity is the

---

[6]Thomas Rid, "*Cyber War Will Not Take Place*," (London: C.Hurst & Co.:2013), p. 9

[7]Julian Jang-Jaccard and Surya Nepal, "A Survey of Emerging Threats in Cybersecurity," *Journal of Computer and System Sciences*, 80:5 (2014)973–993

[8]Ramesh Karri, Jeyavijayan Rajendran, Kurt Rosenfeld, Mark Tehranipoor, "Trustworthy hardware: Identifying and classifying hardware Trojans," *Computer*, 43:10(2010)39–46;

[9]Jaziar Radianti and Jose. J. Gonzalez, "Understanding Hidden Information Security Threats: The Vulnerability Black Market," Proceedings of the 40th Hawaii International Conference on System Sciences (2007)

[10]The most frequent network attacks occur by exploiting the limitations of the commonly used network protocols such as Internet Protocol (IP), Transmission Control Protocol (TCP) or Domain Name System (DNS).

[11]Both a narrow and broad conception of 'payload' are used. In broad terms, payload refers to *all* essential data that is being carried by the capability to its (end) target system. A narrow conception, refers to the part of the capability that eventually causes the effect on the targeted system. This paper refers to the latter definition.

[12]Herr and Rosenzweig, "Cyber Weapons and Export Control," p. 8

[13]Lin, "Offensive Cyber Operations and the Use of Force," p. 67

harmful payload used. The two main payloads of cyber weapons concern resource exhaustion and misinformation. The main resource overloading attacks are Denial-of-Service (DoS) and Distributed-Denial-of-Service (DDoS) attacks, consisting of an overwhelming quantity of packets being sent from multiple attack sites to a victim site.[14]

Cyber weapons greatly differ in their sophistication. Any systematic account of the costs of developing these capabilities has to therefore distinguish between the different types. Sophistication refers to the complexity of techniques put into the development of the capability to allow for the opportunity to gain its objective. The most important factors which feed into this are; the type vulnerability exploited, the level of stealth, the degree of tool-kit customization, and the type of system penetrated. An unsophisticated weapon exploits known-vulnerabilities using a generic tool-kit with a minimal implementation of anti-detection techniques against easy-accessible targets. Sophisticated cyber weapons exploit zero-day vulnerabilities (sometimes multiple) implement various obfuscation techniques and implement customized malware or firmware against difficult to access targets.[15]

II Identifying Cyber Weapons: looking for a needle in a haystack

To move from a *definition* of cyber weapons to the *identification* of cyber weapons is a meticulous exercise. The number of general cyber incidents is almost incomprehensibly high. According to Verizon's 2015 Data Breach Investigations Report, more than 317 million new pieces of malicious software were created last year.[16] That means for each baby born in the world, more than two new pieces of malware are developed.[17] In very few of these cases there was a clear intend to cause harm or damage.

In attempt to overcome this problem, I have created a new *Cyber Incident Dataset*. The dataset includes all cases on which a) an incident report was written by a reputable cyber security firm[18]; b) or the incident has been discussed in a cyber security hearing of U.S. Congress. [19] This means that the dataset is not representative of the general population of cases – as this would include many minor instances as well - but aims to identify cases which are worthy of analysis and could potentially be classified as a cyber weapon. The dataset includes information on i) the date of

[14]Alefiya Hussain, John Heidemann, Christos Papadopoulos, "A framework for classifying denial of service attacks," Proceedings of the SIGCOMM 2003 conference on Applications, technologies, architectures, and protocols for computer communications, p. 99-110

[15]The term 'target' has often been used in a confusing manner. What matters is not so much *which* entity you attack, but *what* aspect of the entity you attack. Let us say tomorrow's headline story in the newspaper is: 'hackers conduct a massive cyber attack against the Hoover dam'. There is high chance the news report talks about hackers taking down the website or twitter account of the facility. The story would be more concerning if the attackers accessed the dam's business systems connected to the internet which holds for example all the admin data. Finally, what would certainly gain the attention of the intelligence community is if the attackers access the air-gapped control systems of the dam and were able to tweak the parameters. A cyber attack on the Department of Defense, power station, or Forbes 500 company can mean very different things. The purpose of the attack matters for the degree of complexity and persistence required to successfully execute it.

[16]Verizon, "Data Breach Investigations Report," (2015), retrieved from: http://www.verizonenterprise.com/DBIR/

[17]131.4 million births per year. Ecology, "World Birth and Death Rates," retrieved from: http://www.ecology.com/birth-death-rates/

[18]This includes the following companies: Symantec, McAffee, Kaspersky Lab, BAE systems, Crowdsrike, Fox-IT, SANS institute

[19]This mostly concerns early cases, like the Morris Worm, when the threat intelligence reporting was not yet a well-established industry. A number of controversial cases mentioned in the hearings – the original logic bomb in 1982, the blast of the Baku-Tbilisi-Ceyhan (BTC) pipeline in 2008, and the Israeli spoofing of Syrian air-defense systems in 2007 – were excluded in this analysis because it is likely the damage was caused by means of kinetic reaction rather than alternating computer code.

incident discovery, ii) type of attacker, iii) motivation of attacker, and iv) sophistication of capability. A wide range of sources – including academic literature, media reports, blog posts, and wikileaks reports - were used to ensure the correct coding of the cases. It is not uncommon for a cyber incident to have multiple names. I have tried to stick with the most commonly used one.

Figure 1 summarizes the data. The figure classifies the cases based on 'date of disclosure' (x-as) and 'level of sophistication' (y-as). I use 'date of disclosure' instead of 'date of exploit' because we often do not know when the system was first compromised.[20] The format of the dot/mark representing an incident also discloses i) the type of actor behind the attack, ii) the type of capability used, and iii) number of targets. Finally, all the cases above the x-as in the figure are considered to be Advanced Persistent Threats (APT). APT is an often used term to refer to the most sophisticated type of attacks. According to Kaspersky, "[t]he 'ecosystem' of malware breaks down into known threats (70%), unknown threats (29%) and advanced threats (1%)."[21]

The earliest case included concerns the Morris Worm, launched in 1988. The most recent cyber incidents found in the figure are Cozy Duke and Duqu 2.0, both discovered in 2015. According to the figure, most cyber attacks directed their efforts against multiple entities instead of focusing on one target. Exceptions include the attack on the German steelworks facility (2014), SONY (2014), Stuxnet (2010), Scientology (2009), and My Doom (2004).

The recent spike in the disclosure of APTs cannot go unrecognised. As the figure shows, since 2010, the number of APTs discovered by anti-virus firms has inflated.[22] There are a number of reasons which might explain this trend. The first is that actors seem to get increasingly more organized. Whereas in the 1990s, the activities of script kiddies and hobbyists were often headline news and able to guide scholarly debate on the future of cyber attacks, they do increasingly less so. Also improvements in cyber defense inherently means that attackers have to develop new methods to exploit the target's computer systems. Finally, it should be noticed that is a more intense effort of cyber security firms to discover and report new vulnerabilities. Cyber firms can gain a real reputational boost if they are the first to unveil a new type of cyber platform. This also means that firms have an incentive to exaggerate some of the threats in order to promote their own detection capabilities. [23]

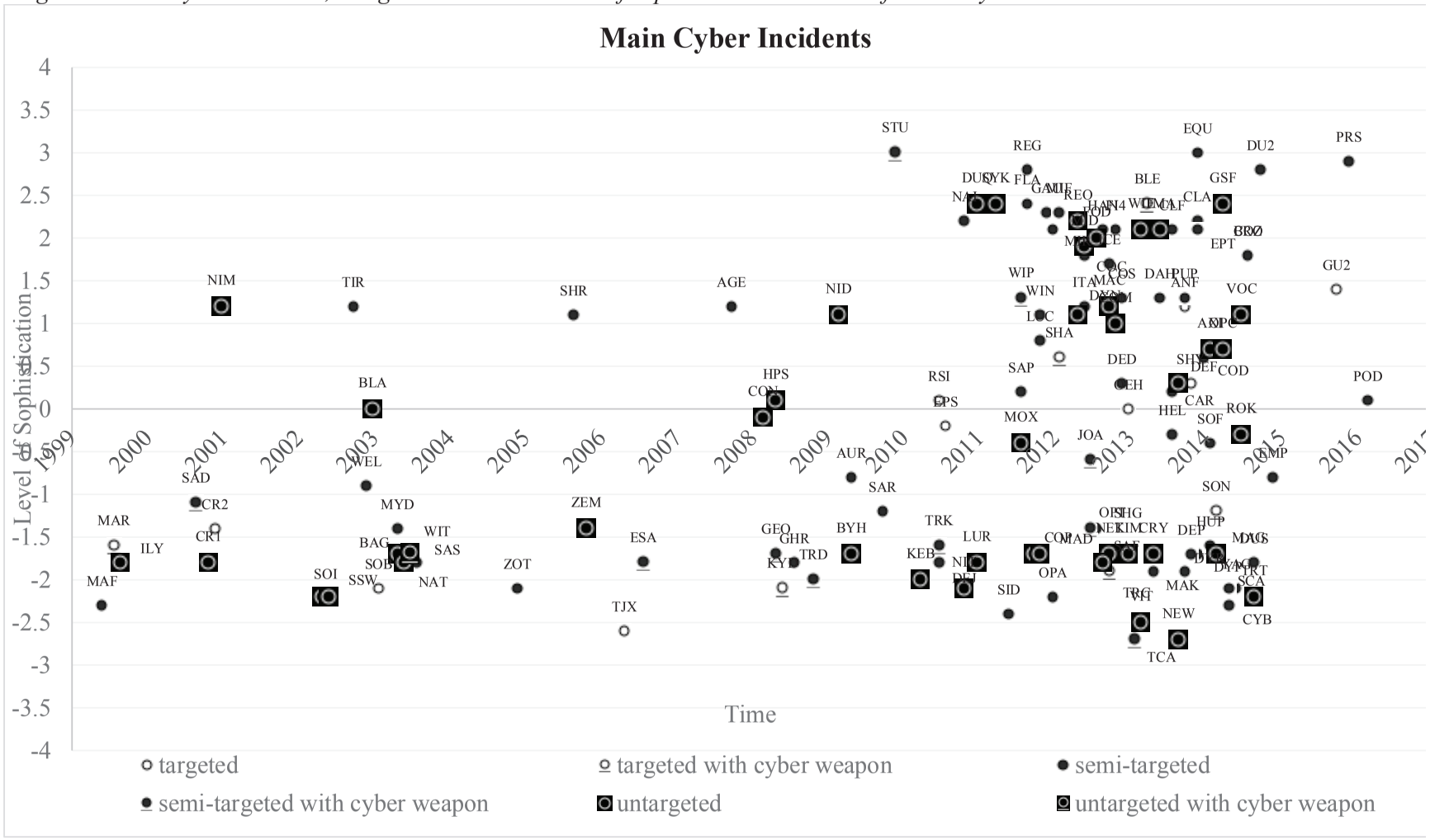
[20] The average time for APT discovery is 3.5 years. One of the more extreme examples is Equation group. The complex cyber attack platform 2014 but first known sample originates from 2002. See Kaspersky Lab, "Equation Group, Questions and Answers," Version 1.5 (February 2015) Retrieved from: https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf, p. 18; The average is calculated using data from: Kaspersky Lab, "Targeted Cyberattacks Logbook." (2016), Retrieved from: https://apt.securelist.com/

[21] The majority of attacks it is relatively easy to defend against with traditional tools. The unknown threats, can be dealt with too if methods are used going beyond stand anti-virus software – such as heuristics and dynamic whitelisting. Yet, it is the 1% of attacks which can remain undetected for multiple years due to their sophistication. See: Kaspersky, "Future Risks: Be prepared: Special Report on Mitigation Strategies for Advanced Threats," (May, 2015), retrieved from: http://media.kaspersky.com/en/business-security/APT-Report.pdf?icid=en-GL:ent-gallery

[22] Technical investigation of the malware has shown numerous linkages– in terms of the way the code is written or type of vulnerability exploited – between the different incidents. For example, most recent: CozyDuke linked to MiniDuke and Cosmic Duke. Duqu 2.0 linked to MiniFlame, Gauss, Flame, Stuxnet, Duqu. Cloud Atlas linked to Red October. Epic Turla linked to Turla.

[23] Also see: Robert M Lee and Thomas Rid, "OMG Cyber!", *The RUSI Journal,* 159:5 (2014)4-12

Figure 1: Main cyber incidents, categorised based on level of sophistication and date of discovery



** Incidents before 2000 not shown to enhance visual presentation. **To download the image for better view: https://drive.google.com/open?id=0B-Uyb2ZTbCInZE9MT1l1SjN1aGc*

III. Case studies of cyber weapons' development costs

Perhaps the most important observation following the figure is that the use of cyber weapons has been rare relative to the use of espionage capabilities.[24] Most of the cases in which a cyber weapon has been used have already been discussed in relation to their disruptive or destructive impact. However, only a few of these cases have been (systematically) evaluated with respect to the resources required to produce them. To facilitate further discussion on this aspect, Table 1 provides an overview of the cyber weapons categorized based on their level of sophistication.

Table 1: Cyber weapon cases based on level of sophistication

Type	**name**	**Characterization**	**Cases**
Type I	DDoS attacks	On the Cheap	Estonia (2007), Hacking Scientology (2008), Kyrgyzstan (2009), Georgia (2009), Black DDos (2010), OPI Israel (2012)
Type II		Lone wolfs	Maroochyshire (2000), Witty Worm (2004)
Type III	Data removals	Moving up the ladder of escalation	Narliam (2008), Dozer (2009), Koredos (2010), Shamoon (2012), Groovemonitor (2012), Jokra/Dark Seoul (2013), Destover/Sony (2014)
Type IV	(Critical) Infrastructure attacks	Crossing the Rubicon	Stuxnet (2012), German Steelworks Facility Attack (2014), Ukraine attacks (2015)

III.I On the cheap

Many of the 'Type I' cases have received widespread attention in the media and also triggered new policy initiatives due to their high visibility. Particularly, the events in Estonia, following the government's decision to move a 6-foot-tall bronze statue commemorating the Soviet defeat of Nazi Germany from the city centre to a cemetery located at the outskirts of Tallinn, have led governments and international organizations to review their ability to respond to threats from cyberspace. Some have even denoted these events as a form of "cyber warfare".[25]

The attacks however are characterized by a low level of sophistication and led to a minimum amount of damage or harm. OPI Israel, intending to "erase Israel from the internet" and claiming to have caused more than $3 billion dollars in damage, in reality was able to only deface one website for several hours.[26] It has proven difficult for Anonymous, an organization eschewing a hierarchical structure, to cause damage to a country's infrastructure following this type of attack. The Georgian attacks – coinciding with the Russian invasion – led to a degradation of certain websites and caused the National Bank of Georgia to stop offering

[24]The dataset suffers from an inherent collection bias in that only *reported* events are listed. We do not know how much we don't know; many exploits currently going on are likely still undiscovered. Yet, notice that this bias only reinforces the statement above as a destructive cyber attack is more likely to be discovered compared to an cyber espionage operation.

[25]See, for example: Jenik Aviram, "Cyberwar in Estonia and the Middle East," *Network Security*, 4 (2009)4-6

[26]Steven Musil, "Anonymous targets Israel in another cyberattack," *CNet*, (7 April 2013), retrieved from: http://www.cnet.com/news/anonymous-targets-israel-in-another-cyberattack/

electronic services for a few days.[27] Yet, the disruption was of short duration – particularly after international support was provided to effectively counter the surge.

What are the costs of mounting these type of attacks? A commercialization of botnet operators has taken place over the last decade. The costs of buying or hiring a botnet mainly depends on the bandwidth of the attack and its duration.[28] In 2007, Vicente Segura and Javier Lahuerta surveyed forums where these services can be bought.[29] It was found that for U.S. $75, one can hire a DDoS Service for 24 hours with a bandwidth of 100 Mbps. A more serious botnet with a bandwidth of 1000Mbps, will cost U.S. $100 to hire for 24 hours. Finally, hiring a DDoS service for a week at a bandwidth of 4570 Mbps costs in the region of U.S. $5500. Since 2007, the price has been falling for these services.[30] Today, you would pay for an hour of 1000 Mbps not more than U.S. $50. [31]

III.II Getting the most bang for buck

The Witty worm and Maroochyshire are considered to be 'type II' cases, characterized by a relatively low level of sophistication but having caused a relatively high level of damage. A number of excellent technical accounts exist on Witty, the worm that was so successful in effecting its target population of computer systems. "Twelve thousand machines was the entire and exposed population," as Bruce Schneier writes, "and the Witty worm infected them all in just 45 minutes."[32] This is an impressive feat, especially considering the short time period in which the worm was written. On March 8th 2004, eEye Digital Security discovered an easily exploitable buffer overflow vulnerability in the BlackICE/RealSecurity Products of Internet Security Systems (ISS).[33] Having been informed about it by eEye, ISS released a patch the day after. On the 18th of March, eEye published a detailed report on the vulnerability. Less than 48 hours after publication, the Witty worm started to spread across the internet.[34]

Nicholas Weaver and Dan Ellis have well-documented the cleverness and the nastiness of the malicious code:

> Witty [...] was an architecturally simple worm [it was less than 700 bytes long]. [...]Although simple, the execution was superb. There were no significant bugs […],

[27]According to one study, the disruption of the Georgian Central Bank and the government communications tactically benefited the Russian military incursion. See U.S. Cyber Consequences Unit (US-CCU), "Overview by the US-CCU of the Cyber Campaign against Georgia in August 2008," *Special Report, US-CCU*, (August 2009), retrieved from: http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

[28]There are also differences in price when you have to buy the complete botnet including command & control as well as zombies, or whether you merely need 'shells' because you have your own Remote Access Trojan Controller.

[29]Vincente Segura and Javier Laheurta, "Modelling the economic incentives of DDoS attacks: femtocell case study," (paper presented at the Workshop on the Economics of Information Security (WEIS), University College London, England, 24-25 June 2009) retrieved from: http://weis09.infosecon.net/files/113/paper113.pdf

[30]Segura and Laheurta, "Modelling the economic incentives of DDoS attacks"

[31]Arbor Networks, "The Risk vs. Cost of Enterprise DDoS Protection How to Calculate the ROI from a DDoS Defense Solution," White Paper (2014), retrieved from: https://enterprise.brighthouse.com/content/dam/bhn/ent/resources/whitepapers/wp-TheRiskvsCostofENTDDoSProtectionWhitePaper.pdf

[32]For full technical account see: Nicholas Weaver and Dan Ellis, "Reflections on Witty: Analyzing the Attacker," *Security*, 29:3 (2004) 34-37

[33]The company ISS was acquired by IBM in 2006.

[34] The possibility that the attacker knew about the vulnerability before the report cannot be discarded.

> avoiding common mistakes. The malicious payload, slowly corrupting the drive, causes immediate damage but does not significantly slow the worm's spread, while randomizing the destination port makes the worm more likely to penetrate firewalls. [Also,] the author seeded the worm [to ensure the worm spreads even faster]. Rather than just starting at a single location, the worm started out on over 110 different victims.[35]

Although we still do not know the author of the worm, several things can be said about the required development costs. The worm, given the way it was constructed, at least required the following three aspects. First, the author was a highly skilled coder. Weaver and Ellis assume it was just *one* coder, but there is no reason we can be certain of this – particularly because of the short release time. Second, as Witty was bug-free, the code was likely tested before. Although theoretically it is possible to write a code without errors in one go, it is more likely that the worm was tested before. The testing does not require a significant capability; one only needs a couple of systems to monitor the network traffic on the test systems. Third, the author(s) must have been well-connected to the hacking environment to seed the attack with 110 computer systems. As Weaver and Ellis write, "[t]he use of previously compromised machines requires that the attacker either obtained access to 110 machines using a different tool, already had access to 110 machines, or took control of these machines from a third party. Thus, Witty's author probably possessed some ties to the [hacker community], to gain access to these machines in the short time frame."[36]

The other 'Type II' case concerns an insider attack.[37] Vitek Boden was an employee at the Hunter Watertech, an Austrialian firm which installs sewage equipment of the Maroochy Shire Council in Queensland. [38] According to a government report, Boden left the company because of a "strained relationship" with his supervisor and applied for a job with the Maroochy Shire Council. [39] The council decided not to hire him. As an act of revenge, Boden issued radio commands to remotely access the sewage equipment on at least 46 occasions between February 9, 2000 and April 23, 2000.[40] He was able to disrupt communication, alter data, disable alarms at four pumping stations and, on one occasion, overflow a pumping station causing 800,000 litres of raw sewage to spill into public areas, including rivers and parks.[41]

Vitek Boden did not need much equipment to cause this much damage. When the police pulled his car over, they found; a laptop with the software used in the sewerage system (re)installed; a two-way radio of the same type used in the Council's system to allow him to

---

[35]Weaver and Ellis, "Reflections on Witty"

[36]Ibid, p.36/37

[37]The event has been well-documented in the Crown criminal case and other public documents.

[38]In 2008 Maroochy Shire was amalgamated with Caloundra City and Noosa Shire to form Sunshine Coast Regional Council. The SCADA controlled system included 142 pumping stations over 1157 sq km installed in 1999. The pumping stations communicate by radio rather than wired network.

[39]Marshall Abrams and Joe Weiss, Malicious Control System Cyber Security Attack Case Study– Maroochy Water Services, Australia, (23 July 2008) retrieved from: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

[40] Ibid

[41]Abrams and Weiss, "Malicious Control System Cyber Security Attack Case Study", p. 5; Congress, "Overview of the Cyber Problem: A Nation Dependent and Dealing with Risk," *Hearing of the Subcommittee on Cybersecurity, Science and Research, and Development*, June 22, 2003, retrieved from: https://www.gpo.gov/fdsys/pkg/CHRG-108hhrg98312/html/CHRG-108hhrg98312.htm

tune into the frequencies of the repeater stations; and a PDS Compact 500 computer control device stolen from Hunter Watertech to spoof the pumping station. [42]

Although the two cases are very different types of capability several similarities can be found. Not least, in both cases it was the work of a skilled individual. In the case of Witty, the attacker(s) developed a well-engineered piece of malicious software requiring many years of experience. In the case of Maroochyshire, as an employee of a contractor that supplied control system technology, Boden had specific knowledge of the systems and equipment used. Also, the resources required in each case are again relatively limited.

III.III Moving up the ladder of escalation

The incident dubbed Wiper came to light in late April 2012 when the New York Times published a story that a mysterious malware attack was shutting down computer systems at businesses throughout Iran. The attack was confirmed by a spokesman from the Iranian Ministry of Petroleum. He was however quick to insist that Wiper caused no permanent damage as a backup of essential and non-essential data was maintained.[43]

The mystery surrounding the attack came from the fact that no one had obtained a sample of the virus to study its code and determine exactly what it did to machines in Iran. The International Telecommunications Union (ITU) asked Kaspersky Lab to investigate the nature of the malware. After several months of research, having obtained mirror images of a number of hard drives that had been hit by the malware, the security firm concluded that: "The malware was so well written that once it was activated, no data survived. So, although we've seen traces of the infection, the malware is still unknown because we have not seen any additional wiping incidents that followed the same pattern as Wiper, and no detections of the malware have appeared in the proactive detection components of our security solutions."[44] The malware contained a carefully designed wiping algorithm to destroy data as effectively as possible. To reduce the chances of discovery, Wiper likely first destroyed the malware components, and only then systematically erased system files causing the systems to crash and unable to reboot.[45] The identity of the attacker remains a matter of speculation, although possible connections have been found with Duqu and Stuxnet, suggesting the U.S. might be behind it. [46]

About a year later, General Keith Alexander, director of the National Security Agency (NSA) and commander of US Cyber Command met up with Sir Iain Robert Lobban, Director of UK's Government Communications Headquarters (GCHQ). [47] The talking points of the meeting prepared by the NSA were leaked by Edward Snowden. The top-secret document states that:

---

[42]Abrams and Weiss, "Malicious Control System Cyber Security Attack Case Study"

[43]Kim Zetter, "Wiper Malware that Hit Iran left Possible Clues of it Origins," Wired, (29 August, 2012), retrieved from: ; also cited in Rid, "Cyber War Will Not Take Place"

[44]Kaspersky Lab's Global Research & Analysis Team, "What was that Wiper thing?," (29 August 2012), retrieved from: https://securelist.com/blog/incidents/34088/what-was-that-wiper-thing-48/

[45]Ibid

[46]As Kaspersky states "[i]nteresting enough, on some systems we noticed that all PNF files in the INF Windows folder were wiped with a higher priority than other files. Once again, this is a connection to Duqu and Stuxnet, which kept their main body in encrypted ".PNF" files." Ibid

[47] NSA, "Iran - Current Topics, Interaction with GCHQ," (12 April, 2013), Retrieved from: https://www.eff.org/files/2015/02/21/20150210-intercept-iran_current_topics_-_interactions_with_gchq.pdf

> Iran continues to conduct distributed denial-of-service (DDOS) attack against numerous U.S. financial institutions […]. NSA expects Iran will continue this series of attacks, which it views as successful, while striving for increased effectiveness by adapting its tactics and techniques to circumvent victim mitigation attempts. [..] Iran's destructive cyber attack against Saudi Aramco in August 2012, during which data was destroyed on tens of thousands of computers, was the first such attack NSA has observed from this adversary. Iran, having been a victim of a similar cyber attack against its own oil industry in April 2012, has demonstrated a clear ability to learn from the capabilities and actions of others.[48]

The last sentence refers to the Wiper attack. The malicious software which struck Saudi Aramco, is known as Shamoon, named after a folder name in one of the strings. Shamoon attacked the hard drives of 30,000 workstations owned by the Saudi oil firm. Like Wiper, Shamoon was designed to destroy data. The payload overwrites the segment of a hard drive responsible for rebooting the system as well as partition table and most files with random data, including a small segment of an image that allegedly shows a burning American flag.[49] Although Shamoon did not cause physical damage to the production facilities of the oil company, the damage was significant. Saudi Aramco reportedly needed weeks – if not months - to recover from the attack, hiring six computer security firms to help with the post-attack clean up and forensic investigation.[50] Later that month a number of reports were published that Qatari RasGas was hit with the same wiper attack. [51]

These cases seem to be part of a broad trend of malware with a destructive functionality. Narilam (2008) and Groovemonitor (2012) are similar pieces of malware that have mostly targeted entities in the Arabian Peninsula. Dozer (2009), Koredos (2010), Jokra (2013), and Destover (2014) have been prominent cases in the Korean Peninsula. What all these cases have in common is that they have not been very sophisticated, yet highly effective. No damage to physical production facilities was caused, yet the operational costs due to wiping of disk drivers was considerable.

Most experts do not believe that the same actor was behind these attacks, but rather that different actors were able to learn from each other.[52] This type of learning generally comes in two forms: learning *how* something is possible and learning *that* something is possible. Let me use a sports analogy to clarify this distinction. First, the most common type of learning, is that of athletes trying to copy techniques of other outstanding sports(wo)men. At a tennis academy a coach might show a series of slow-motion videos of Roger Federer's outstanding single-handed backhand. Players will analyse these videos with as aim to improve their own technique. This first type of learning is the one implicitly referred in all the cyber incident reports. Especially the technical linkages between Shamoon, Destover/Sony, and Jokra/DarkSeoul have received a great deal of attention – which I have summarized in Figure 2. Notice, however, that these case might also (at least partially) embody a second type of learning. On 6 May 1954 Roger Bannister was the first person to ever run a mile under four

---

[48]Ibid

[49]See: Symantec Security Response, "The Shamoon Attacks," Symantec Official Blog (16 August 2012), retrieved from: http://www.symantec.com/connect/blogs/shamoon-attacks

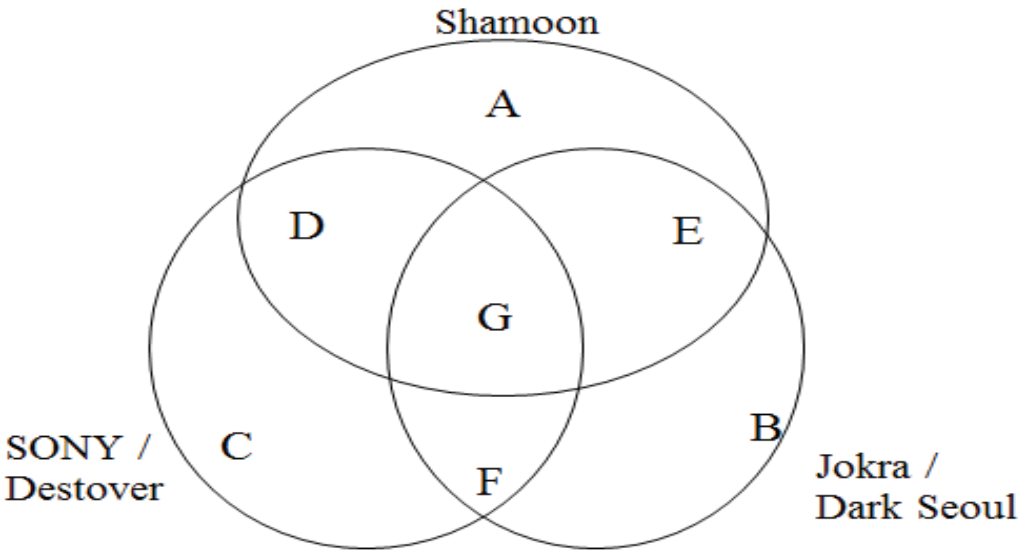
[50]See Rid, *Cyber War Will Not Take Place*

[51]There are a number of reports that the computers at RasGas were affected as well. See: Kim Zetter, "Qatari Gas Company Hit with Virus in Wave of Attacks on Energy Companies," Wired, (30 August 2012) Retrieved from: http://www.wired.com/2012/08/hack-attack-strikes-rasgas/

[52]For a systematic analysis on the diffusion of cyber capabilities see: Ben Buchanan, "The Life Cycles of Cyber Threats," *Survival: Global Politics and Strategy*,1, (2016): 39-58

minutes at Iffley Road track in Oxford with a time of 3 minutes 59.4 seconds (he did so with relatively little training). What is interesting is that once Roger Bannister debunked the widely propagated myth that a four-minute mile was impossible, it changed the mindset of all the other athletes. This psychological dimension, the awareness of an achievable target, meant that it did not take long before many others would run below 4 minutes as well. In fact, Bannister's record lasted just 46 days, after John Landy ran a time of 3:57.9 in Finland.

Figure 2: Connections between Shamoon, Jokra and Destover.



A: Shamoon's main targets were in the Arab Peninsula (like Narilam and Groovemonitor)
B: /
*C: The Destover malware lacked *nix scripts necessary to erase partitions across Linux systems.*
D: For both capabilities, the droppers' resource section contained the wiper drivers
E: For both Shamoon and Jokra vaguely encoded political messages were used to overwrite disk data and the master boot record (MBR)
F: I) Main targets were in South Korea; ii) shared files name; iii) used the same internal web server to display messages on affected computer screens; iv) and used the same colour and messaging schemes
G: I) all were destructive pieces of malware; ii) lacked technical sophistication; iii) did not affect critical infrastructure systems; iv) were politically motivated; v)configured to perform a delayed wipe; vi) used the commercially available RawDisk library from Eldos for disk hardware access; vii) groups claiming credit for intrusion had no prior (hacking) history or real identity.[53]

[53]Symantec, "Are the 2011 and 2013 South Korean Cyberattacks Related?", (29 March 2013), retrieved from: www.symantec.com/connect/blogs/are-2011-and-2013-south-korean-cyberattacks-related; Choe Shang Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," The New York Times, (9 July 2009), retrieved from: www.nytimes.com/2009/07/technology/10cyber.html?_r=0; Symantec, "Four Years of DarkSeoul Backscatters Against South Korea Continue on Anniversary of Korean War," (26 June 2013), retrieved from: www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war; Symantec, "W32.Distrack," (22 August 2012), retrieved from: www.symantec.com/security_response/writeup.jsp?docid=2012-081608-0202-99; Novetta, "Operation Blockbuster: Unraveling the Long Thread of the Sony Attack," 4 December 2014, retrieved from: www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf; Dimitry Tarakanov, "Shamoon The Wiper: Further Details," (11 September 2012), retrieved from https://securelist.com/blog/incidents/57784/shamoon-the-wiper-further-details-part-ii/; Kurt Baumgartner, "Sony/Destover: mystery North Korean actor's destructive and past network activity: Comparisons with Shamoon and DarkSeoul," (4 December 2014), retrieved from: https://securelist.com/blog/research/67985/destover/; Jim Finkle, "Exclusive: FBI warns of 'destructive' malware in wake of Sony attack," Reuters, (2 December 2014), retrieved from: www.reuters.com/article/us-

III.IV Crossing the Rubicon[54]

Former NSA and CIA director Michael Hayden said in 2012 that someone "crossed the Rubicon", referring to Stuxnet, as the worm caused physical damage to Iran's nuclear centrifuges in Natanz. [55] The worm first came to light in June 2010, when Sergey Ulasen, heading an antivirus division of a relatively unknown security firm in Belarus, VirusBlokAda, stumbled upon it when analysing the computer of a customer in Iran. [56] Stuxnet was the brainchild of the United States and Israel.

Ralph Langer indicates that Stuxnet is actually not one weapon, but two.57 The earliest version is also referred to as Stuxnet 0.5., and was in development prior to November 2005.58 This early version is considered to be the most sophisticated of the two, focusing on the closing the isolation valves of the Natanz uranium enrichment facility.59 The latter, better-known version followed a different modus operandi as it aimed to change the speeds of the rotors in the centrifuges.

The later Stuxnet was the old version on steroids.60 As Langer writes, "All of a sudden, Stuxnet became equipped with the latest and greatest MS Windows exploits and stolen digital certificates as the icing on the cake, allowing the malicious software to pose as legitimate driver software and thus not be rejected by newer versions of the Windows operating system".61 This worm took advantage of four zero-day vulnerabilities in its exploitation of both the Windows platform and the Siemens systems – two of those zero-days were used to

---

sony-cybersecurity-malware-idUSKCN0JF3FE20141202; Ryan Sherstobitoff, Itai Liba, and James Walter, "Dissecting Operation Troy: Cyberespionage in South Korea," McAfee, (20 March 2013), retrieved from: www.mcafee.com/it/resources/white-papers/wp-dissecting-operation-troy.pdf

[54]Considering the limited word space, I decided to only focus here on Stuxnet and leave out a discussion on the Ukrainian attacks and the German Steel Mill attacks. On the former, there is however a significant amount of information available about the sophistication and costs of the attacks. See: Kim Zetter, "Everything We Know About Ukraine's Power Plant Hack," Wired, (20 January 2016), Retrieved from: … Kaspersky Lab's Global Research & Analysis Team, "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents," Securelist, (28 January 2016), retrieved from: https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/; Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, (3 March 2016), retrieved from:

[55]CBS News, "Fmr. CIA head calls Stuxnet virus 'good idea," 60 Minutes, (1 March 2012), Retrieved from: http://www.cbsnews.com/news/fmr-cia-head-calls-stuxnet-virus-good-idea/

[56]When the firm posted about it a month later, other security firms soon started to inspect the worm as well – all quick to realize that the code was too sophisticated to be designed by a loosely affiliated group of hackers. Yet, it was Liam Murchu, working for Symantec, who was the first to notice that Stuxnet was much more complex and sophisticated than just a skilled industrial espionage case. See: Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," Wired, (7 November, 2011) retrieved from: http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

[57]Ralph Langer, "Stuxnet's Secret Twin," Foreign Policy, (19 November 2013), retrieved from: http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/; Ralph Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," The Langer Group, (November 2013), retrieved from:http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, p. 5

[58]http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

[59]Langer, "Stuxnet's Secret Twin"

[60]As Langer notes, it also comes at the cost that it became much less stealthy. Ibid

[61]Langer, "To Kill a Centrifuge," p. 11

escalate privilege on the compromised systems.[62] It also used various propagation techniques, via infected removable drives, local area network communications, as well as infected Siemens project files. Within these three propagation mechanisms, Stuxnet utilized at least seven different vulnerability exploitation techniques for spreading to new computers in a system.[63] Furthermore, to avoid suspicion, the driver files were digitally signed with two compromised digital certificates.[64]

What means are required to develop a Stuxnet-like capability, the most sophisticated cyber weapon to date? Costin Raiu, former Director of Kaspersky's Global Research and Analysis Team, estimates that it would costs in the region of $100 million to develop Stuxnet.[65] This seems to be an extremely conservative figure considering the costs of additional intelligence gathering, infiltration, and above all for testing. The complexity of the worm means that thorough testing was required to see whether the bug could do what it was intended to do. The U.S. therefore had to produce its own P-1s, perfect replicas of the variant used by the Iranians at Natanz.[66] At first, small scale tests were conducted borrowing centrifuges stored at the Oak Ridge National Laboratory in Tennessee, once taken from Muammar Qaddafi in late 2003 when he gave up the program. [67] The tests grew in size and sophistication – obtaining parts from various small factories in the world. As Sanger reports, at some point the U.S was "even testing the malware against mock-ups of the next generation of centrifuges the Iranians were expected to deploy, called IR-2s, and successor models, including some the Iranians still are struggling to construct."[68]

Next to the amount of resources poured into Stuxnet, the required institutional infrastructure was at least as significant. The project was likely established under the Bush Jr. administration and continued when President Obama came to office – featuring collaboration with the Israelis. In those years, numerous new institutions were set up – both at the Defence Department and the NSA – to build up the required offensive cyber capacity. Jon Lindsay goes to great length to describe the great deal of planning and support to successfully implement Stuxnet:

> Planners needed expertise in computer science, ICS and nuclear engineering, and covert intelligence operations in order to hack into Natanz.[..] Intelligence preparation for Olympic Games in particular began years before the Stuxnet attack with cyber reconnaissance to map out Natanz's networks. [...]The actual human agents used for insertion may have been affiliated with the Mossad's proxy force in Iran, Mujahedeen-e-Khalq. [..]The operation would further need program managers,

---

[62]It also used a number of known vulnerabilities - for example, the "Conficker" vulnerability was used to propagate through unpatched computers.

[63]Eric Byres, Andrew Ginter, Joel Langill, "How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems," Version 1.0, (22 February 2011), Retrieved from: http://www.abterra.ca/papers/how-stuxnet-spreads.pdf

[64]Falliere et al., "W32.Stuxnet Dossier"

[65]David Gilbert, "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog," International Business Times, 6 February 2014) retrieved from: http://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451

[66]As Lindsay also notes such testing must have involved a fully-functional mockup IR-1 cascade operating with real uranium hexafluoride because both overpressure and rotor speed manipulations have completely different effects if executed on empty centrifuges. (The Libyan P-1 centrifuges are essentially the same as the IR-1)

[67]Sanger, *Confront and Conceal*, p. 197

[68]Ibid, p. 198

operational planners, and commanders to oversee planning, financing, and monitoring of the years-long attack.[69]

Finally, it should be noticed that the attackers prioritized three aspects. First, they went took great care to avoid getting caught (especially with the first attack). Second, they went to great lengths to avoid catastrophic damage. And third, they tried to minimize collateral damage. As General Michael Hayden, former director of the NSA and CIA, observes, the attack was "incredibly precise". […] "Although it was widely propagated, it was designed to trigger only in very carefully defined, discreet circumstances" – not acknowledging the US was behind the attack, but stating that it has been launched by a "responsible nation".70 Inherently, an actor that does not prioritize these issues will be able to do conduct this type of attack at a much lower costs.71

IV Bringing it together: the main hurdles to overcome

Pulling the empirical data strings together from the section above, this section digests the main obstacles for cyber weapon development by way of comparing them to nuclear weapons. Generally, one can identify three obstacles actors have to overcome to develop a certain weapon system. First, weapon development requires *know-how*; the knowledge required to design and acquire the weapon. Second, there are the *material* and *economic* costs. Third, weapon development often requires an *organizational structure* as various actors have to work together to develop a certain capability. Table 3 summarizes the main obstacles for development; I have tried to include only the most important aspects in the hope it would be easier to read (hence, basic things like labour costs are not included in the table).

Table 2: Main obstacles for cyber weapon development

	Unsophisticated Cyber weapon	**Sophisticated Cyber weapon**	**Nuclear weapon**[72]
Knowledge	*Essential* • Only generic info required about target • Intelligence gathering not critical • Targets are interchangeable • One person can have all the knowledge required	*Important* • Very specific information required about target • Intelligence gathering essential • Targets not interchangeable • understanding	*Important* • Only generic info required about target • Intelligence gathering not critical • Targets interchangeable • (initially) needs a large group of the most apt and brilliant

[69]Lindsay, *Stuxnet and the Limits of Cyber Warfare*

[70]According to David Sanger, Obama became increasingly concerned about the potential collateral damage of Stuxnet. See: Sanger, *Confront and Conceal*, p. 204

[71]Langer states the following after his three year long investigation: "Stuxnet was particularly costly because of the attackers' self-imposed constraints. Damage was to be disguised as reliability problems. I estimate that well over 50 percent of Stuxnet's development cost went into efforts to hide the attack, with the bulk of that cost dedicated to the overpressure attack which represents the ultimate in disguise – at the cost of having to build a fully-functional mockup IR-1 centrifuge cascade operating with real uranium hexafluoride." Langer, "To Kill a Centrifuge", p.. 21

[72]Gartzke and Jo only discuss three aspects for nuclear weapons; economic, knowledge and material. Yet, as more recent studies have indicated the organizational component is at least as important. See; Dong-Joon Jo and Erik Gartzke, "Determinants of Nuclear Weapons Proliferation" *Journal of Conflict Resolution,* 51, (2007)167-194

		ICSs/PLCs • Needs a large group of the most apt and brilliant	
Economic and Material	*Unimportant* • food and drinks	*Important* • Labour costs • Intelligence costs • mirroring ICS testing environment	*Essential* • Plants associated with fissile material production • High cost refinement U-235
Organizational	*Unimportant* • No organizational structure required	*Important* • Coordination intelligence and military • High level of secrecy; not just of design but project itself • months-long planning	*Important* • Secrecy of design • Interaction various agencies

** For each capability, I either denote the obstacle as I) 'essential'; the primary aspect to overcome to develop the capability; 'important'; one of the main aspects to overcome to develop the capability; and III) 'unimportant'; the aspect is not required for the development of the capability.*

First, unlike nuclear weapons, the knowledge component is the most essential aspect underlying the development of cyber weapons. Part of that knowledge is explicit and transferable in a formal or systematic manner; for example, being able to code in a certain language. The most significant part of this knowledge, however, is tacit –as Michael Polanyi states "'we can know more than we can tell."[73] It concerns knowledge embedded in a hacker's experience or a cyber command's (implicit) operational processes.[74] The cases studies above reveal that the amount of knowledge required – both explicit and tacit – differs greatly depending on the cyber weapon's level of sophistication. What is perhaps less evident from the case studies, however, concerns the difference in the amount of information required of the target between cyber weapons. Unsophisticated cyber weapons are more generic in their target. The process of usage generally follows the pattern: 'I have this capability; against who/what can I use it?' As a result, it often leads to attacks on relatively easy targets. Highly advanced capabilities tend to follow the reverse process; 'I would like to target this entity, how can I do it?' This makes intelligence gathering activities an essential aspect of sophisticated cyber weapons, whereas for unsophisticated capabilities it matters much less. The difference in intelligence preparation between the two types of cyber weapons can be likened to the difference between someone attacking a stranger on the street with a knife/gun versus a covert attack operation. In the case of the street attack, the offender normally knows (and needs to know) little of the victim's background. He or she can also decide last minute to change target depending on the situation. For the covert operation, however, significant intelligence gathering activities are required to ensure the attack is successful.[75]

[73]Michael Polanyi, *The Tacit Dimension,* (London: Routledge: 1967)

[74]Also see Rid, *Cyber War Will Not Take Place,* p. 83-84; Martin Davies, "Knowledge – Explicit, implicit and tacit: Philosophical aspects," in *International Encyclopedia of Social and Behavioral Sciences*, James D. Wright (ed.) retrieved from: http://www.mkdavies.net/Martin_Davies/Papers_files/KnowledgeExpImpTacit.pdf

[75]Indeed, although there is little public information on the exact way information is gathered for sophisticated cyber operations, it likely follows the typical phases of intelligence gathering, which are: i) selection and discovery, the attackers use publicly available resources to collect details about the target; ii) resource

Second, the material and economic components are of lesser importance for the development of cyber weapons compared to nuclear weapons. Even today, acquiring the necessary materials to fuel a nuclear bomb remains difficult.[76] One reason is that isotope U-235, more commonly denoted as weapons-grade uranium, is a highly unstable form that makes up only 0.7 percent of the concentration of uranium ore that is dug up. Also, the uranium needs to be refined to a concentration of at least 80 percent U-235 to be weapons grade, though upwards of 90 percent is preferable. Although the economic resources required to build a nuclear bomb lowered, they remain significant as well.[77] For cyber weapons the material and economic costs do not even come close to these figures. But for developing sophisticated cyber weapons, it has become clear that a lot of financial and material resources are required as well. Information available about Stuxnet reveals the high costs of establishing an Industrial Control System (ICS) testing environment.

Third, a move along the spectrum of cyber weapons also signifies a shift in the number of people and organization(s) required to develop a cyber weapon. Perhaps the most interesting organizational feature of developing sophisticated cyber weapons is not the amount of institutional capacity required, but its level of secrecy. In the case of the Manhattan Project, the *design* of nuclear weapons was secret during World War II.[78] However, the very fact that the U.S. was developing a nuclear bomb was *not* secret. Notice that in the case of Stuxnet the capability *itself* – the very idea that it was possible to sabotage an industrial control system in the way it did – was kept secret.[79] In fact, this secrecy was a requirement for the cyber weapon to work.

---

extraction and mining, the attackers dig deeper to collect raw data about the target; iii) resource correlation and information; the attackers spend time to correlate data before processing it iv) and attack modeling; the attackers sketch outline of the attack by using processed information from the previous phase. See: Par Aditya Sood and Richard Enbody, Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware, (Elsevier, Waltham, 2014)

[76]Due increased amount of public information on nuclear weapons, the know-how to develop the technology has not been a major problem over the last decades. The Nth country experiment has proven this. The experiment was conducted by the Lawrence Livermore National Laboratory in May 1964. The lab recruited three early-career physicists, with no experience in (nuclear) weapon development, to "design a nuclear explosive which, if built in small numbers, would give a small nation a significant effect on their foreign relations." The physicists, using only publicly available documents, were able to draft up a credible design for a nuclear bomb within three years of appointment. Similar experiments were conducted in later years – taking even less time. Jim W. Frank, "Summary Report of the Nth Country Experiment," Lawrence Radiation Laboratory, (March 1967)

[77]According to Frank Barnaby, "[t]he development and production of even modest nuclear forces used to be a costly enterprise. The British and French nuclear forces, for example, cost well over $10 billion. The development of the nuclear warheads was a major part of this cost." When a nuclear weapons are produced as a 'by-product' of peaceful nuclear programs – like India – the costs are significantly lower. Frank Barnaby, "How States can "go nuclear," *Annals of the American Academy of Political and Social Science*, 430 (1977):29-43

[78]Although Soviet spies were able to gather a great amount of information about the production and design through a number of spies.

[79]The centrifuges to run the large-scale tests were spread out over several national laboratories of the U.S. Energy Department. Also there are reports that Stuxnet had been tested at the Israel's Dimona nuclear facility. See: William J. Broad and David E. Sanger, "Israeli Test on Worm Called Crucial in Nuclear Delay," The New York Times, (15 January 2011), retrieved from: ; Isabel Kershner, "Meir Dagan, Israeli Spymaster, Dies at 71; Disrupted Iran's Nuclear program," The New York Times, (17 March 2016), retrieved from: http://topics.nytimes.com/top/news/international/countriesandterritories/iran/nuclear_program/index.html?inline=nyt-classifier

There is a widely held conception that the cost of cyber weapon development will dramatically fall in the (near) future. This begs the question; to what degree the obstacles outlined above still exist in a few years' time? As cyber weapons have a significant non-material component – particularly less advanced capabilities - the most critical part of cost reduction comes from what economist call 'experience' and 'learning curve' effects.[80] I identify at least four predictable aspects which underlie the cost reduction process of cyber weapons. First, there is cost reduction through *labour efficiency*; attackers become more dexterous in that they spend less time learning, experimenting and making mistakes in writing code. Second, there is also the aspect of *standardization* and *specialization*; certain parts of cyber weapons have become increasingly standardized (such as exploit tool kits), leading to an increase in efficiency. Also, states' cyber commands continue to grow in staff, meaning a higher level of specialization is able to occur for cyber weapons produced by states. Third, there is cost reduction through *product redesign* as attackers have gained experience in producing cyber capacities that are effective for the least money. Last, there are *shared experience effects*; as was noted above, technical malware has shown numerous linkages between various cyber capabilities. Any efficiency learned from one capacity can be applied to other capacities.

The potential for cost reduction should however not be exaggerated – especially not for sophisticated cyber weapons. The defense measures we have seen in recent decades has forced actors to develop more complex capabilities to still be effective. For a government attracting the 'brightest minds' to develop these capabilities does not come cheap – especially when a hacker has the opportunity to work in the private sector as well. Also notice that a cyber weapon program requires a continuous production schedule rather than a terminate production schedule. Due to the malleability of cyberspace, cyber weapons are highly transitory nature; meaning they have short-lived or temporary ability to effectively cause harm or damage to a living or material entity.[81] This means that the commitment to the development of cyber weapons must be unceasing and crucial resources must remain available. The unique decay function of cyber weapons, characterized by 'random crashes' rather than gradual decline, due to the patching of a to-be-exploited vulnerability, means that it is more difficult to estimate the required costs to maintain a capability. [82]

Conclusion

The purpose of this research was to clarify the main obstacles actors have to overcome to develop a cyber weapon. I argued that the costs of developing unsophisticated cyber weapons are low. Both the material and organizational costs for these capabilities are minimal. With 'know-how' being the most essential type of input to develop these type of weapons, the costs of these capabilities are likely to further fall in future through learning curve effects like standardization, labour efficiency, product redesign, and shared experience effects. Hence, it does not require a resourceful formal organization, long-term planning, or highly specialized knowledge to acquire these capabilities.

---

[80]Marvin B. Lieberman, "The Learning Curve, Diffusion, and Competitive Strategy," *Strategic Management Journal*, 8:5 (1987):441-452; Boston Consulting Group, "Perspective on Experience," *Technical Report* (1972)

[81]For a more extensive discussion on this topic see: Max Smeets, "A Matter of Time: On the Transitory Nature of Cyber Weapons," Paper Presented at ISA Annual Convention 2016, Atlanta

[82]Ibid

However, the article addressed that the material and immaterial resources required to acquire sophisticated cyber weapons are disproportionately higher. Direct access to a dedicated intelligence network is required to obtain sufficient information about the target's computer systems. It was also noticed that the mirroring of an Industrial Control System environment is an obstacle even well-funded actors find difficult to overcome. Finally, intelligence and military organizations have to work closely together to develop and use these capabilities while maintaining a high level of secrecy.

What I have described as type I, type II and type III cases all provide a good 'bang for buck ratio' for the attacker. The costs of developing these capabilities are low relative to the havoc some of these capabilities can cause. The ratio between cost and impact seems less favorable for highly sophisticated cyber weapons. Yet, notice that these capabilities can provide something unsophisticated cyber weapons cannot provide. A responsible actor – like the US government – seeks more from a weapon than merely the ability to cause harm or damage. The weapon needs to be discriminate, in that it can be used in accordance with the principles of distinction and proportionality. There also needs to be a high level of certainty that the weapon will be effective. For many unsophisticated cyber weapons these aspects do not hold. There has historically been a mismatch between the intend and the actual harm or damage caused by a cyber capability. When graduate student Robert Morris released one of the first computer worms distributed via the internet in 1988, he never intended to create an overall system downtime – leading computers to slow down to the point of being unusable.[83] The worm's purpose was to measure the size of the Internet but a critical bug in the spreading mechanism transformed it into a highly disruptive attack. Stuxnet is such a special case exactly because it was incredibly precise. The careful development, and the continuous testing and re-testing of the worm meant that there was enough trust it could be reliably deployed. Cyber – as a destructive means – became an 'extra option' for a responsible nation adding a rung on the ladder of escalation. "The intent of the operation was twofold," Sanger writes about Stuxnet. "The first was to cripple, at least for a while, Iran's nuclear progress. The second, equally vital, was to convince the Israelis that there were a smarter, more elegant way to deal with the Iranian nuclear problem that could quickly escalate into another Middle East war, one that would send oil prices soaring and could involve all the volatile players in the region." [84]

Along the way of developing this argument, this paper attempted to introduce useful typologies and new data that might benefit other cyber-related studies as well. I should also point out the severe limitations of this research. In 2006, about sixty years after the first atomic bomb was dropped on Hiroshima, Robert Harney and his colleagues published their study entitled "Anatomy of a Project to Produce a First Nuclear Weapon." The authors outline a detailed timeline of almost 200 tasks required to produce a uranium-based nuclear weapon. This study does not live up to a similar standard. Given the still high level of secrecy surrounding actor's offensive cyber capability development, this study has to settle on providing a more abstract discussion.

---

[83]Bob Page, "A Report of the Internet Worm," (November 7, 1988); Ted Eisenberg, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn, Thomas Santoro, "The Cornell Commission: On Morris and the Worm," *Communications of the ACM,* 32(6): (1989) pp. 706-709

[84]Sanger, *Confront and Conceal*, p. 190

Global Digital Futures Policy Forum 2016: Issues Brief

Panel 3B: Cyber Conflict: Prevention, Stability and Control

By Jason Healey[1] and Tim Maurer[2]

'Removing the Heat from Cyber Competition and Conflict'

Only a few years ago, there were almost no norms globally accepted by governments on cybersecurity or cyber conflict. Even the United States, which had long pushed such norms, had publicly announced very few. The United States and a few other allies confirmed that laws of armed conflict (otherwise known as International Humanitarian Law or the "Geneva Convention") applied to cyberspace.

This has changed with tremendous progress recently, so much so that 2015 could be called was the Year of Global Cyber Norms.

Norms and Cyber Norms

In the academic literature, norms have been famously defined by Peter Katzenstein as "collective expectations for the proper behavior of actors with a given identity."[3] Norms generally can range from the global level to the nucleus of the family and they can be implicit or explicit. For example, laws can but do not always represent a norm. A law to which people adhere can represent "a collective expectation for the proper behavior of actors with a given identity." On the other hand, a law that's in the books but that nobody adheres is not reflective of an actual norm and collective expectation for the proper behavior.

In the international cybersecurity discussion, "norms" have taken on a slightly different meaning. The 2015 report of the UN Group of Governmental Experts states that "Voluntary, non-binding norms of responsible State behavior can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law."[4] Cyber "norms" in this sense could be seen as "potentially a precursor to

---

[1] Jason Healey is Senior Research Scholar at Columbia University's School of International and Public Affairs and Senior Fellow at the Atlantic Council.
[2] Tim Maurer co-leads the Cyber Policy Initiative at the Carnegie Endowment for International Peace and serves as a member of the Research Advisory Network of the Global Commission on Internet Governance.
[3] Peter Katzenstein. *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press: 1996) 5
[4] United Nations, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (22 July 2015) UN Doc A/70/174

eventual customary international law (through practice) that might eventually (after years) be codified."[5]

The narrative about norms for cyberspace (or alternately, ICTs for Information and Communication Technologies) is rooted in politics, as with most norms. The process started with a Russian proposal in the late 1990s for a legally binding cybersecurity treaty.[6] According to Sergey Ivanov, Russia's Minister of Defense from 2001 to 2007, "Russia wants to develop international law regimes for preventing the use of information technologies for purposes incompatible with missions of ensuring international stability and security."[7] However, the Russian government's proposal was met with skepticism not just by the U.S. government. As Ronald Deibert, professor of political science, explains

> Russia has been pushing for arms control in cyberspace, or information-weapons control. Most people dismiss this as disingenuous, and I tend to agree. Most observers see it as Russia's attempt to constrain U.S. superiority in the cyber domain. Russia is more concerned about color revolutions and mobilization on the Internet by dissident and human rights groups – and trying to eliminate the United States' ability to support that type of social mobilization – than it is about protecting the Internet.[8]

These concerns are complemented by skepticism regarding the enforceability and verifiability of a treaty relating to cybersecurity. The United States pushed its own process, leading to five unanimous UNGA resolutions on "Creating a Culture of Cybersecurity, because "challenges to cybersecurity was better answered by a good defense than by constraining offense (technology), providing a juxtaposition to the Russian argument that security could only be accomplished through arms control."[9]

The norms agenda really started to pick up speed when the Obama administration took office with a marked shift toward more international engagement. This shift included greater engagement in discussions about cybersecurity, with the US starting to actively promote the idea of international norms for cybersecurity after it largely ignored the resolution in the UN General Assembly's First Committee for the first decade.[10]

---

[5] Michele Markoff, Department of State, in email conversation with authors, 7 April 2016.
[6] Tim Maurer, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?", Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011
[7] Christopher A. Ford, "The Trouble with Cyber Arms Control," The New Atlantis – A Journal of Technology & Society, Fall 2010, http://www.thenewatlantis.com/publications/the-trouble-with-cyber-arms-control.
[8] Ronald Deibert, "Tracking the emerging arms race in cyberspace," Bulletin of the Atomic Scientists 67.1, January/February 2011, http://thebulletin.org/2011/januaryfebruary/ronald-deibert-tracking-emerging-arms-race-cyberspace.
[9] Michele Markoff, Department of State, in email conversation with authors, 7 April 2016
[10] White House. "U.S. International Strategy for Cyberspace". 16 May 2011;

Over time, the norms agenda evolved, as it was adopted and expanded by other countries and became a concerted effort of the international community. The overarching goal of the diplomatic efforts to date has been to agree to norms guiding behavior in cyberspace. From an academic perspective, these discussions can be broken down into four components: contestation, translation, emergence, and internationalization.[11]

Cyber Norms: Contestation, Translation, and Emergence

Norm contestation: At first, there was disagreement in the international community whether existing international law and norms already apply to cyberspace or if the international community should develop new laws specific to cyberspace. A few countries, China, in particular, contested the idea that existing norms apply and were a proponent and promoter of the latter approach. Conversely, the United States and United Kingdom announced a set of set of norm-like policy goals or "rules of the road" (in the words of then UK Foreign Minister William Hague), as did Dr. Hamadoun Touré, the Secretary General of the International Telecommunications Union.[12]

However, in 2013, the UN Group of Governmental Experts (with representatives from 15 countries including China, Russia and the United States), published a consensus report affirming that "international law and in particular the United Nations Charter, is applicable." This report and the year 2013 can therefore be seen as the end of the norm contestation period, especially regarding the application of international humanitarian law. Though pushback flares up occasionally, the idea of norms in this space has been largely put to rest.

Norm translation: In parallel to these political negotiations, other experts had been investigating how existing norms and laws could be translated to cyberspace. The United States, United Kingdom, Australia and other states had already announced that they believed the laws of armed conflict applied to military cyber operations. However, there was little work describing precisely *how* they applied.

Accordingly, the most important effort of norm translation has been the *Tallinn Manual on the International Law Applicable to Cyber Warfare* developed by a group of international (but all Western) lawyers under the auspices of NATO's Cooperative Cyber Defense Center for Excellence published in 2013.[13] It examines in significant detail how existing international law governing activity above the threshold of use of force and armed attack could apply to

---

U.S. Department of State, International Security Advisory Board. "Report on A Framework for International Cyber Stability". 2 July 2014

[11] This section is based in part on Maurer, Tim. "Cybersecurity and Asia" (September 2015) https://static.newamerica.org/attachments/9847-cybersecurity-and-asia/Cyber-security%20and%20Asia.b7302cdb44324fc38d6c49455429b59e.pdf.

[12] Jason Healey, "Comparing Norms for National Conduct in Cyberspace," Atlantic Council, 20 June 2011, http://www.atlanticcouncil.org/blogs/new-atlanticist/comparing-norms-for-national-conduct-in-cyberspace.

[13] Cooperative Cyber Defense Center of Excellence, "Tallinn Manual," https://ccdcoe.org/tallinn-manual.html.

cyberspace. This area has moved to the center of the cyber-security community's attention. The Tallinn Manual 2.0 expected in 2016 is only one example of an increasing flurry of activity focusing on this issue.

Norm emergence: Just as the year 2013 saw the end of the phase of global discussions on norm contestation, so was 2015 the year of norm emergence and internationalization.

The process started with a speech in May 2015 in Seoul, wherein Secretary of State John Kerry laid out two sets of norms important to the United States; the first set already rooted in international law, the second are proposed norms to create better rules of the road on cyber offense and defense:

> [T]he basic rules of international law apply in cyberspace. Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties.
>
> We also support a set of additional principles that, if observed, can contribute substantially to conflict prevention and stability in time of peace...
>
> First, no country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure.
>
> Second, no country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm.
>
> Third, no country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain.
>
> Fourth, every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way.
>
> And fifth, every country should do what it can to help states that are victimized by a cyberattack.[14]

These norms were treated with a bit of caution by many experts. As expressed by General Michael Hayden, former head of the Central Intelligence Agency and National Security Agency, "We only steal stuff to keep you free and to keep you safe. We do not steal stuff to make you rich. I know of four other countries that can say those last two sentences. Everyone else steals for commercial advantage." This complicates the U.S. government's push that national intelligence agencies should not steal commercial secrets for the benefit of local companies, Kerry's third norm.

---

[14] Secretary John Kerry, "An Open and Secure Internet: We Must Have Both," remarks in South Korea, 18 May 2015, http://www.state.gov/secretary/remarks/2015/05/242553.htm.

Yet it turns out, these norms were in fact the beginning of a new era. With the growing number of bilateral and multilateral agreements, norm internationalization is now also starting to take center stage.[15]

Cyber Norms: 2015, the Year of Internationalization

Just a few months after the Secretary Kerry laid out the U.S. perspective on norms, in July 2015, another UN Group of Governmental Experts, this time comprised of representatives from 20 countries, agreed to a new consensus report including the following cyber norms in addition to several others focusing on supply chain integrity and responsible vulnerability disclosure:

- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- States, in ensuring the secure use of ICTs, should respect … the promotion, protection and enjoyment of human rights on the Internet, as well as … the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;
- A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.
- States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
- States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams … of another State. A State should not use authorized emergency response teams to engage in malicious international activity.[16]

This was a far richer set of norms than most outside experts had expected the UN GGE to be able to agree on; after all, the level of tension between the United States, China and Russia on a range of issues, not just cyber, was already high. The Snowden revelations of US cyber espionage seemed likely to torpedo any significant agreement, yet there was more concordance to come.

---

[15] *See* Tim Maurer, "The new norms." *Jane's Intelligence Review* (March 2016): 52-53

[16] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UNGA A/70/174, 22 July 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

During his September 2015 visit to the United States, President Xi Jinping of China and President Barrack Obama welcomed the UN GGE report and agreed to "establish a high-level joint dialogue mechanism on fighting cybercrime and related issues" as well as important norms:

> The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities.
>
> The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.[17]

A month later, when Xi visited London, he struck a similar agreement on theft of trade secrets with Prime Minister Cameron:

> UK and China agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage.[18]

According to press, when Premier Angela Merkel of Germany was in Beijing, she was able to secure the same promise, so that "China and Germany agreed to work on stopping economic cyber spying between the two nations," however, unlike the US and UK agreements, this has yet to appear in a formal, concluding statement by the leaders.[19] Even so, there was still more norm internationalization to come.

At the Ankara Summit, in November 2015, the leaders of the G20 nations – including from true cyber powers such as Russia, China and the United States but also from Brazil, India and Indonesia – gave their approval to this latest UN GGE report and called out several specific norms:

> We affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.
>
> All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications.

---

[17] The White House, "FACT SHEET: President Xi Jinping's State Visit to the United States," 25 September 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
[18] UK Government, "UK-China Joint Statement 2015," 22 October 2015, https://www.gov.uk/government/news/uk-china-joint-statement-2015.
[19] Stefan Nicola, "China Working to Halt Commercial Cyberwar in Deal With Germany," Bloomberg Technology, 29 October 2015, http://www.bloomberg.com/news/articles/2015-10-29/china-working-to-halt-commercial-cyberwar-in-deal-with-germany.

> We also … affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs.[20]

Secretary Kerry's speech in Seoul has just been in May 2015 and by November of that same year, just six months later, norms went from proposal to agreement at the top levels of global governance.

Private-Sector Norms

In addition to states proposing international cybersecurity norms, non-state actors have also been actively participating in this discussion. In one sense, the Internet was built on norm-like international behavior, from technologists building the network based on "rough consensus" to cooperating across boundaries to limit disruptions to the network. In late 2014, Microsoft took these norms one step further, launching a report proposing six specific norms overlapping with certain norms proposed by states:

1. States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.
2. States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
3. States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.
4. States should commit to nonproliferation activities related to cyber weapons.
5. States should limit their engagement in cyber offensive operations to avoid creating a mass event.
6. States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.[21]

Complementing its substantive proposals, Microsoft also issued a procedural recommendation proposing a G20 + ICT20, the G20 member states meeting with twenty leading ICT providers, to develop an "agreed-upon norms document" which would "allow the 20 most developed economies to hold themselves and others accountable to the agreed-upon behaviors in cyberspace."

---

[20] G20, "G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015," http://www.consilium.europa.eu/en/meetings/international-summit/2015/11/G20-Antalya-Leaders-Summit-Communique-_pdf/.

[21] Angela McKay, Jan Neutze, Paul Nicholas, and Kevin Sullivan, "International Cybersecurity Norms," Microsoft, December 2014, http://aka.ms/cybernorms.

Why Was 2015 the Year of Cyber Norms?

While these norms include certain caveats, for example, what is considered "unlawful" will depend on each country's domestic laws, it appears the remarks by Secretary Kerry lit a spark which took norms from an area of contention toward much greater international appeal, including G20 backing and statements by heads of state. The two most repeated norms include one of the least controversial (that "the basic rules of international law apply in cyberspace" which had been previously agreed to in the 2013 UN GGE report) up to certainly the most controversial (that "no country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain").

There are at least six likely, overlapping reasons why 2015 was a year when so much progress was made on articulating cyber norms.

Rising cyber tensions. Certainly within the United States, but assumedly in other nations as well, government officials and experts were seeking means to counter the rising frequency and violence of cyber attacks. From cyber espionage, to disruptive attacks like Stuxnet or against Sony, each nation seems to feel strategic vulnerability to others in cyberspace. Norms, in part, gained appeal because key states saw stability as being in their national security interest.

Leadership's personal attention. Within the United States, this concern was driven by the personal attention of President Barrack Obama who raised the issue with President Xi Jinping in the Sunnylands summit, mentioning the "deep concerns we have as a government around theft of intellectual property."[22] In China, President Xi named himself chair of an Internet security working group.[23]

Diplomacy and summit politics. Diplomats sometimes need a win for national (or even personal reasons) and may be willing to make tradeoffs they'd otherwise refuse. Likewise, leaders want to have successful summits. China came ready to the United States and the United Kingdom to make deals and ensure the summits would be a success. According to discussion with participants in the earlier 2013 UN GGE report, similar to President Xi having his first summit with President Obama at Sunnylands, the Chinese delegation was willing to compromise at the 2015 UN GGE.

Universality. When the governments selected norms at least some of them were meant to be relatively easy for most states to agree to, as it would be in their long-term interest. Therefore, key criteria were universal appeal and utility to be good for all states' national security.

---

[22] The White House, "Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting," 8 June 2013, https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-.

[23] Shannon Tiezzi, "Xi Jinping Leads China's New Internet Security Group," The Diplomat, 28 February 2014, http://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/

Hard diplomacy. Diplomats, especially but not only from the US State Department, put in long hours negotiating and dealing with their counterparts to make progress over the course of 2015. Key international conferences, such as the Global Conference on Cyberspace in The Hague in April 2015, kept this momentum thanks to hard work by the Dutch government.

Low cost to commit to norms. It is also possible nations were willing to commit to norms because there give modest gain at relatively low cost. After all, if attribution continues to afford plausible deniability, then it could be hard for other states to prove that a nation is violating the norms. Many pessimistic experts felt there is little-to-no chance countries would forego cyber espionage. Likewise, other experts doubt states will live to up to the norm that "States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products."

Looking Forward

This last possible reason - a perceived low cost for committing to norms - points to the key factor in whether these new international norms will be effective.

The new, most pressing question will be whether and how states will implement and internalize the norms to which they agreed. According to the lead US diplomat negotiating these norms,

> most states are not in a position to accept new binding concepts in cyberspace. This allows them to initially sign on with no real penalty - that is, until the international community makes it common practice. Then deviations in behavior may be punished by the international community whether the norms are codified or not.[24]

Since the Obama-Xi agreement to limit stealing intellectual property for commercial gain, there has been intense debate within the US cyber community on whether China is living to the letter (or even the spirit) of the norm. But even if it leads to a reduction, but not an elimination, of such cyber espionage, it should still be considered a success. After all, diplomacy isn't binary. It's analog and if the norm leads to "less but not zero" – it is still a win for the United States and other nations facing such thefts.

If norms are in fact "collective expectations for the proper behavior of actors" then actors that fail to live up to those expectations will suffer at least reputational costs, especially if heads of state personally and publicly committed to them. In fact, this can be a central goal of diplomacy, to unveil the hypocrisy of other actors. So if a givens norm is not enacted national leaders who received a face-to-face agreement from President Xi will be in a much stronger position to respond to Beijing over its commercial espionage. The same holds true for other nations who may feel their critical infrastructure has been targeted or attacked by the Russian or

---

[24] Michele Markoff, Department of State, in email conversation with authors, 7 April 2016.

the US military or intelligence community, despite the explicit commitments by those governments.

Even though the progress on cyber norms over 2015 was sudden, that success had in fact been built on the years of hard work by diplomats, cyber experts, and many others. It is now time for more hard work, to help nations live up to these norms to ensure a more peaceful cyberspace in future.

Section 2:
Global Internet Governance

The Brazilian Multistakeholderism on Internet Governance[1]

Fernanda R. Rosa

Working paper – October, 03 2016

Columbia University's School of International and Public Affairs

Abstract

This work analyzes the Brazilian Internet Steering Committee's (CGI.br), a pioneering experience of multistakeholderism in the field of Internet governance, since 1995. It describes the CGI.br's development that culminates in a self-sustainable financial model, the establishment of an election process to choose the civil society representatives, and the emergence of different kinds of multistakeholderisms within the organization. This work shows how the government has had a central role in the construction of the current CGI.br, sponsoring multistakeholder efforts since its conception, elaborating its decree and assenting to be subject to a homogeneous hierarchy among other stakeholders. It analyzes some of the controversies that emerge from the institutional design of CGI.br, its legal sponsorship and the openness to more participation, revealing the challenges of its current procedural rules. Considering the CGI.br a successful case in multistakeholderism and also in policy, this work proposes improvements, in terms of rules and design, to leverage their consistence and the diversity of interests within the organization. This work is informed by a 2-month fieldwork research conducted through participatory observations and in-depth interviews at the executive office of CGI.br and at events supported by it. Based on that, suggestions for future research are proposed.

Keywords: national Internet governance, multistakeholderism, participation, representation, electoral colleges, Brazil.

1. Introduction

The purpose of this study is to analyze the Brazilian Internet Steering Committee's (CGI.br)[i] trajectory, an experience of multistakeholderism in the field of Internet governance at a national level. Considering that the inconsistencies in the country's political life have generated the inclination to constant policy and institutional changes as well as discontinuity (Frey, 2000), the fact that CGI.br is a 21-year-old institution makes it a prominent policy case study[ii].

While CGI.br is framed here as part of the policy realm, the present work problematizes this categorization through an examination of the organization institutional design and the CGI.br

[1] This research was possible thanks to the Columbia University's School of International and Public Affairs and Carnegie Research Support.

multistakeholderisms, which can be defined as both representative, and emergently participatory.

This work critically reflects on the literature on multistakeholderism and issues that emerged in a 2-month field work research project[iii] where the researcher, guided by a qualitative and ethnographic approach, conducted participatory observations and in-depth interviews (Lofland, Snow, Anderson, & Lofland, 2006; Duneier, 2011, Maxwell, 2013) at the Brazilian Center for Information and Coordination of dot-BR (NIC.br)[iv]. NIC.br is subordinated to CGI.br, and it hosts its monthly meetings. During the field work, participatory observations were also conducted at events such as the Brazilian Internet Governance Forum (the Brazilian IGF), in Porto Alegre; the School of Internet Governance in Brazil (EGI)[v], organized by NIC.br in São Paulo, and the Expotec, a technology exhibition partially supported by NIC.br, with debates and seminars that took place in João Pessoa.

This article, first, presents a brief history of the conception of CGI.br, focusing on its development trajectory, the different multistakeholder efforts used to build the institution, and the role of government in the process. Then, it describes the types of multistakeholderisms identified within CGI.br and the procedural rules that define its current operation. Finally, it discusses the challenges that have emerged from the design and the rules of the institution, problematizing some of the research findings, pointing out areas for future study, and proposing alternatives for improving the mechanisms of social participation.

By raising some yet unexplored issues in the debate, this paper aims to contribute to join efforts to better understand the multistakeholderism dynamics, and to leverage more inclusive, transparent and democratic models of Internet governance.

2. The multistakeholderism debate

While the Internet has been running for years, with a growing number of both actors involved in its governance, and new users, it was not before 2005 that a definition of the term Internet governance emerged. As a result of the first phase of the World Summit on Information Society (WSIS) in 2003, the Working Group on Internet Governance (WGIG), composed by representatives of government, private sector and civil society, defined that *"Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."* (WIS/WGIG, 2005, p. 4).

While the WGIG sought to build a "… *descriptive*, *concise* and *process-oriented"* definition (WIS/WGIG, 2005, p. 3), normative analyses of it are recurrent, emphasizing meanings related to inclusion, participation, transparency, openness and bottom-up policy development meanings (Kleinwächter, 2011), to name a few.

First, this expresses how political and social discourses are embedded in the Internet governance debates, even when such discussions are said to be guided by one of the WSIS principles, specifically concerned with the network technical aspects, or "the stable and secure functioning of the Internet" (WIS/WGIG, 2005, p. 4). It reveals the impossibility of dissociating properties of the same phenomenon, in a clear example of how what is considered technical is inherently political (Latour, 1994; DeNardis, 2014).

Second, the definition stated the necessity of collaboration between three sectors, namely, government, private sector and civil society, laying an implicit conception of a generic multistakeholder model into the Internet governance characterization. With such a broader concept, previous and future experiences, even if not based in principles stated by the WSIS documents, were able to be accommodated. The historical circumstances that the group was expected to answer (Raymond & DeNardis, 2015) are also important to understand the definitions that evolved by that time. The search for equal footing among nations, the reduction of the United States prominence, and the participation of non-governmental parties in the arena where Internet governance issues were discussed, were then at the center of the debate (Mueller, 2010).

Third, the conditions and the participants who were involved in that debate within WGIG also contribute to understand the dilemmas behind the scenes. While some scholars consider that the WGIG had a good balance and diversity in terms of its 40 participants (Mueller, 2010; Epstein, 2013), Raymond and DeNardis (2015) take a critical approach. They emphasize, on the one hand, the considerable number of government officials and countries that are recognizably adept of repressive Internet policies, among the participants, and on the other hand, the absence of the United States in the group. For these authors, *"the formulation of an international definition of multistakeholderism was arguably not a multistakeholder effort"* (Raymond & DeNardis, 2015, p. 587). Such divergences show the importance of the expanding multistakeholderism scholarship to deepen our understanding on the kinds of self-nominated multistakeholder models in practice.

Through the empirical analysis of the dynamics of the IGF, Epstein (2012) found out that there is a "multiplicity of practices of multistakeholderism" within the forum (p. 208). In studying multistakeholder arrangements, he shows that not only the types of forum activities matter, but also the actors who participate.

Raymond and DeNardis (2015) define two types of multistakeholder models with focus on procedural rules and the type of authority among actors: the heterogeneous polyarchy, "in which distinct actors (or classes of actors) possess different formal powers (such as the division of authority between branches of government)" (p. 580) and the homogeneous polyarchy, "where actors have similar formal powers (such as individual voters in a democracy where each citizen receives an equal vote)" (idem).

The authors are emphatic in stating the authority of rules to establish the common governance in a multistakeholder institution. These rules can verse about the types of actors who will participate, the terms of participation, etc., and ensure the consistency of an organization (Raymond & DeNardis, 2015, pp. 580-581). In this regard, it is important to recognize the procedures for membership of an organization, and the guiding logics behind it, such as if they are based on hierarchical processes of representativeness or a liberal model of participation (Epstein, 2013).

Beyond the procedural aspects, the plurality of stakeholders' interests needs to be considered. Previous works have emphasized that traditional sectorial divisions - such as government, civil society, private sector -, although useful to contrast approaches and worldviews in some situations, do not imply a total alignment within these groups (Mueller, 2010; Belli, 2015). Instead, "political views held within each of these categories are extremely diverse." (Mueller, 2010, p. 265). Hence, Belli (2015) proposes a step forward, suggesting that the nature of a

multistakeholder approach should consider not only the kind of institutions that the stakeholders represent, but the interests that they in fact defend.

Based on the elements discussed above, the Brazilian Internet Steering Committee (CGI.br) figures as a substantive case to be analyzed.

3. The conception of CGI.br

3.1. First phase: a fully government-sponsored multistakeholder organization

The history of the Brazilian Internet Steering Committee (CGI.br) can be told, at least in part, by a list of federal executive ordinances and a decree. In May 1995, a joint-ministerial ordinance of the Ministry of Communication and the Ministry of Science and Technology created the organization, defining its attributions, criteria for participation and the length of mandate. At that time, the committee's composition was defined as including five representatives from government, and four from civil society, including one from the "academic community", one from "service providers", one from the "business community" and one from the "community of Internet service users". The committee members were nominated for a period of two years, through a new joint-ministerial ordinance in July of the same year. Some of the attributions of the organization, at that time were:

> "monitor the provision of Internet services in the country; establish recommendations concerning: implementation strategy and interconnection networks, analysis and selection of technology options, and functional roles of companies, educational institutions, research and development (…);" "recommend standards, technical and operational procedures and the use of code of ethics for all Internet services in Brazil; coordinate the assignment of IP (Internet Protocol) and the registration of domain names; recommend network management operational procedures; collect, organize and disseminate information on the Internet service in Brazil" (Brazil, 1995a)[vi].

In 1995, the telecommunication services were a state-owned monopoly, under Telebrás, a company founded in the 1970s, during the military dictatorship. In order to create different business models to the Internet development, another ministerial ordinance, known as Norm # 4, was released by the Ministry of Communications at the same day that CGI.br was conceived. It defined that the Internet is not a telecommunication service, but rather a "value added service", which supplements a telecommunication network to create new uses and activities (Brazil, 1995b). In this scenario, the government authority on the Internet would not come from its direct market exploration, as it used to occur with telecommunication services until then.[vii] In regard to the network technical aspects, with its initial focus on the registration of domain names, it was put formally the CGI.br's responsibility.

The assignment of the country code top-level domain (ccTLD) .br to Brazil was done back in 1989, directly from Jon Postel to Demi Getchko (Adachi, 2011). The latter is known for his important role in the first TCP/IP Brazilian connection while working at the São Paulo Research

Foundation (FAPESP) – a well-known academic state foundation that used to be the main authority of names and numbers in Brazil before the creation of CGI.br, evidencing part of the academic root of the Internet in Brazil[viii].

Under an unusual design for a research foundation, FAPESP continued to be responsible for names and numbers, but then under the auspicious of CGI.br. Hartmut Glaser was the Special Advisor to the FAPESP's Chairman and became responsible for leading the project that would respond to the brand-new CGI.br for 10 years more, with some substantial changes from the beginning. After 1998, CGI.br defined that the registration of domain names, until then conducted free of charge, should be charged according to "values compatible with existing internationally" (CGI.br, 1998).[ix]

At that moment, the government was no longer the financial supporter of the CGI.br activities, although it continued to be, in a federal level, its legal sponsor, through the joint-ministerial ordinances that conceived and structured it, and its political-sponsor, through the nominations and selection of the CGI.br participants. In a State level, the government continued to be its executive arm through FAPESP.

The fact that FAPESP was a research foundation brought questions about how much the nature of the CGI.br project fit the mission of the institution, since this was not a typical research and development project (CARVALHO, 2006). It was not before the new presidential term, in 2003, that the idea of making a transition from FAPESP to another organization was fully developed. In parallel to that, there were also critiques from civil society about the limited social participation in the CGI.br, and proposals to change it (RNP, 2003).

3.2. Second and current phase: the transition to a more participative multistakeholder model

The political change in the federal government in 2003, from the Brazilian Social Democracy Party to the Workers Party, meant immediate changes for CGI.br. Three months after the new government began, a joint-ministerial ordinance of the Executive Office of the Presidency of the Republic (Civil House), the Ministry of Communications and the Ministry of Science and Technology defined a new composition for the committee, with a temporary mandate of less than 8 weeks. In the new composition, the number of participants, all of them nominated by the Federal Government, increased from 9 to 17, corresponding to 7 representatives from the federal government, 1 from the State government, 7 from non-government organizations and 1 from the academic community, seat that was occupied by the president of the National Research Network (RNP), an organization linked to Ministries of the Executive branch[x]. Thus, the academic seat in the temporary composition of CGI.br was also government.

The priority established for the new steering committee was to "study and propose a new model for Internet Governance in Brazil" (Brazil, 2003a).

Table 1. CGI.br temporary composition, in 2003, in charge of defining a new Internet Governance model

I. Federal Government
1. Ministry of Science and Technology (coordinator)
2. Civil House - Executive Office of the Presidency of the Republic
3. Ministry of Planning, Budget and Management
4. Ministry of Communications
5. National Telecommunications Agency - ANATEL
6. Ministry of Development, Industry and Foreign Trade
7. National Counsel of Technological and Scientific Development – CNPq
8. Academics Community
II. Private Sector
9. Telecommunications Infrastructure Providers
10. Internet Service and Access Providers
11. Informatics and Software Industry
12. Business Community
III. Others (1 seat)
13. Cultural and Educational Community
14. Internet Users Community
15. Third Sector (NGOs)
16. Information Technology Workers
17. National Forum of State Secretaries for Science and Technology Issues

Source: Based on Brazil (2003a). In blue, seats remained from the previous composition[xi].

At least three members of the transitory CGI.br body would be active actors at the World Summit on Information Society (WSIS), two years after, in 2005. Arthur Pereira Nunes (Ministry of Science and Technology), the coordinator of the committee, would join the Brazilian representation at the summit. Carlos Afonso (NGO) and José Alexandre Bicalho (ANATEL) would be part of the working group that built the definition to the global Internet Governance as a multistakeholder activity (WGIG, 2005). This is in fact

This transitory steering committee composition encompassing from the Executive Office of the Presidency to IT workers shows that the effort to create a multistakeholder group was contextual and contingent. From a broader perspective, the period of 2003-2010 was characterized by an increasing number of social participation mechanisms in the federal government, as assessed by previous research, establishing what has been defined as social participation as a government method (Pires & Vaz, 2012). Interestingly, well-known civil society actors became part of government at that time. Sergio Amadeu, from the Executive Office of the Presidency, office that created the CGI.br transitory body, is one example of that.

Among the main resolutions of the transitory body is the definition of a quadripartite multistakeholder model, that corresponds to the CGI.br model until now. It is based on the representation of government, private sector, third sector (that is civil society organizations or NGOs), and scientific and technological community. The federal government now holds 8

seats[xii] and the state governments 1 seat. The federal government was also assigned the right to nominate a notorious knowledge representative on Internet issues. The private sector and the NGOs hold 4 seats each, while the scientific community holds 3 seats, totalizing 21 places. Unlike the government, who nominates its representatives, the civil society elects them (as it will be discussed in the next section).

These changes in the seats composition have clearly impacted the strengthening of non-government actors in the steering committee. Comparing with the CGI.br first design, the private sector and the scientific and technological community gained two more seats, while the NGOs passed to be recognized as part of the Brazilian multistakeholder model, with four seats. Government also amplified its participation with three more Ministries, including the Ministry of Defense, the Ministry of Planning, Budget and Management and the Civil House, which is the Executive Office of the Presidency.

Table 2. CGI.br current composition defined by a presidential decree, in 2003

I. Federal Government
1. Ministry of Science and Technology (coordinator)
2. Civil House - Executive Office of the Presidency of the Republic
3. Ministry of Communications
4. Ministry of Defense
5. Ministry of Development, Industry and Foreign Trade
6. Ministry of Planning, Budget and Management
7. National Telecommunications Agency
8. National Counsel of Technological and Scientific Development - CNPq
II. Private Sector
9. Telecommunications Infrastructure Providers
10. Internet Access and Content Providers
11. Computer, Telecommunications and Software industry
12. Enterprises that use the Internet
III. Scientific and Technological Community
3 seats
IV. Third Sector (NGOs)
4 seats
Others (1 seat)
20. Notorious Knowledge in Internet issues
21. National Forum of State Secretaries for Science and Technology Issues

Source: Based on Brazil (2003c). In yellow, seats remained from the previous composition[xiii].

Another fundamental resolution of the temporary committee was the openness to create a new organization to constitute the executive office of the multistakeholder committee, replacing the FAPESP role as the Brazilian registry and registrar in the domain name system. The references of registries at that time showed a range of distinct models[xiv]. In the decree, it was established that the new organization under the CGI.br should be either a public or a

private non-profit institution. Behind this decision, there was the perception that the .br domain was a public good on the Internet, or the Brazilian "cyber-flag", as it was described by Hartmut Glaser[xv], who left FAPESP to keep his position as the head of the CGI.br executive office in the new organization.

The Brazilian Center for Information and Coordination of dot-BR (NIC.br) was created in 2003 under the CGI.br. It is a civil, private and non-profit legal entity that not only assumed, in 2005, FAPESP activities developed to CGI.br, but also amplified its scope with specific areas dedicated to different aspects of the Internet and the web operations since then divided by different areas. Currently, its activities involve coordinating the domain name system (Registro.br), studying and responding to security incidents (CERT.br), studying network technologies (CEPTRO.br), producing indexes on information and communication technologies (CETIC.br), implementing and operating the Internet Exchange Points (IX.br), enabling the participation of the Brazilian community in the global web forums and supporting new public policies (CEWEB.br), and housing the W3C office in Brazil (W3C.br), among others[xvi]. According to the authors' observations, these areas are very independent among them, having, including their own logos and websites, following together the purpose of working "for an Internet increasingly better in Brazil"[xvii]. The atmosphere, the facilities, the human resources policies, the financial management and audit are very business-oriented, deserving organizational studies under the realm of public administration.

With the new activities delegated to NIC.br, in 2005, the centrality of government had once more its role reduced in the national Internet governance. Additionally, the attributions of the CGI.br as defined in 2003 became more strategic. They reaffirm the steering committee as the main authority to define the policies regarding the DNS within the country, to promote studies and technical and operational standards for guaranteeing the security of networks and the leverage of Internet use, and to legitimize it to have representations in national and international forums (Brazil, 2003c). This is especially important, because ANATEL, the telecommunication agency regulator, is the official Brazilian representative at the International Telecommunication Union ITU. In some sense, CGI.br has officially received an international authority on Internet issues, having representatives at ICANN, IETF, and other organizations.

Although the CGI.br actions are not the focus of the present work, it is worth mentioning that, beyond the day-to-day activities that keeps the Internet in Brazil working, CGI.br's resolutions have contributed to build equilibrium among competitive forces that try to enact their proposals for shaping the Internet resources. It has also supported major political decisions even without any regulatory power. The creation of the "Principles for the Governance and Use of the Internet", also known as the CGI Decalogue[xviii] (CGI, 2009), which was used as a framework to build the public consultations of the *Marco Civil* (Almeida, 2015), and the coordination of the NETmundial Meeting in 2014 are some of the CGI.br actions that highlight its place in the national and global Internet governance.

4. The multistakeholderisms of CGI.br and their characteristics

As it happens in other multistakeholder institutions, the CGI.br has more than one model of multistakeholderism. A representative multistakeholderism can be found in its main body,

following the general lines defined in the decree that conceives it. A non-representative with participatory mechanisms follows a participative format and is called consulting chambers[xix].

4.1. The Representative model: the CGI.br main body

A structural change in the previous CGI.br model occurred with the resolution that non-government representatives should be elected by their own sectors, instead of being nominated by the government. This measure faced a considerable resistance from some government representatives, but it was defended by key governmental voices (Amadeu, 2008). To Rogerio Santanna, from the Ministry of Planning, Budget and Management at that time, such institutional modifications were important to bring legitimacy to Brazil's position of advocating the need to democratize the Internet and its infrastructure management in the global level (Amadeu, 2008, p. 6). Beyond the momentum of Brazilian politics, the global and local relations seemed to have served as a motivating factor to such changes.

4.1.1. The electoral colleges

Every three years, CGI.br forms an electoral college to elect 11 representatives, out of which 10 are nominated. To be precise, 6 electoral colleges are formed through the registration of organizations that want to vote. The multiple electoral colleges are necessary because each sector has its own voters, which are institutions whose nature of action can be classified within that sector. Among the private sector, the organizations need "to express in its constitution document the purpose of defending the interests of the segment" (Brazil, 2003c) in which they want to sign up. Among the scientific and technological community, the entities need to both have a scientific or technological nature and be representative of entities or scientists and researchers from that category. Finally, among the third sector (NGOs), the requirement to be a voter is to be classified within that sector. The entity does not need to be a representative organization as in the other sectors[xx]. This brings consequences that will be discussed below.

As a voluntary voting process, the formation of the electoral colleges every three years depends on the effort of some candidates to convince organizations to register. Thus, campaigning also means working on the formation of the college. Although the NIC.br communication releases information about the electoral process on their website and social media, the responsibility for increasing the awareness of the CGI.br and its elections is massively dependent on either the candidates or voluntary organizations and individuals who see the importance of doing it. The NIC.br's legal department is responsible for checking the documentation of such entities and approving their registration. An electoral commission is also formed to be in charge of specific questions during the process.

4.1.2. The voting process

Once the electoral colleges are closed, each entity can indicate one candidate. In accepting the indication, these individuals become the official candidates. NIC.br, then, sends the entity-

electors e-mails for them to vote. The voting process is electronic, based on the e-mail registered in the beginning of the process. According to the rules, the vote need to come from the legal representative of each entity (Brazil, 2003c), which is sought to be assured by the initial e-mail registration. It is also allowed to issue a letter of attorney giving power to another person to vote. This is a non-secret voting process, and the final results are published on the web.

Unlike the other sectors, the third sector (NGOs) entities could vote for four candidates, since 2004, given that the segment holds four seats. In 2016, the CGI.br changed this procedure (CGI.br, 2016a), allowing only one vote per institution in order to avoid the creation of informal tickets, where voters could be inclined to vote for a pre-defined group of four candidates, facilitating their decision process. With this action, the CGI.br has changed what was defined in the decree that conceives the committee, interpreting that this detail should be considered part of its own internal rules, thus, subject to the committee's autonomous definition. Officially, it is not, though.

The number of votes defines the holders and the alternates for each position and it varies substantially per sector. This occurs, in part, because of the campaigning process, but also because, unlike the private sector and the scientific and technological community, whose voters are representative entities, the third sector (NGO) voters are defined to be any single entity classified within that group. In 2013, for instance, the most voted holder of the scientific community got 4 votes, while the telecommunications infrastructure provider got 12 votes, the users-business sector reached 90 votes and the most voted third sector holder had 165 votes (CGI.br, 2013b).

There is lack of information on how the nominations from government occurs, but it commonly follows the decisions took by previous Ministers, nominating who is in charge of certain roles in the organizations. For instance, the National Secretary for Information Technology Policy of the Ministry of Science, Technology, Innovation and Communications is commonly nominated to be the coordinator of CGI.br[xxi].

Once part of the steering committee, all participants have similar formal powers, characterizing a homogeneous polyarchy, in Raymond and DeNardis's terms (2015) [xxii].

4.2. The participation model: the Consultative Chambers

As a way to leverage participation from civil society and government agencies which are not represented in the CGI.br main body (CGI.br, 2015), four tematic consultative chambers were created: Security and Rights on the Internet, Innovation and Technological Capacity Building, Content and Cultural Goods, and Universalization and Digital Inclusion. They were reformulated in 2015, but from the committee meeting minutes and from its webpage, it is not clearly stated yet the inputs that such arrangements should bring for the dynamics of the CGI.br meetings. They come as part of some broader efforts to make the CGI.br more public and open to contributions of other actors (CGI.br, 2013a). The expectations are that the steering committee also encompasses itinerant open meetings, online public consultations and public hearings on specific topics (idem).

The chambers are coordinated by current conselours and have permanent participants and specialists invited by them. These can be think tanks, NGOs, academia and government representatives, the CGI.br's alternate members, NIC.br staff, among others.

In 2016, the chambers were also the trails of discussion in the Brazilian IGF. With the coordinators and the permanent participants, the trails were also public meetings of the chambers, where the common audience also participated in the discussions. While interesting, the dynamics of participation will probably need some improvements. According to the authors' observations in the Security and Rights on the Internet chamber, information is lost when dependent on the systematization of one facilitator, who is responsible for sharing the results of small groups discussions with the whole chamber. The time constraints also limited participation, showing the trade-off between the format and the content.

Mechanisms to leverage participation and to guarantee that varied groups in terms of sectors, race, gender, cultural identity and other particular interests are heard, need to be developed. Nothing assures at this point actual participation has been really multi-stakeholder and diverse. Forms of accountability to make possible for ordinary participants to see how the content produced are integrated in the CGI.br discussions are also necessary to make the chambers an inclusive and supportive instrument for the main body of CGI.br.

5. Challenges of the CGI.br multistakeholderisms

5.1. The authority of procedural rules

Considering the CGI.br composition, a fundamental distinction can be noticed between the private sector, the third sector (NGOs), and the scientific and technological community. While the private sector has 4 subdivisions (see Table 2 above), and each of them is supposed to have its own electoral college to define one representative, the other two sectors do not have such subdivisions, which affects the profile of representatives.

In 2013, the elections of the scientific and technological sector resulted in representatives with background from three different areas: informatics, computer science, and communication. Interviews with current and former CGI members conducted during the field research show tensions associated to this result. Since the elections started at CGI.br in 2004, it was the first time that a member from the applied social sciences became part of the group. On the one hand, how much "technical" the representatives of this sector should be (Anastácio, 2015) seems to be a relevant question for the counselors. On the other hand, according to interviewees, intense rivalry during the meetings, given the different approaches brought by so distinct profiles, requires effective mediation to avoid confrontation. Not only there is a dispute about what "scientific and technological" means, but also there are implicit challenges to the authority of the procedural rules, which consider this sector open to any area of knowledge which has "Internet among its objects or initiatives and activities" (CGI, 2016a).

While those who defend more profiles specialized in the network operations are concerned with leveraging the Brazilian participation in the "technical" Internet debates, such as the Internet Engineering Task Force (IETF) (Anastácio, 2015), those who argue for more diversity in the body of the scientific sector recognize, according to the interviews, the value of having

different perspectives added to the debate, and the importance of areas, such as communication, law, medicine and others, for the Internet governance discussions. The conflicts make explicit the lack of consensus about the current rules.

Regarding the elections for the third sector (NGOs), controversies have intensified recently. As a result of the rules and the sector amplitude, a myriad of very diverse organizations has been part of the third sector electoral college, for instance, Regional Councils of Accounting, Service of Family Orientation, Cooperative of Agricultural Producers, Association of Fishermen, Friends and Residents, Environmental Support Center, among others. This situation has attracted a variety of criticisms, including the fact that many organizations are not closely related to Internet issues (Anastácio, 2015); the regional concentration of many of these organizations, and the lack of knowledge among the voters about what the role of CGI.br is (Wiziack, 2016).

These critiques reveal different understandings of what the CGI.br should be for some stakeholders. They, once more, challenge the authority of the institution procedural rules, which does not circumscribe the voters to Internet-related organizations, but imply that any organization is legitimate to vote for a representative at the CGI.br.

Regarding the critiques on the regional concentration[xxiii], brought by the interviewees, the study of the process shows that this can be a result of, at least, three factors, all related to the electoral process:

a) the cost of voting in a non-mandatory election process – the institutions need to both know about the process and be convinced to vote;

b) the centrality of candidates to build electoral colleges – the candidates are the responsible for leveraging public awareness and convincing entities to vote; and

c) the campaigning strategies – the candidates tend to focus on the regions and fields that they are closer to.

If regional representativeness starts to be considered a key element for composing the main instance of national Internet governance, then rules will have to be changed. Regional seats and rotation to give space for different regions to compose the committee are possibilities - and not only among the NGOs. This measure could also contribute to expand the public understanding on the CGI.br and prevent that CGI.br members, with strong electoral colleges, are continuously reappointed every three years.

Finally, on the lack of public knowledge on CGI.br, there are some elements that could be further studied. In the election process, that are, at least, two ways through which one voter-organization can delegate the right to vote to a third part. One is informing an e-mail, which will receive the link to vote, that is not administered by the legal representative of the organization. The second one is to issue a letter of attorney, during the registration process, informing that another person will vote instead of the legal representative. This person is not required to be from the same organization.

According to the interviews, in the 2013 elections, third-eight voter-entities informed the same e-mail to receive the electronic ballot to vote. At that time, the electoral commission decided to issue a letter to each organization asking for the legal representative to confirm that that was the correct e-mail address to receive the electronic ballot. All the entities confirmed the information. For the 2016 elections, the commission decided to add a new requirement in the

registration process, that is a “declaration signed by the entity's legal representative stating the reasons why the entity is interested in participating in the CGI.br” (CGI.br, 2016a).

While it is impressive the efforts to bring transparency to the electoral process at CGI.br, it is also visible that there is a trade-off between practicable and reliable mechanisms of voting. Surely, the transparency is affected when a voter-entity delegates its right to vote to someone else, informing a third-part e-mail in the registration process. The finality of the registration process is also challenged if an entity, which is apt to be a voter, issues a letter of attorney transferring such right to someone that could or could not be apt to vote according to the rules.

It seems imperative that the CGI.br voting process is revised in light of the challenges faced by the current mechanisms. The role of CGI.br and NIC.br in leveraging the public understanding of the process should also be reconsidered. The more society knows about national Internet governance issues, the more legitimate organizations can become voluntary voters, independently of the candidates’ campaign. This can strengthen the link between the electoral colleges and candidates’ platforms, and weakening possible votes based on personal characteristics or agreements.

5.2. Legitimacy in multistakeholder representation

All stakeholders have interests, including the NGOs (Belli, 2015). This can mean bridging the digital divide, fighting against child online violence, and inumerous indirect issues related to that. Interviews show that there are political benefits for the counselours’ causes when becoming part of the CGI.br due to their projection in national and international forums, and the political capital that emerges from that. Although this is still an area to be better studied, a dimension that is even less explored is the political and social gains for voters, specially in regions commonly with less influence over Internet policies.

According to the author’s observations in Paraiba, a small state in the northeast and from where one of the CGI.br’s representatives comes from, riverside dwellers, and Indigenous communities express satisfaction for having someone who they know as part of the Brazilian Internet Steering Committee. Those already involved in Internet discussions can notice the CGI.br importance through many different actions and events supported by CGI.br. The IGF 2015, which took place in João Pessoa, Paraiba’s capital, and the Brazilian IGF, which occurs in different cities within the country are some examples. Hence, while a rural settlement association may not seem to have a direct relationship with Internet issues, some of their interests is *to have access* to the Internet. From a democratic and inclusive perspective, given that the Internet has become an essential means of communication, their demands are legitimate and strategically canalized to the CGI.br, where the Ministry responsible for broadband programs is also part.

The argument for the exclusion of some entities, based on pre-judgments about their legitimacy to vote, needs to be problematized. What seems to be at stake in this contentious debate are the differences in the electoral rules among sectors and the voter-entitities legitimacy to give similar power to all the CGI.br’s participants, independently of their own prominence and social recognition as an entity.

5.3. The government role on national Internet governance issues

It is worth mentioning that the critiques about the supposed lack of legitimacy of the third sector's electoral college have been echoed by the telcos, which have publicly advocated for having more than one seat in the CGI.br (Prescott, 2016). The contentious situation arises at a moment when telco companies are trying to adopt data cap in their services. The CGI.br has issued a resolution saying that, in view of the Marco Civil, technical, legal and economic studies are necessary before such practices are adopted (CGI.br, 2016b), showing the balance that a multistakeholder organization can impose on the arguments of a unique stakeholder[xxiv].

The moment is propitious for this kind of pressure, given that recently there was an abrupt change in the Brazilian federal government, through an impeachment process that raised to power right-wing political groups, after fourteen years of a center-left government. The fact that the CGI.br is defined through a decree makes it a possible focus of reorganization in face of changes in the federal government. The number of government nominees – ten, considering eight from federal government, one from state level, and the Internet expert – is also larger than any other sector individually. Thus, there are reasons for accepting arguments that identify Brazil as a "hierarchical state society relations" kind of nation, similar to other BRICS countries (Raymond & DeNardis, 2015, p. 608). There are also reasons for the CGI.br to be considered a "state-sponsored multistakeholder effort" (Mueller, 2010, p. 120).

However, the financial independency, built on the NIC.br's registrar function, and the fact that the government nominees represent a minority member in the committee as a whole – 10 vs. 11 (currently 9 vs. 11 due to the merge of two Ministries) can be considered counterweights for this kind of reputation. It would be simplistic not to recognize the innovation of CGI.br not only for the Internet governance in Brazil, but also for the policy realm in general. While it centralizes the DNS functions and the installation and maintenance of Internet exchange points (IXPs), preventing market exploration, it also implies a policy meaning for such activities that, instead of being run by government, are run guided by a multistakeholder organization.

The eventual changes in rules, defined in the State decree, by CGI.br resolutions, as mentioned before, shows the kind of autonomy that the steering committee tries to acquire to execute its functions. This tension urges to be addressed. Considering the nature of both the Internet and a multistakeholder Internet governance institution, the dependence on a decree explicit the controversial legal subjection to government, which can, in thesis, change unilaterally the design of the governance. Mechanisms to assure the prevalence of public interest at CGI.br are necessary due to the pressures for changes that can occur, mainly in political transition periods, as it occurred in 2003 has occurred in 2016. Guaranteeing that any change in CGI.br occurs only after a multistakeholder decision to avoid interest capture is a possible action.

Questions that need to be further studied are related to the heterogeneity of interests inside the segments. Interviews with members and former members of CGI.br suggest that the government has not uniform positions, and different Ministries can represent different interests. Because the agenda for the meetings is approved by the coordinator, who represents the federal government, and is announced beforehand to all participants, dynamics among members to speculate and make agreements on positions are possible strategies. Given that the government is larger than any other sector, in case of voting, instead of consensus agreements, such political strategies can be determinant for the deliberation results.

5.4. Multistakeholderism beyond sectors

Although sectorial and regional inequalities are commonly used to discuss multistakeholderism, when the focus goes to diversity in the interests represented, this opens to other variables, such as race, gender, ethnicity, among others. Studies have shown how technologies are shaped by social values (Winner, 1986). They can definitely reproduce stereotypes and prejudices against subaltern groups and minorities, in both the infrastructure and web levels, as well as in their governance (Sweeney, 2013; Massanari, 2015; DeNardis & Hackl, 2016). What seems to be exclusively technical is always political.

Harassment and hate speech are issues of Internet governance according to the literature aforementioned, but why does not it become a recurrent topic in the agenda of governance organizations? There are innumerous challenges even when one's ideals are to create open structures of discussion and deliberation. As Fraser points out when criticizing the Habermas's bourgeois public sphere, this was not "simply an unrealized utopian ideal; it was also a masculinist ideological notion that functioned to legitimate an emergent form of class rule" (Fraser, 1990, p. 62). In the current CGI.br composition, there is visible misrepresentation of ethnicities, women and other gender identities, even though the most recent Brazilian IGF had a visual identity praising the population diversity.

Source: Brazilian IGF website (http://forumdainternet.cgi.br/)

As Fraser continues, even in the absence of any formal exclusions, social inequalities play their role in deliberation, including because unequally empowered social groups are likely to cultivate unequally valued cultural styles that generate marginalization on their contributions (Fraser, 1990). Fraser doesn't believe that it is possible to create artificial spaces, insulated from societal characteristics. She is emphatic in saying that "where societal inequality persists, deliberative processes in public spheres will tend to operate to the advantage of dominant groups and to the disadvantage of subordinates" (Fraser, 1990, p. 66).

This is why Beli (2015)'s argument on the importance of using mechanisms to map the interests of multistakeholder organizations' members, while informative, isn't sufficient to assure diversity beyond sectors. The active participation and proper hearing of subaltern groups in deliberation processes tend to be undermined.

Fraser is skeptical of single public spheres to congregate diverse and socially unequal discourses, suggesting instead, parallel arenas, or “counterpublic spheres” where “members of subordinated social groups invent and circulate counterdiscourses, which in turn permit them to formulate oppositional interpretations of their identities, interests, and needs as contestatory spaces” (Fraser, 1990, p. 67).

Talking specifically about the CGI.br, this doesn’t mean that groups currently underrepresented in its main body should stop trying to be part of it, obviously. Instead, in parallel to such efforts, they should also be incentivized to create their parallel arenas, that could be formally connected to the main body, as a way to support the counselors and guide the committee’s agenda toward the public interest. As showed here, CGI.br is already investing in the emerging model of Consultative Chambers, which could serve as an inspiration to a model focused not only on thematic issues, but also on subordinated social groups. This tends to increase CGI.br’s accountability and transparency, aligned with the purposes of the institution.

5. Conclusions

This paper sought to analyze the Brazilian Internet Steering Committee considering its current model and the historical trajectory that led the organization to evolve until nowadays. Undoubtedly, the CGI.br is a successful multistakeholder and policy case, emerged in a challenging national political environment, where advanced democratic mechanisms of participation and active civil society coexist with fragile stability and clarity of the public legitimacy.

A more attentive examination shows that CGI.br multistakeholderisms are in movement towards more participation, representativeness and responsiveness to society. Tensions on the meanings and interests at stake make the challenges explicit. Alternatives and ways to improve the election process and the CGI.br’s role on it, to leverage the public understanding of technology, and formally prevent arbitrary and unilateral government interventions are necessary. Further research on the characteristics of the voting process, the electoral colleges, the diversity of interests within the segments, and the meanings of being a representative and a voter at the committee are suggested.

In a broader scenario, the trajectory of CGI.br shows that context matters for the design of multistakeholder organizations, and that more studies of such models are necessary, in order to help materialize more precisely the various kinds of multistakeholderisms in vogue. Because the procedural rules of an organization can favor some groups over others, a deep understanding of them can help also improve current and future multistakeholder institutions.

Bibliography

Adachi, T. (2011). Comitê Gestor da Internet no Brasil (CGI.br): Uma Evolução do Sistema de Informação Nacional Moldada Socialmente (Doctoral Dissertation). Retrieved from: http://www.teses.usp.br/teses/disponiveis/12/12139/tde-10102011-165732/pt-br.php Last access 09/02/2016.

Almeida, G. A. (2015). Marco Civil da Internet - Antecedentes, Formulação Colaborativa e Resultados Alcançados. Em G. (. Artese, *Marco Civil da Internet: Análise Jurídica sob uma Perspectiva Empresarial* (pp. 19-64). São Paulo: Quartier Latin.

Amadeu, S. (2008) O Brasil e as disputas na Cúpula da Sociedade da Informação (WSIS - World Summit on the Information Society). Annals of the 6st Meeting of the Associação Brasileira de Pesquisadores de História da Mídia, May, 2008, Niterói, Rio de Janeiro. Available at: http://www.ufrgs.br/alcar/encontros-nacionais-1/encontros-nacionais/6o-encontro-2008-1/O%20BRASIL%20E%20AS%20DISPUTAS%20NA%20CUPULA%20DA%20SOCIEDADE%20DA.pdf Last access 09/19/2016

Anastácio, K. (2015). Brazil's approach to multistakeholderism: multi-participation in the Brazilian Internet Steering Committee (CGI.br). Berkman Center for Internet & Society at Harvard University. pp. 1-14

Belli, L. (2015). A heterostakeholder cooperation for sustainable internet policy making. *Internet Policy Review*, 1-21.

Brazil. Ministry of Communications and Ministry of Science and Technology (1995a). Portaria Interministerial N° 147, de 31 de maio de 1995. Available at: http://www.cgi.br/portarias/numero/147 Last access 09/19/2016

Brazil. Ministry of Communications (1995b). Portaria nº 148, de 31 de maio de 1995. Available at: http://www.anatel.gov.br/legislacao/normas-do-mc/78-portaria-148 Last access 09/18/2016

Brazil. Civil House of the Presidency of the Republic, Ministry of Communications and Ministry of Science and Technology (2003a) Portaria Interministerial N° 739, de 2 de abril de 2003. Available at: http://www.cgi.br/portarias/numero/739 Last access: 09/19/2016

Brazil. Civil House of the Presidency of the Republic, Ministry of Communications and Ministry of Science and Technology (2003b). Portaria Interministerial N° 740, de 2 de abril de 2003. Available at: http://www.cgi.br/portarias/numero/740 Last access: 09/19/2016

Brazil. Presidency of the Republic, Civil House (2003c). Decreto Nº 4.829, de 3 de setembro de 2003. Available at: http://www.cgi.br/pagina/decretos/108 Last access: 09/24/2016

Brazilian Internet Steering Committee – CGI.br (1998). Resolução 002/1998 de 15.04.1998. Available at: http://www.ufrgs.br/sedetec-intranet/pagina/eitt/download/registro/resolucao_cg2.pdf Last access: 09/19/2016

Brazilian Internet Steering Committee – CGI.br (2009). Resolução CGI.br/RES/2009/003/P. Available at: http://www.cgi.br/resolucoes/documento/2009/003 Last access: 09/24/2016

Brazilian Internet Steering Committee – CGI.br (2009). Ata da Reunião de 15 de janeiro de 2010. Available at: http://cgi.br/reunioes/ata/2010/01/15 Last access 09/25/2016

Brazilian Internet Steering Committee – CGI.br (2013a). Resolução CGI.br/RES/2013/005. Available at: http://cgi.br/resolucoes/documento/2013/005 Last access 09/25/2016.

Brazilian Internet Steering Committee – CGI.br (2013b). Resultado do processo eletrônico de votação da Eleição CGI.br 2013. Available at: http://cgi.br/pagina/resultado-do-processo-eletronico-de-votacao-da-eleicao-cgi-br-2013/145 Last access 09/25/2016

Brazilian Internet Steering Committee – CGI.br (2015). Ata da Reunião de 27 de março de 2015. Available at: http://www.cgi.br/reunioes/ata/2015/03/27 Last access 09/25/2016.

Brazilian Internet Steering Committee – CGI.br (2016a). Chamada para convocação do Processo de Eleição em 2016, dos representates da Sociedade Civil para integrarem o CGI.br. Available at: http://www.cgi.br/processo-eleitoral/chamada-eleicoes-2016 Last access 09/26/2016

Brazilian Internet Steering Committee – CGI.br (2016b). Resolução CGI.br/RES/2016/015. Available at: http://cgi.br/resolucoes/documento/2016/015 Last access 09/27/2016.

Carvalho, M. S. R. M (2006). A Trajetória da Internet No Brasil: do Surgimento das Redes de Computadores à Instituição dos Mecanismos de Governança (Masters' thesis) Last access 09/03/2016

DeNardis, L. (2014). *The global war for internet governance.* New Heaven: Yale University Press.

DeNardis, L., & Hackl, A. (2016). Internet control points as LGBT rights mediation. *Information, Communication & Society*, 753-770.

Duneier, M. (2011). How not to Lie with Ethnography . *Sociological Methodology*, 1-11.

Epstein, D. (2013). The making of institutions of information governance: the case of the Internet Governance Forum. *Journal of Information Technology*, 137-149.

Frey, K. (2000). Políticas Públicas: Um Debate Conceitual e Reflexões Referentes à Prática de da Análise de Políticas Públicas no Brasil. Planejamento e Políticas Públicas, 211-259.

Fraser, N. (1990). Rethinking the public sphere: A contribution to the critique of actually existing democracy. *Social Text*, 56-80.

Kleinwächter, W. (2011). *MIND: Co:laboratory Discussion Paper Series nº 01 # 2 Internet Policy Making.* Berlin - Nairobi: Internet and Society Co:llaboratory.

Knight, P. T. (2014). The Internet in Brazil: Origins, Strategy, Development and Governance. Bloomington: Authorhouse

Latour, B. (1994). Jamais fomos Modernos. São Paulo: Editora 34

Lofland, J., Snow, D. A., Anderson, L., & Lofland, L. H. (2006). *Analyzing Social Settings: A Guide to Qualitative Observation and Analysis.* Cengage Learning.

Massanari, A. (2015). #Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. *Media & Society*, 1-18.

Maxwell, J. (2013). *Qualitative Research Design: An Interactive Approach.* New York: Sage Publications.

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance* . Cambridge: The MIT Press.

NIC.br; CGI.br (2016) VI Fórum da Internet: Congresso e Internet em números http://forumdainternet.cgi.br/files/ApresentacaoJuridico.pdf

Pires, Roberto; Vaz, Alexander (2012). Participação social como método de governo? Um mapeamento das "interfaces socioestatais" nos programas federais. Brasília: Institute for Applied Economic Research (Ipea).

Prescott, Roberta (2016). Para diretor da América Móvil, CGI tem problemas de transparência, escopo e composição (06/29/2016). Available at: http://www.abranet.org.br/Noticias/Para-diretor-da-America-Movil,-CGI-tem-problemas-de-transparencia,-escopo-e-composicao-1117.html Last access: 09/26/2016.

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: anatomy of an inchoate global institution. *International Theory*, 572-616.

Rede Nacional de Pesquisa – RNP (2003). Governo dá prazo até 25 de maio para CG propor novo modelo de governança da Internet no Brasil. Available at: http://www1.rnp.br/noticias/2003/not-030417b.html Last access 09/19/2016

Sweeney, L. (2013). Discrimination in Online Ad Delivery. *arXiv:1301.6822*, 1-36.

Winner, L. (1986). Do Artifacts Have Politics? . Em L. Winner, *The Whale and the Reactor: a Search for Limits in an Age of High Technology.* Chicago: University of Chicago Press.

Wiziack, Julio (2016). Governo quer mudar regras de comitê gestor da internet. Folha de São Paulo. 07/16/2016. Available at: http://www1.folha.uol.com.br/mercado/2016/07/1792333-governo-quer-mudar-regras-de-comite-gestor-da-internet.shtml Last access 09/25/2016

Working Group on Internet Governance - WGIG (2005). Report of the Working Group on Internet Governance. Chatêu de Bossey (June, 2005). Available at: http://www.wgig.org/docs/WGIGREPORT.pdf Last access 09/23/2016

[i] Comitê Gestor da Internet no Brasil.

[ii] For instance, the Congress has already 32 bills trying to change the Marco Civil, the Brazilian Civil Rights Framework for the Internet, a law which passed in 2014 and was celebrated by national and international Internet community (NIC.br. CGI.br, 2016).

[iii] This field work research was conducted between July and August of 2016 in São Paulo, Porto Alegre and João Pessoa, in Brazil, and was possible thanks to the Columbia University's School of International and Public Affairs and Carnegie Research Support. The trip to João Pessoa resulted of an invitation to moderate a seminar at the Expotec, supported by CGI.br and the National Association for Digital Inclusion (Associação Nacional para a Inclusão Digital, ANID).

[iv] Núcleo de Informação e Coordenação do Ponto BR.

[v] Escola de Governança da Internet no Brasil.

[vi] The translation of this and others ordinances, decrees, and legal documents excerpts issued in Portuguese were done by the author.
[vii] Later, in 1998, the Telebrás would be privatized.
[viii] To more information on the origins of the Internet in Brazil, see Knight (2014).
[ix] The annual price was defined in 50 reais, and in 2007 it was shrunk to 30 reais (less than 10 dollars, in 2016) (Carvalho, 2006; Adachi, 2011). In 1996, FAPESP had approximately 1,000 Internet Protocol (IP) numbers available, according to the interviews.
[x] According to its website, the RNP has been a "Social Organization (OS) bonded to the Ministry of Science, Technology, Innovations and Communications (MCTIC) and maintained thereby together with the Ministries of Education (MEC), Culture (MinC), Health (MS) and Defense (MD)" since 2002. Available at: https://www.rnp.br/en/institutional/who-we-are Last access 09/20/2016. Its president at that time was Nelson Simões da Silva.
[xi] Two seats were extinct and don't appear in the new composition: Telebrás and the National Research Network (RNP). The first lost its centrality in the Brazilian telecommunication after being privatized in the former government, while the RNP occupied the academic seat, as previously explained.
[xii] In May, 2016 the Ministry of Communications and the Ministry of Science, Technology and Innovation, which have two seats at CGI.br according to the decree, were merged into one. The new Ministry of Science, Technology, Innovations and Communications holds now only one seat, keeping the coordination of the steering committee.
[xiii] Beyond the three federal government representatives, the CGI.br composition in 1995 had also one seat for each of the following: Telebrás, National Research Network (RNP), academic community, service providers, business community, Internet users community, totalizing nine seats. The categories for non-government, as defined in 1995, were broad.
[xiv] In Latin America, there were models administered by academic institutions (e.g. Chile, Mexico) and by government (e.g. Argentina). There were also other globally well-known models where the market (e.g. United States) or non-profit organizations (e.g. Germany) were in charge of the names and numbers coordination.
[xv] Interview to the author.
[xvi] Available at: http://nic.br/perfil/ Last access in 09/24/2016.
[xvii] "Por uma internet cada vez melhor no Brasil", in Portuguese. Available at: http://www.nic.br/nic-br-por-uma-internet-brasileira-cada-vez-melhor/ Last access in 09/24/2016.
[xviii] Decálogo do CGI, in Portuguese.
[xix] Câmaras de Consultoria, in Portuguese.
[xx] According to the interviews, because the third sector is a very distributed and powdered segment – under-institutionalized in Mueller's terms (2010) – the CGI.br transitory body decided for not restricting the voters to representative entities, numerically limited in the country.

[xxi] A different pattern was noticed when Vanda Scartezini, in 1999, was the Secretary for Information Technology Policies. Ivan Moura Campos was nominated the CGI.br coordinator instead of her.
[xxii] It is worth mentioning that because the number of votes necessary to be elected at the CGI.br is so distinct, in thesis, the vote of a NGO values less than the vote of a scientific and technological or of a private sector representative entity. Consequently, the cost to be elected is also different. On the one hand, if this is calculated in terms of votes, this cost is higher for NGOs candidates. On the other hand, if one supposes that a council needs to approve such vote in representative entities, the cost of one vote is not the same of ones NGO's vote. Differences among the electoral colleges at the CGI.br and their consequences deserve further studies.
[xxiii] The data on the regional origins of the voters-organizations are not released by the NIC.br (e.g. https://elections.registro.br/eleicoes-cgi/entidades) to confirm to what extent these critics are characteristic of the electoral process. It is valid to analyze this information quantitatively.
[xxiv] In a recent conference, the CGI.br counselor Eduardo Levy, who represents the telecommunication sector declared: "I am the [telco] representative at the CGI.br. Out of 21 members, 20 are bandwidth consumers and one is who invests to provide the service. So, if there is voting - and my struggle is that there is always consensus – I always lost by 20 to 1" (Prescott, 2016).

Global Digital Futures Policy Forum 2016: Issues Brief

Panel 1: Global Security Challenges and Data: Intelligence Gathering, Encryption, and Sharing in a World of ISIS

By David Omand

We are living through the beginnings of a revolution in human affairs enabled by the digitization of information and means of communication through the Internet, web and mobile devices (with the Internet of Things to come). We are now dependent on this technology for our economic and social progress, to deliver international economic development and for our national security and public safety. As set out below, trust has to be built in the open Internet as a safe place to innovate, to do business, to shop and to interact socially, and in the ability of the authorities to be able to uphold the law in cyberspace. That trust cannot be taken for granted.

Conflicting priorities arise at three levels:

- Surveys record increasing *concerns by individuals* for their right to privacy, for protection of their personal information from hackers, from carelessness on the part of corporations, from unrestrained government surveillance, from new techniques such as predictive analytics, and from the very business model of the Internet that rests on the monetization of personal data. One result is the demand for end-to-end encryption, anonymization software, for secure apps and mobile devices and for stronger data protection law. Another is the risk of fragmentation of the Internet as some governments seek to restrict where their citizens' data may be processed or stored.

- At the same time, *law enforcement* expresses growing concern over the way that serious criminals are able to exploit the vulnerabilities of digital technology (and human behavior when using it) to conduct their crimes at scale. Daesh terrorists have been able to use the web to publicize their atrocities and recruit new followers whilst being able to hide their communications from the authorities. Criminal activity using the Internet (including the Dark Net) includes terrorist facilitation, sale of cyber attack exploits, global fraud and money laundering, narcotics trafficking, proliferation of weapons of mass destruction, human trafficking, child sexual abuse and intellectual property theft. Law enforcement is finding it increasingly difficult to counter these threats, to establish the identities of those responsible and to secure the evidence they might have in the past to bring the criminals to justice, especially when they are hiding overseas, or the evidence is in corporate databases in another jurisdiction.

- Meanwhile, *national intelligence agencies* have been able to exploit digital technology to gather information for the protection of national security (the fundamental duty of government) including generating intelligence for military operations and force protection around the world, to support diplomacy and national security policy making and to protect the critical national infrastructure from destructive cyber attacks. At the same time, intelligence agencies have been

trying to use their advanced capabilities to assist law enforcement in their mission to keep the public safe, uncovering global criminal networks, and especially tracking terrorists across frontiers. The legal framework for such activity has been shown to be defective or missing altogether in many nations. The exposure of many of these capabilities has heightened the concerns over privacy described above.

As with all hard public policy issues there is no easy way of reconciling competing demands. Place security of personal data and anonymity on the Internet above all else and law enforcement is shut out, the rule of law is undermined, crime, terrorism and cyber attacks will flourish. Prioritize access for law enforcement and intelligence agencies, for example through weakening encryption standards, and confidence in the Internet as a secure medium will be lost and fragmentation of the Internet will spread.

A set of satisficing measures is needed sufficient to ensure respect for *all* our fundamental rights - to the rule of law, to life, to freedom of speech and assembly, to enjoyment of property, to privacy for personal and family life - without lurching to any extreme. In particular, security and privacy should not be traded off one for the other: a sufficiency of both is necessary in a civilized society.

What makes these issues even harder is that solutions have to be found not just nationally but internationally, and in the context of a global struggle over the governance of the Internet itself. Measures are needed that reinforce the nature of the Internet as a secure, open and safe medium, that are technically sound and that make business sense as well as encouraging the 'permissionless' innovation that is the hallmark of the Internet. Government policies might therefore:

- Insist upon continuing multi-stakeholder Internet governance engaging governments, the Internet companies, the tech community and civil society.

- Oppose mandatory data localization and the fragmentation of the Internet into national blocks.

- Maintain the open nature of the Internet where data flows are based upon efficient routing principles and protocols and on open standards openly arrived at.

A promising approach is to encourage in forums such as the OECD, the UN Governmental Group of Experts, the Internet Governance Forum, NETmundial, G20 and the World Summit on the Information Society the development of norms of responsible conduct in cyberspace for like-minded States (accepting that although not all States will initially comply, the reputational cost of bad behavior will be raised). Governments, civil society and the tech community should:

- Insist upon the application of International Humanitarian Law to constrain offensive activity in cyberspace as much as in the everyday physical world.

- Insist upon Governments not weakening or compromising encryption or other standards on which the integrity of the Internet depends. The core infrastructure of the Internet must remain stable and secure.

- Ensure the development of the Internet of Things includes security, and is not based on closed, proprietary systems.

- Enable cyber security partnerships between government agencies, the private sector operators of the critical national infrastructure and the tech community.

- Encourage the development of the cyber insurance industry.

- Insist that any restrictions on Internet content are solely for the purposes of public safety and security and as provided by law and oppose governments trying to shift to the private sector responsibility for policing the content of Internet traffic.

- Encourage the development of new trust architectures, such as may come from blockchain innovation

Governments should, in particular:

- Work to develop common standards of data protection across borders to build confidence in data hosting and processing where most efficient.

- Build effective international information and evidence arrangements to tackle current issues of terrorism, organized global criminality and cyber security. Starting with discussions between the US and the EU seek to reform Mutual Legal Assistance Treaty MLAT processes and develop cyber-MLATs and cross-border arrest warrants for cyber crimes.

To reinforce both security and privacy, governments, civil society and the tech community should:

- Accept the necessity for digital intelligence activity (including, when necessary, access to the Internet in bulk as a legitimate means of gathering foreign intelligence and managing the risks of hostile cyber attacks) but insist all such activity must be covered by the rule of law. Statutory safeguards should involve:

    - Regulation of intelligence and law enforcement agencies stipulating the purposes for which they may acquire secret intelligence and the safeguards for privacy and other human rights that must be applied when intrusive methods are used.

    - Authorization procedures that cover all the ways of accessing digital intelligence: from communications data, the content of communications, interference with equipment (including hacking into adversaries' systems) and the holding and exploitation of databases containing personal information about individuals.

    - Independent judicial and legislative oversight of intrusive intelligence activity.

    - Independent judicial investigation of allegations of abuse and right of redress if proven.

- Apply the principles of the Universal Declaration of Human Rights, accepting that the right to privacy in cyberspace is not absolute where there are legitimate, necessary and proportionate reasons for the authorities to intrude (including 'reasonable searches and seizures' as provided for in the U.S. Constitution's 4th Amendment).

- Accept that law enforcement has the right to seek, with proper authority, evidence relevant to investigations that is held by Internet companies, and that companies have a duty to respond cooperatively where there is no conflict of laws, where the request is legally sound and reasonable in the circumstances, and where to comply with the request would not place at risk unreasonably the security of other users of cyberspace.

- Accept that privacy rights are engaged when the authorities seek bulk access to personal information (in motion or stored). The extent of privacy intrusion, and thus whether it is compatible with privacy rights, depends then upon whether computerized search algorithms to filter, target and select material for analyst examination comply with the principles of lawfulness, necessity and proportionality. Mass surveillance, on the other hand, should be considered unlawful.

- Provide for added protection where legal professional privilege, journalistic material, ministers of religion and legislators are concerned.

- Accept that there are legitimate reasons for enabling anonymity on the Internet, including for use by dissidents in repressive regimes and by journalists to protect their sources but that, as with privacy, it is not an absolute right. In particular, there is no right to anonymity for operation of websites on the dark net.

- Redefine legal thresholds for so that the most revealing forms of meta data such as the complete browsing history of an individual are treated in the same way as content of communications, whilst allowing basic communication data – who called, when, where, for how long, by what means – to remain a basic tool of policing.

Global Digital Futures Policy Forum 2016: Issues Brief

Panel 2: National Data Governance in a Global Economy

By Anupam Chander

Introduction

Global data flows are the lifeblood of the global economy today and of the technologies of the future. Yet, the regulation of how data is to be handled remains largely the province of national laws. How we resolve the dilemmas of global flows within a nation-state structure will impact the digital economy, free expression, privacy, security, consumer protection, and taxation. Just as we once built an architecture for cross-border flow of goods, we need to build an architecture for cross-border flow of information.

Problem Statement

In the absence of, at minimum, a *modus vivendi* for global data flows, the World Wide Web may increasingly tear apart, and the global Internet may disintegrate into national or regional 'Splinternets.'

Issues

Global Data Flows Are Crucial to Innovation

Many of the most promising technologies and economic innovations rely on global data flows. Consider the following ten recent developments:

1. **The Internet of Things.** Devices like an Apple Watch or a Samsung Smart TV — or even a John Deere or Komatsu heavy machine — depend on the flow of information across national borders to gather and process data.
2. **App Economy.** Individuals and small companies can now build applications and leverage global marketing, distribution, and payments networks to sell their products and services to the nearly 2 billion smartphone users across the world.
3. **Outsourcing of Services.** The ability to outsource business processes and information technology services depends on the cross-border flow of information.
4. **E-commerce.** Companies like Alibaba and eBay depend on global information flows to enable people to sell to, and buy from, global markets.
5. **Cloud computing.** Cloud computing depends on the transfer of large volumes of information, often across borders, to server farms typically located based on network efficiencies, security, and costs. Robots, for example, increasingly depend on cloud-based information storage and processing.
6. **Big data.** Data sets can be larger if they include people across borders; analytics are often performed using tools and companies located in foreign jurisdictions.
7. **Digital products and streaming services.** Digital music and video services, from Apple, Netflix, Spotify, and others, increasingly allow customers across the world to download

or stream audiovisual content.

8. **Social media and websites generally.** Social media, and the Web generally, implicate significant information sharing across borders.
9. **The sharing economy**. AirBnB, Uber, and the like allow one to share one's resources, often for a price, with people from anywhere in the world.
10. **Crowdfunding**. People planning new projects can now raise funding from supporters across the world.

Rules that make it difficult to move data across borders will complicate and even at times make impossible efforts to offer such innovations. For example, if companies rolling out Internet-enabled devices have to create or purchase separate data infrastructures for each country in which they operate, the costs of providing many such devices may prove prohibitive. Companies like AirBnB, Uber and Upwork depend on individuals across the world sharing information across national borders. Finally, rules that prevent information from leaving home except in difficult to obtain circumstances can effectively bar foreign service providers offering back office outsourcing from processing information (a result that trade protectionists favor).

The Rise of Internet Border Controls: From Censorship to Data Localization

Efforts by national governments to assert control over global data flows trace back at least to the turn of the Millennium. A French court ordered Yahoo! to prevent Nazi material from being made available within France. Yahoo! protested that they should be governed by the liberal free speech codes of their American home, but the French court was unpersuaded, and Yahoo! voluntarily complied by removing the material from its services everywhere. A more notorious application of governmental efforts to control information can be found in the so-called Great Firewall of China, which enlists Internet companies in censoring material within the country. Recently, France's privacy regulator has penalized Google for failing to remove search results subject to the "right to be forgotten" from sites outside France, not just from results accessible in France as Google was prepared to do.

The French Yahoo! decision and the Great Firewall of China represent what we might describe as the first generation of Internet border controls, that is, efforts to control information coming *into* a country. "**Data localization**" is the name for a less familiar but increasingly popular new kind of Internet border control. This second generation of Internet border controls seeks to keep information from going *out* of a country. Governments seek data localization on a variety of grounds, from data protection to outright protectionism.

Many governments have increasingly sought "**data sovereignty**," often seeking both to control data within their countries and to limit the flows of data outside their countries. The globalization of data raises issues that the globalization of goods did not, because data often contains very personal information, for example about our searches, our likes, our friends, our finances, and our health. It is easy to use the sensitivity of data to bar foreign service providers by requiring that data be stored or processed by local providers. Assertions of data sovereignty often coincide with a general industrial plan to grow a local set of Internet services to displace the largely American leaders (including Google, Apple, Facebook, and Amazon, or "GAFA" as

they are sometimes labeled in Europe). Experience with trade in goods, however, tells us that it is possible to meet varying national safety standards even when importing goods from abroad.

Figure 1. Internet Border Controls

	First Generation	**Second Generation**
Type of control	Censorship	Data Localization
Stated Goals	Prevent unwanted information from entering country for social or political purposes	Prevent information from leaving country to (1) protect privacy (though privacy can be protected even when information is processed abroad); (2) assist local law enforcement, surveillance & control; (3) promote local enterprise
Examples	Great Firewall of China	Russian data localization

Protecting Privacy and Avoiding Foreign Surveillance

Last year, the European Court of Justice took up an Austrian law student's challenge to Facebook's processing of his personal information. In *Schrems v. Irish Data Protection Commissioner*, the court concluded that United States surveillance practices meant that European data could no longer be processed in the United States under an existing Safe Harbor agreement. In response the United States has agreed to added protections against mass surveillance for Europeans under a "Privacy Shield" arrangement, including a right under a new United States Judicial Redress Act to sue the U.S. government for mishandling their data. Some in Europe have criticized the new arrangement as containing inadequate guarantees.

The case against Facebook recalls two other cases in which American companies have been asked to assist U.S. law enforcement. In 2013, a US. judge directed Microsoft to turn over user information stored on its Irish servers, but Microsoft has challenged the order, earning the support of the Irish government. Most prominently, in a domestic case with international implications, Apple fought the U.S. government's initial efforts to compel it to assist in defeating a security feature on its iPhone, in part because complying would empower other governments to demand Apple's assistance as well.

Because both Europe and the United States recognize the importance of cross-Atlantic data flows to the economies of both regions, a new arrangement permitting transfer must be found to allow information to flow across the Atlantic. As it stands now, companies and individuals continue to transfer information because of necessity, but lack any assurance that such transfers will not subject them to liability. As the European Union (EU) implements the new General Data Protection Regulation (replacing the 1995 Data Protection Directive), liability

under EU law becomes ever more alarming, potentially subjecting a company to fines up to four percent of the company's annual global turnover.

Conclusion: Charting a Path Forward in Cyberspace

If we are to gain the enormous benefits from information exchange made possible by the Internet, we will need to engage in a series of reforms. These may include:

- *Surveillance Reform*. Need for respecting dignity of foreigners abroad; recognize that International Covenant on Civil and Political Rights (ICCPR) obligations apply to a government's actions not just at home, but also with respect to foreigners abroad. The US EU Privacy Shield provides some assurance that Europeans will not be subject to mass surveillance by U.S. authorities, including actionable guarantees of freedom from mass surveillance under the Judicial Redress Act. Thus far, it is unclear whether citizens of foreign countries outside Europe might benefit from similar guarantees of freedom from mass surveillance.

- *Privacy protections*. Governments need to ensure data protection, so that privacy and security are upheld regardless of where data flows. Here there a number of competing models, including the European Union's General Data Protection Regulation (an omnibus consent based approach to all processing of personal information regardless of entity) or the United States sectoral privacy law (focused on certain categories of sensitive information held by industry professionals) coupled with privacy promises enforced by the Federal Trade Commission and class action lawyers.

- *Free Trade Commitments*. Commit governments to permit data to flow across the world and services to be performed from abroad, unless legitimate interests such as privacy require otherwise. If it is ratified, the Trans-Pacific Partnership agreement between a dozen Pacific rim nations would require governments to permit cross-border data flows unless justified by a "legitimate public policy objective." It is unclear whether the Transatlantic Trade and Investment Partnership (TTIP) being negotiated between the United States and Europe will subject European crossborder data flow restrictions to any trade disciplines. Finally, the Trade in Services Agreement (TiSA) being negotiated now between a large number of developing and developed nations, including the United States and nations of Europe, seems likely to include provisions favoring crossborder data flows.

- *Crossborder Government Access to Data*. Reform of the cumbersome Mutual Legal Assistance Treaty process is needed, but any reform must respect human rights limits on government access. The current process is flawed in multiple respects. As a map by Access Now makes clear (see https://mlat.info/), not every country has a law enforcement information sharing agreement with every other country. A United States statute from 1986, the Stored Communications Act, prohibits Internet companies subject to the law from sharing information with foreign governments, permitting sharing only with "governmental entities" (defined as "a department or agency of the United States or any State or political subdivision thereof"). Finally, even when a law enforcement agency

seeks information through the MLAT process, compliance is painfully slow. Governments will need to work in multiple forums to improve human rights-protective systems of government access to information stored across borders. Because security information held abroad will often be held by corporations, corporations too must pay increasing attention to what rules they follow in providing access to foreign service providers.

- *Dispute Resolution*. Encourage the development of Internet-based crossborder dispute resolution systems. Existing trade agreements and even the "twenty-first century" agreements being negotiated now lack low cost mechanisms accessible to consumers and businesses to resolve disputes. Companies like eBay and PayPal have created their own global dispute resolution systems, and it seems likely that more private efforts to create such Internet based mechanisms will emerge.

Section 3:
Economic Issues in a Digital World

Building the Superfast Internet One City at a Time: The Case of Google Fiber[1]

Burcu Baykurt[2]
Columbia University

Abstract: This paper examines the case study Google Fiber's experiment in Kansas City, and discusses "how infrastructure happens" (Star and Bowker 2006) on the ground. It asks: how does the gigabit internet transform into an ostensibly civic technology? What motivates city dwellers to turn private services into quasi-universal infrastructure projects? Drawing on interviews with city officials and civic leaders who led or participated in the drive toward becoming a "gigabit" city, I discuss the motivations and efforts that aimed to make Google Fiber experiment succeed. In the first part of the paper, I demonstrate how internet connectivity is strategically positioned, simultaneously, as a basic infrastructure, a technical experiment, and a speculative catalyst of economic growth. I then examine the implementation process and emerging setbacks to explain what the subsequent civic mobilizing to remedy problems on the ground reveals about the blurred boundaries between public and private services in the digital city.

[1] I am indebted to Benjamin Dean, Merit Janow, Michael Schudson, and the participants of NYLON workshop at New York University for their valuable feedback on various iterations of this brief. This study has been funded by the Carnegie Corporation of New York, the Tech and Policy initiative at Columbia SIPA, and the Tobin Project Graduate Student Fellowship.

[2] Burcu Baykurt is a Ph.D. student at Columbia University with research interests in cultural sociology, public policy, and media studies. Her dissertation explores social and cultural implications of information technology, especially in cities and local governance. Other research projects deal with the consequences of networked communications in journalism and free speech, the interaction between cultural change and policymaking, and the role of culture in international relations.

"Emerging Markets for Cybercriminals: Ransom and Purchase of Stolen Data by Victims and Authorized Intermediaries"

Josephine Wolff[1]

The business model of cyber criminals who steal or access protected information and computer systems for the purpose of profiting financially is increasingly shifting from a market in which those criminals sell their stolen information to other criminals and fences to a market dominated by the sale of that data back to its original owners. This strategy of selling data back to its original owners can take multiple forms, including ransomware, in which a victim's computer systems are compromised and typically encrypted until a payment is made to the perpetrators, or data exfiltration, in which a firm's proprietary information is stolen and then purchased by that firm itself in attempt to prevent it from being sold to competitors. Both of these forms of victims purchasing their own data—acquiescing to ransomware demands and purchasing stolen data on the black market—present several challenges for law enforcement, provide significant economic incentives to criminals, and raise complicated questions around the ethics and legality of otherwise law-abiding citizens funding criminal endeavors and legitimizing the markets for stolen data. This paper examines the emerging trends in cyber crime that point towards increased activity in selling stolen data back to victims and their authorized intermediaries, and analyzes the relevant legal regimes that might apply to the victims who engage in these activities and current ambiguity around when victims may purchase access to stolen or compromised data. Finally, it proposes policy recommendations intended to disincentivize the payment of ransoms and purchase of stolen data by victims, while incentivizing the implementation of appropriate data protection measures and security controls.

[1] This research was made possible by a grant of the Carnegie Corporation of New York.

The Economic Effects of Information Security Failures on Firms, 2005-2015

Christos Makridis and Benjamin Dean[1]

Abstract

We construct the first firm-level panel dataset containing both financial outcomes and information security failures for a subset of publicly traded companies between 2005-2015. First, we document several stylized facts about the types of firms with cyber breaches based on size, assets, and profitability. We subsequently examine the associations between information security incidents and financial firm-level outcomes. Second, we document how two key empirical challenges in this space---unobserved firm heterogeneity and selection---create serious problems for causal inference. Unobserved heterogeneity arises from the fact that larger and more productive companies may be more likely to be the target of cyber attacks, but are also more likely to have better information security. Selection arises from the fact that firms may not report all their breaches since disclosing a breach signals a technology and/or security gap in their infrastructure. We show that simply having panel data on firms is not sufficient to resolve the problem of unobserved firm heterogeneity when selection is also present. While we find evidence of a strong negative effect of cyber breaches on firm productivity, our estimates are imprecise and not necessarily causal. Third, we conclude by underscoring ways in which policymakers might take these insights to better partner with academics and deal with security gaps in the current infrastructure.

Keywords: Cyber crime; firm-level cyber incidents; productivity; selection; unobserved heterogeneity.

[1] Stanford University and Columbia University; email: cmakridi@stanford.edu and bcd2120@columbia.edu.
Acknowledgments: Christos Makridis thanks Columbia SIPA for their doctoral fellowship from the Carnegie Corporation of New York. We also thank Jay Healey at SIPA for comments on an early version of the draft and Herb Lin and the Stanford Cybersecurity Initiative for feedback.

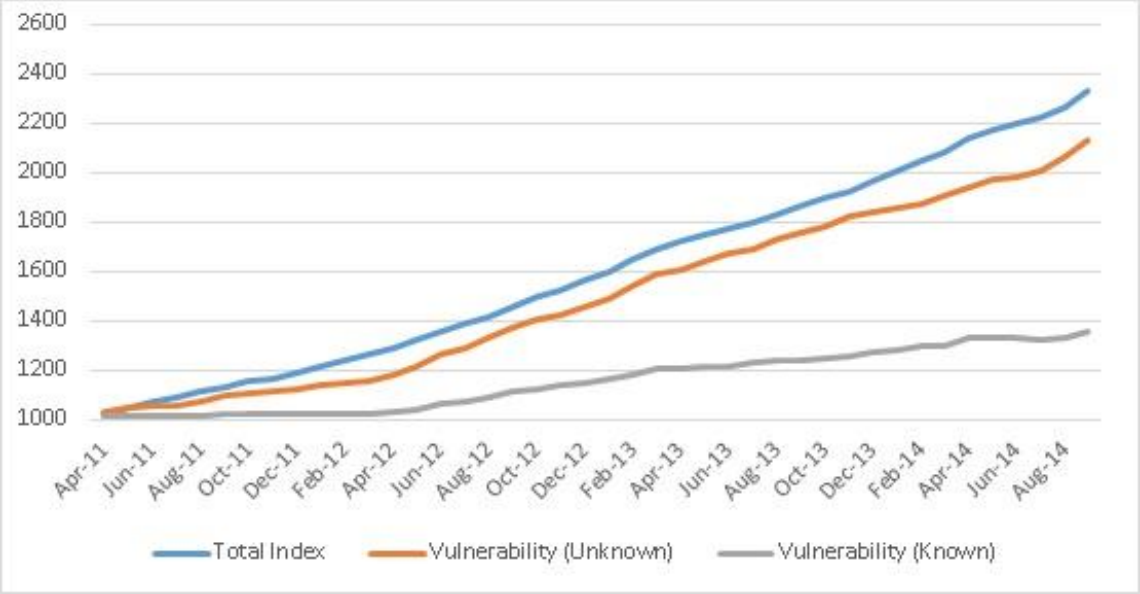
The loss of industrial information and intellectual property through cyber espionage constitutes the "greatest transfer of wealth in history." -- General Keith Alexander.

Measurement is the first step that leads to control and eventually to improvement. If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it. -- H. James Harrington

1. Introduction

Information and security has become a pressing issue in the wake of several large-scale and high-profile data breaches in recent years. Historically, attacks were driven by financial gain, but attacks are increasingly motivated by espionage, whether for state or commercial purposes.[2] The changing nature of these attacks has generated significant concern from corporate decision-makers and policymakers. One of the most concerning elements of the cyber security landscape arises from the fact that many system vulnerabilities and their magnitudes are not known, meaning that it is generally infeasible for researchers and policymakers alike to bound the range of possible outcomes (see Figure 1).

Figure 1: Index of Cyber Security Threats, 2011-2014



Notes.—Source: Index of cyber security. The cyber security index is a sentiment-based measure of the risk to infrastructure from perceived cyber security threats (http://www.cybersecurityindex.org/). The survey is administered monthly to a cross-section of industry, government, and academic participants, and includes questions over threat levels from prospective attackers (e.g., groups), weapons (e.g., malware), targets (e.g., infrastructure), defense, and public perception.

Despite the increasing importance of cyber security, little is known about its effects on firm-level investment and other economic outcomes. Unfortunately, the lack of information has made it difficult for corporate and governmental decision-makers to determine the optimal allocation of both private and public funds towards information security or public policies that might bring some benefits consummerate with costs. The lack of information is further clouded by the fact that many popularly

[2] See Verizon's Data Breach Investigations Report (http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf).

cited prior analyses use either qualitative surveys or self-reported incidence reports, which are not necessarily representative of the underlying economic costs and/or firm-level behavior. These surveys are useful heuristics, and the efforts are laudable, but they are limited. The relationships are not micro-founded in any theories about organizational dynamics, nor are the implied cost estimates grounded in statistical theory. These surveys also tend to suffer from sampling and methodological problems.

Unfortunately, there has not been any serious causal analysis of the relationship between financial and cyber security outcomes. Those studies that do exist, and contain some measurements of financial information, tend to focus exclusively on stock prices, rather than broader and more long-run measures of firm outcomes. Since stock prices are only useful metrics of firm performance when markets are able to capitalize information into prices, they may be not be very informative since uncertainty over the ramifications of cyber risk is high (e.g., Figure 1) and they often takes many years to fully materialize.

We document and characterize two major empirical challenges to statistical inference. The first challenge is unobserved firm heterogeneity. On one hand, larger and more productive companies might be more likely to be targets of information security incidents because attackers have more to gain through a successful attack. On the other hand, larger and more productive companies may also tend to have better security since they have better management and more investments in information technology, which are likely inputs towards information security. The magnitude of these two competing channels will determine the direction of the bias. The second challenge is sample selection. If not all cyber breaches are reported, and firms are less likely to report breaches during quarters or years when their profits and productivity are lower, then estimates of cyber breaches will be biased towards zero.

The primary contribution of this paper is to bring new evidence to bear on the economics of cybersecurity by producing and analyzing the first panel database containing cyber and financial outcomes at the firm-level. Our study combines data on publicly traded firms from all three public information security incident databases: the Privacy Rights Clearinghouse database (PRCD), the VERIS Community Database ("Veris"), and the US Department of Health and Human Services (HHS). In each of these databases, we identify publicly-traded firms in these datasets and match them with their publicly available financial statements accessible through Compustat. Our main solution to unobserved firm heterogeneity is the inclusion of relevant financial variables (e.g., number of employees), which proxies for firm-specific characteristics that are correlated with unobserved productivity both in the cross-section and over time. We also present results using a fixed effects estimator, which removes time-invariant sources of variation across firms by exploiting only the within-firm changes in firm and information security outcomes.

Using our newly constructed database, we identify two main limitations of the publicly available data. In our Veris and PRC samples, there is zero correlation between information security incidents and/or other cyber outcomes (e.g., fraud) and various financial outcomes at the firm-level. The zero correlation exists with or without firm fixed effects. We juxtapose these results with analogous regression models from the HHS, which provides breach incidents for healthcare companies. Healthcare

is the industry most targeted by cyber attacks and contains cleaner reporting records, creating a unique laboratory for us to further test these relationships.[3]

With this alternative sample, we do find negative correlations between financial outcomes and cyber breaches with our preferred estimate suggesting that a 1% rise in breaches is associated with a 0.17% decline in cash on hand. While we believe that the coefficient is not fully econometrically identified, we clearly show that even comparable data sources generate strikingly different results. Our interpretation of the evidence is that these differences do not reflect differences in the actual ramifications of cyber incidents, but rather the limitations of each specific dataset.

Our paper is closely related with a broader strain of research on the economics of privacy and information technology, recently surveyed by Grossklags, Jens et al. (2007). Most closely related to our paper is event study literature that infers the impact of cyber breaches on stock prices. For example, Campbell, Katherine et al. (2003) found a statistically significant adverse effect among breaches involving unauthorized, confidential data, but no effect when the data was not confidental. This result suggests that the type of information matters greatly in understanding the economic costs; not all records are perfect substitutes---some impose greater costs on firms than others. Looking specifically at information security breaches, Cavusoglu, Huseyin et al. (2004) found that announcing such an incident is negatively associated with the market value of the announcing firm, though the bulk of the decline is regained after two days. Kannan, Karthik et al. (2007) later found that firms do not earn significantly negative abnormal returns in the long-term due to information security incidents. While these studies make important strides in identifying the presence (or lack thereof) of short-run financial effects on firms, but they do not focus on long-run and dynamic considerations.

2. Literature Review

A. Economics of Information Security

Information technology has fueled economic growth over the past three deacdes at all levels: at the industry-level (Stiroh, 2002), at the firm-level (Bloom, Nicholas et al., 2012; Bresnahan, Timothy et al., 2002), and at the individual-level (Aral, Sinan et al., 2009). Information technology (IT) has helped promote global integration (Van Alystne, Marshall W. et al., 2005), greater firm-level innovation, (Tambe, Prasana et al., 2012), increased product variety (Brynjolfsson, Erik et al., 2011), and lower costs of doing routine tasks (Autor, David H. et al., 2003). At the same time, information security has lagged. There are many systemic vulnerabilities at the infrastructure, logical, and software layers that create risks for the firms and individuals who use and rely on these technologies.

The impact of these risks on firms can vary widely. Within an instant, firms can completely lose public trust in their service offerings if, for example, customers' private information held by the firm is exfiltrated and publicly released. In addition to the effects on any individual firm, cyber security also has features of a public good in that investment in cyber security by one firm can have positive externalities on the security of other firms (similar to the way that vaccines work at a society-level). Due to network complementarities, say between a bank and an electric utility, the breach of one entity has the potential

[3] http://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#2e911fca3954

to open vulnerabilities in another, which in turn also has the potential to wreak havoc and financial distress on all entities.

Lack of investment in information security over the past two decades is influenced by a number of market failures.[4] Information security is not a pure private good (Grossklags, Jens et al., 2007). It conveys externalities since a network is often only as strong as its weakest link. Even within a single organization, one department might have strong defense capabilities, but another may have obvious vulnerabilities. To the extent that organizational productivity depends on their joint production, then the more vulnerable department may put the entire company at risk. In a related vein, moral hazard arises from information asymmetries. The losses from information security failures do not entirely fall on the entity whose information security has failed. For instance, the time losses due to the breach of payment card data held by a large retailer fall on the customers, who must spend time replacing their cards, and the banks, which have got to go to the lengths of replace all the breached cards.

Moral hazard also manifests itself between firms. Since software and hardware makers have a strong incentive to rush their products to market in order to obtain a first mover advantage against their rivals, products are often shipped out with vulnerabilities and are only patched on an ad-hoc manner in the future. While forward looking firms might anticipate that intermediaries have these incentives to rush their products to the market, there is a limited market for "quality testing" the vulnerabilities of software and hardware in a cost-effective manner. These features of cyber security highlight the importance of sound and credible federal intervention.

Unfortunately, there is currently too little empirical content to ground decision-making. For instance, in late 2014, Sony Pictures Entertainment suffered a cyber-attack. The company reported that half of their network was destroyed and hundreds of gigabytes of employee files and emails were stolen.[5] Yet, in their subsequent earnings reports, Sony only quoted expenses of US$15 million for investigation and remediation following the attack.[6] In later reports, including out of pocket costs, this figure rose to $41 million.[7] Either way, this represents a fraction of the firm's annual revenues and much of which was reimbursed subsequently through insurance. On one hand, these direct expense estimates potentially omit integral direct costs imposed on other related victims (e.g., employees whose emails were subsequently dumped on the Internet) and the indirect costs (e.g., lower goodwill with consumers and investors). On the other hand, many of the current estimates of cyber crime are based on restrictive assumptions and extrapolations, generating large estimates of the aggregate costs ranging between $445 billion (CSIS, 2014) and $1 trillion (McAfee, 2011). These incidents naturally prompt questions about the return on investment in cyber security defenses and infrastructure. Some research suggests

---

[4] Knight, Rory F. et al. (1996) found that firms are affected by catastrophies depending on how well prepared and how well they respond to a catastrophe. Those that responded to a catastrophe poorly ('non-recoverers') experienced an average loss in shareholder value of 5% while those who responded well ('recoverers') received an average increase of 11% in shareholder. These effects were found to persist over time. It is unclear though whether this would hold more narrowly for information security incidents given the wide scope of the study. Knight, Rory F. et al. (1996) fits into the broader class of papers using event studies to examine shocks to stock prices due to information security incidents. We address concerns about differences across industries by including industry fixed effects, on top of other financial firm-level covariates (e.g., employment or capital).

[5] http://fortune.com/sony-hack-part-1/

[6] http://www.sony.net/SonyInfo/IR/library/fr/150204_sony.pdf

[7] http://fortune.com/sony-hack-final-part/

that information security countermeasures might be most cost-effective with an approximate 17-21% return on investment (Soo Hoo, 2001), but serious improvements are required to understake robust econometric analyses relating to information security.

Where there is evidence, the research undertaken has not led to solid conclusions. One study found that there is a stable power-law tail distribution of personal identity losses per information security incident (Maillart, Thomas et al., 2010). Yet, Edwards, Benjamin et al. (2015) found that neither the severity nor frequency of data breaches has increased over the past decade. Instead, those incidences that have attracted attention can be explained by the heavy-tailed statistical distributions underlying the dataset. Clearly, understanding whether the increasing attention towards cyber security is a function of the salience versus substance is an important issue for disciplining regulation and policy. The role of privacy in cyber security further complicates analysis by making it more costly to store and secure information, let alone using it for empirical analysis (Wheatley, Spencer et al., 2016).

B. Methods for Estimating Costs

The prevailing approach for estimating the costs of information security incidents in the literature is to gather estimated costs and number of breaches from a cross-section of companies. Many of these analyses are implemented using either qualitative surveys (e.g. those conducted by the Ponemon Institute) or self-reported incidence reports. The survey responses provide information on the estimated total breach damage and the number of records breached such that the cost per record is obtained by taking the ratio between the two. Verizon (2015) criticizes estimates by Ponemon (2014) by using their collected data on a restriction of the overall sample consisting of breaches with under 100,000 records breached. While they obtain a 58 cent average cost of record breached under this sample restriction, they obtain $201 per record breached from the full sample. Verizon (2015) argues that they obtain a better fit, measured by a simple R-squared statistic.

These surveys are useful heuristics, and the efforts are laudable, but they are limited by a number of factors. The relationships are not micro-founded in any theories about organizational dynamics, nor are the implied cost estimates grounded in any theory of statistical inferences. By averaging highly heterogeneous breaches and estimated costs together, these studies are challenged by fundamental identification problems arising from omitted variables bias. Specifically, these approaches fail to not only control for time-invariant sources of heterogeneity across companies, but also basic time-varying differences, such as employment and assets.

Deferring to simple measures of overall fit from the R-squared in order to evaluate the quality of the model is not a fruitful endeavor. Given that there are significant cross-sectional differences in productivity in even narrowly defined industries (Syverson, 2004), and economists still are trying to understand the factors underlying the distribution of productivity (Syverson, 2011), comparing statistical models on information security failure costs based on relative R-squared fits is a deceptive endeavor.

Many studies use self-reported surveys and suffer from a variety of sampling and methodological problems (Herley, Cormac et al., 2011). For instance, self-reported incidence reports are produced annually by the Federal Bureau of Investigation's Internet Crime Compaint Center. These reports provide information on the number of incidents of various forms of Internet-related crimes, the demographics of those who reported being victim of an Internet-related crime and the losses due to the crime as reported by the person or company in question. There are many short-comings of the

methodology used in these reports. The lack of representativeness in the sampling results, owing to the fact that only those companies or people who report the crime are included in the sample, leads to non-reprentative sampling of the losses in aggregate. The true extent of the incidence of the Internet-related crimes and their financial impact on the average firm or individual is thus not clear. Moreover, the method for estimating the losses incurred by each person or company are not provided, and likely differ across the reporting companies, again leading to undreliable total loss estimates (Florencio, Dinei et al., 2011).

Some studies use an accounting approach to measure the economic costs of security incidents. They assign values to particular activities affected by the breach and publicly report the aggregate quantities (Anderson, Ross et al., 2014). The wide variance of the estimates of the global cost of cyber-crime in these studies points to the inaccuracy of the methods used to make the estimates. One commonly cited paper by national security leaders claims global costs amounting to $445 billion while another, previously cited by the President of the United States, suggests over $1 trillion (CSIS, 2014; McAfee, 2011). These studies too suffer from similar methodolgical issues as those using self-reported surveys, such as the exclusion of firms that have suffered a security incident but are not aware of it. They also use models that are not based upon optimizing economic behavior. Rather, they make unrealistic extrapolations of total costs based on accounting cost estimates at a firm level multiplied by the estimated total number of firms in the economy.

3. Institutional Context and Measurement

A. Data Sources

For this study, we gathered data from three sources: the Privacy Rights Clearinghouse database (PRCD), the VERIS Community Database ("Veris") and the U.S. Department of Health and Human Services (HHS). These datasets document the incidence of information security failures based on geographic location and organizational entity.[8] We extracted all relevant variables and manually matched entries for publicly-listed firms in these datasets with their publicly-available financials through Wharton's Data Research Services Compustat ('Compustat').

The PRCD is compiled by a nonprofit corporation and contains records of breaches starting from 2005 with 4,564 separate breach incidents as of November 2015. The Veris data is similarly compiled and contains records of breaches starting from roughly 2005 (although coverage is very weak). While the combined PRCD/Veris data contains roughly 5,233 incidents as of January 2016, only 173 are breaches for publicly traded companies (67 coming from Veris and 143 coming from PRCD). The vast majority of the variables in Veris are also missing, making the number of records breached the only reliable measurement for our purposes. The U.S. Department of Heath and Human Services catalogues all notifications of breaches of unsecured protected health information for incidents affecting 500 or more individuals. While the database contains 1,561 unique entries as of July 2016, only 113 are

[8] See www.privacyrights.org/data-breach and http://veriscommunity.net/.

breaches for publicly traded companies that we are able to match. Though these datasets are the most extensive publicly available data, they cover only a small fraction of total information security incidents.[9]

For the PRCD, we observe the name of the company breached, the date that the breach was made public, the total records stolen, the ascribed cause of the breach (one of eight categories: unintended disclosure, hacking or malware, payment card fraud, insider, physical loss, portable device, stationary device, unknown or other) and the firm's industry (one of seven categories: nonprofit, healthcare and medical providers, government and military, educational institutions, businesses - retail/merchant, businesses - financial and insurance services, businesses - other).[10]

For the Veris dataset, we observe the name of the victim company that has sustained an information security failure, the year in which the incident took place, the assets compromised due to the information security failure (confidentiality/possession, integrity/authenticity or availability/utility), and the victim firm's primary industry (using NAICS code). The Veris dataset includes information security incidents beyond simply data breaches, including incidents such as denial of service attacks, 'crimeware' and privilege misuse (among many others).

For the HHS dataset, we observe the name of the breached entity, breach submission date, the number of affected individuals, the type of breach (hacking/IT incident, improper disposal, loss, theft, unauthorized access/disclosure, unknown or other), the location of the breach (desktop computer, electronic medical record, email, laptop, network server, other portable electronic device, paper/films, or other), the type of covered entity (health plan, heathcare clearing house or healthcare provider), the state in which the entity is located, whether a business associate was present, and a description of each incident. The HHS data offer an improved probability of detecting potential relationships, relative PRCD or Veris, since the reporting is cleaner and contains less measurement error. The healthcare sector has largely modernized and the publicly traded companies in our data generally have integrated technology into their services, providing fewer opportunities for mis-reporting.

While many of the breaches from PRCD are descriptive for government departments and educational institutions, we restrict our analysis to publicly listed companies in order to match them with financial records from the Compustat database between 2005-2015. We hand-code each company to have a unique identifier between the PRCD, Veris and Compustat databases. This brings our sample down to 1,100 observations in the PRCD and 1,723 in Veris. Since only the breaches involving some loss of confidential information contain lost records, we set observations involving other types of breaches to zero. Observations are distinct from firms; there are only 286 in the PRCD and 187 in Veris. The remainder of the observations are set to zero under the assumption that, if firms did not report a breach during this time period, then they had zero breaches.

A final distinction that is important to point out is that there are many years that a company may not be observed in either database even if they are observed once. For example, a firm might incur a breach that is publicly reported in 2012, but they are not observed in 2010 in the cyber databases. Does

[9] Kuypers, Marshall A. et al. (2016) examine detailed micro-data at a single firm containing over 60,000 cyber security entries---several times more cyber incidents than the PRCD and Veris datasets put together.

[10] There are a few entries that include multiple firms, which we omit from the analysis since there is no way to reasonably infer the fraction of the reported total accounts breached that correspond to each of the included firms.

this mean that they had no cyber incidents in 2010? Or, does it mean that they did not have a large enough incident that led to public recognition? There is a potentially major selection problem here---years a firm is not observed might not be "true" zeros in the sense that they had breaches that were simply not reported. We, therefore, present results under the "pooled" and "partial" samples and discuss both sets of results. We generally find better traction when working with the "partial" samples, indicating that the pooled sample suffers from attenuation bias due to measurement error in reported breaches.

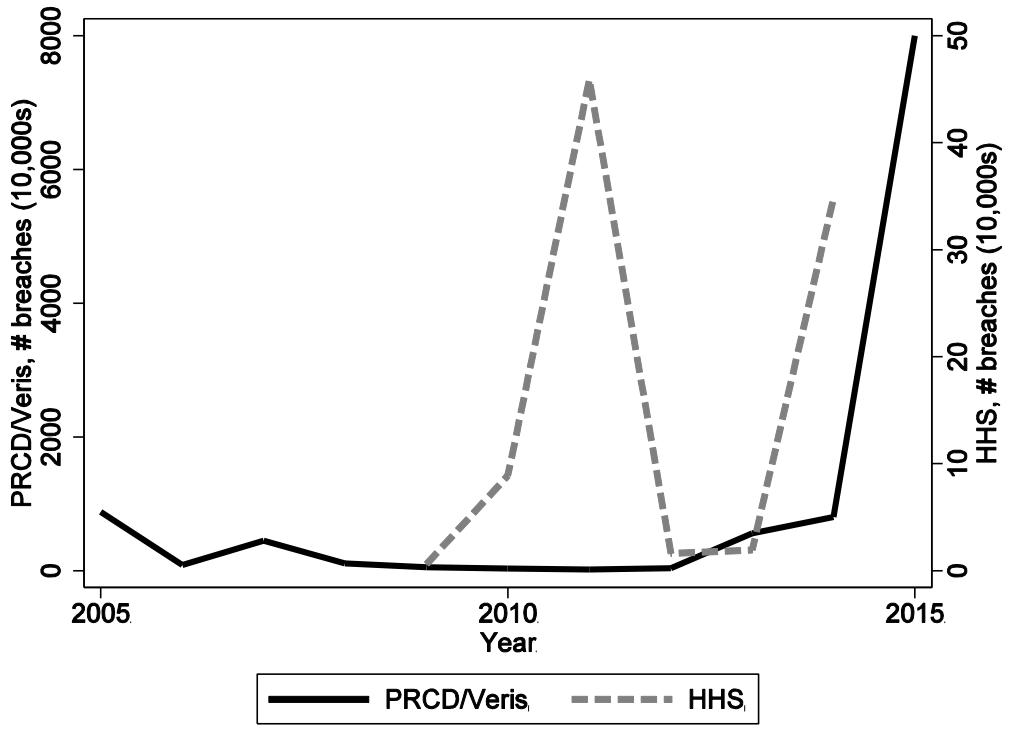
B. Descriptive Statistics

We turn towards examining various descriptive features of our data. We begin by plotting annual breaches in the combined PRCD/Veris and HHS databases (see the first panel of Figure [fig:cyber motivation]). One immediate observation is that the number of records breached in each of the databases is not smooth; there are large year-to-year swings that are based on, for example, one or just a few very large security incidents. For example, Anthem Inc. had several large breaches in the sample: 1,023,209 records in 2010 and 839,711 records in 2014. Even though the year-to-year averages seem to represent relatively random fluctuations---partially because of sample selection issues, which we discuss later---the probability of facing a breach at a firm-level is endogenous. We also plot the distribution of breaches (see the second panel of Figure [fig:cyber motivation]). Interestingly, the distribution of breaches is quite different in these two samples, which further reflects issues of comparability that we return to later.

To investigate the potential differences across the different samples, Table 1 compares firms from PRCD, Veris, HHS, and the pooled Compustat samples for all financially linked data and breaches at an annual frequency. While PRCD and Veris samples are relatively similar, they represent companies that are much larger than the average publicly traded company. For example, whereas assets are approximately $1,000 million in the pooled Compustat sample, they are approximately $6,000 million in PRCD and Veris. Not surprisingly, PRCD and Veris companies also tend to hold much greater quantities of cash by a factor of five. PRCD companies tend to hold a third more cash than their Veris counterparts. The average Compustat company also spends much less on R&D expenditures than the PRCD and Veris counterparts by a factor of eight. Finally, the average firm is much larger (measured through number of employees) in PRCD and Veris with an average of 68,000 employees versus 8,000 in the full Compustat sample. However, the firms in the HHS sample are all much larger with average assets of $33.2 million and sales of $23.1 million. Naturally, since these are healthcare companies, research and development is much larger, even relative to PRCD and Veris samples with an average of $40.7 million per year.[11]

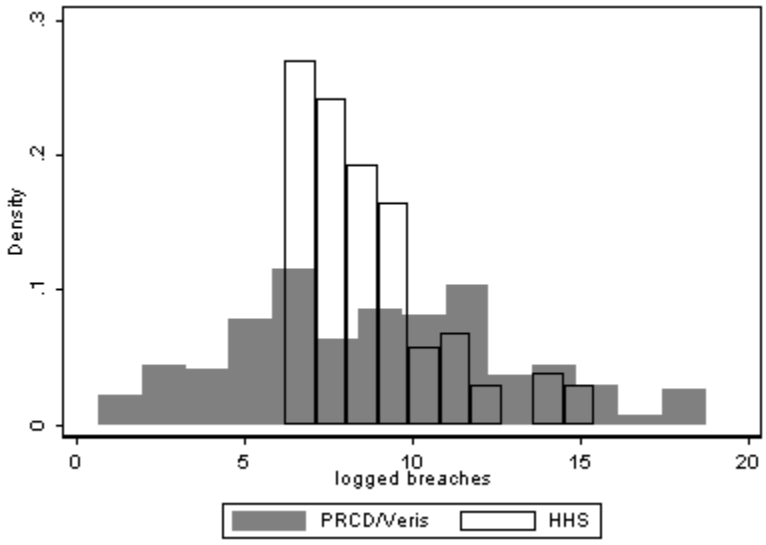
Figure 2: Records Breached (tens of thousands), 2005-2015

[11] These numbers are converted into annual frequencies by multiplying their quarterly rates by four.



Notes.--Sources: Privacy Rights Clearinghouse Database, Veris Community, and Department of Health and Human Services. The figure plots the mean annual number of breaches in tens of thousands restricted to the set of publicly traded companies in the corresponding databases.

Figure 3: Distribution of breaches, 2005-2015



Notes.--Sources: Privacy Rights Clearinghouse Database, Veris Community, and Department of Health and Human Services. The figure plots the mean annual number of breaches in tens of thousands restricted to the set of publicly traded companies in the corresponding databases.

Turning towards data breaches, the PRCD sample tends to have much weaker coverage than Veris at the earlier part of the sample (e.g., around 2005) with only an average of 25,700 records breached, compared to 258,097 in Veris.[12]

Moreover, the sample sizes are somewhat comparable: 2,144 observations in PRCD and 2,058 in Veris. Importantly, these sample sizes reflect an average across all years when an information security failure is reported and when one is not reported; in these latter instances, the records are replaced with a zero. Turning towards the latter 2011-2015 period, the PRCD sample also has lower average incidents (257,771 in PRCD versus 356,864 in Veris). Perhaps the most interesting observation is the skewness of the distribution of incidents: the standard deviation is 3,961,325 in PRCD and 5,884,047 in Veris, which is approximately a factor of over 16 relative to the mean. This can be explained by the wider range of possible incidents covered by the Veris dataset.

Turning towards the categories of breaches, PRCD and Veris contain different labels for the attacks. Out of the incidents reported in PRCD with labels on the type of attack, the number of incidents changes dramatically over the two periods. Over 2005-2010, the bulk of the incidents are due to portable losses (e.g., stolen laptop) whereas, over 2011-2015, the bulk of the incidents are due to hacks and insider threats. The Veris dataset contains three categories of potentially overlapping attacks that have some effect on the confidentiality of information, integrity of information, and/or availability of information (the so-called "CIA triad").[13] Confidentiality refers to the protection of information from disclosure to unathorized parties; integrity refers to protecting information from modification by unauthorized third-parties; and, availability refers to guaranteeing that authorized third-parties have access to the information when necessary. Out of the incidents in Veris, all of the publicly traded firms have at least some exposure of confidentiality, 27-44% affect integrity, and 25-31% have a detrimental effect on data availability (e.g., the attack impacted availability, or access, to information).

[INSERT TABLE "Descriptive Statistics" ABOUT HERE]

We examine how differences in data breaches look across different types of companies. Table 2 partitions the sample---restricted to the instances when a breach is observed---into different quantiles based on the number of employees and size of current assets. There is a strong positive relationship between the two: larger companies---regardless of how "large" is defined---also tend to have more records breached per data breach reported. We also document the differences in the type of attack. Larger companies tend to have about 12% reporting some type of cyber espionage, relative 4% and 7% among small and medium sized publicly traded companies. However, smaller companies tend to have slightly more credit card fraud and unambiguously more website breaches, reflecting the fact that they have a weaker technology infrastructure for dealing with basic types of cyber attacks.

---

[12] We omit the median, which is zero in each case. Of course, when the sample is restricted to observations with non-zero breaches (e.g., the records from PRCD/Veris/HHS that we do not fill in as zero when the companies are not observed in the dataset), the median is also non-zero. In PRCD/Veris, it is 6,850 records lost and, in HHS, it is 4,305 records breached. The distinction between breached and lost is ambiguously defined from our interpretation of these databases.

[13] http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/

[INSERT TABLE "Cyber Security Incidents, by Firm Size" ABOUT HERE]

We now restrict the sample to healthcare companies, which contains much more granularity over the type of attack, to understand the potential determinants of breaches through negative binomial regressions of the form

$$Breaches_{it} = \exp(\beta X_{it} + \rho BreachCharacteristics_{it} + u_{it}) \qquad [1]$$

where $Breaches$ denotes the number of breaches at firm i in quarter/year t and $\underline{u}$ is the overdispersion parameter, which adjusts the variance independently from the mean. We estimate Equation 1 using a negative binomial model due to the massive dispersion that is bundled into the error arising from the skewness of cyber security incidents; estimating it with, for example, least squares produces very noisy estimates. The regressions are implemented in two sets of samples. The first pools all years between 2009 and 2015 together, including those that the company is not observed in the HHS data (and thus assumed to have no breach). The second examines only those observations in periods where a cyber breach is observed.[14]

Table3 documents these results. Companies with greater assets tend to have greater cyber breaches, but those with greater sales and/or cash tend to have fewer cyber breaches. For example, a 1% rise in assets is associated with between a two to four increase in the number of records breached (with the exception of a less statistically precise estimate in column 2). Similarly, a 1% rise in sales is associated with between a -0.50 to -2.30 decline in the number of records breached. These financial outcomes indicate that larger companies (e.g., those with greater assets) might be bigger targets, but also that more productive companies (e.g., those with more sales) might be better equipped to defend against attacks.

The estimated coefficients on the victim indicators are much less straightforward to interpret since their signs differ dramatically between the two sample restrictions. Since there is little reason to suspect truncation of measurement error in the health care industry---since they tend to be high-technology companies and especially since these are publicly traded firms---we defer to the pooled sample. Most of the breaches tend to be those among associates or colleagues, whereas health plans and providers tend to occur half as frequently. Finally, the estimated coefficients on the type of attack indicate that theft is the most common form of cyber breaches, taking place almost twice as often as those that fall into the "other", "hacking" or "unauthorized use" categories.

We also considered negative binomial regressions with our PRCD/Veris samples. If we pool all firms together, we find a coefficient of -1.60 (p-value = 0.001) and 2.16 (p-value = 0.00) on logged assets and sales, respectively. (The coefficient on logged cashflow is statistically insignificant.) The estimates are very similar in the restricted ("partial") sample. While the coefficient on logged assets is similar, it is qualitatively different on logged sales. We do not have a parsimonious explanation for why, but one reason could be the nature of the breaches are very different in non-healthcare companies. That is, changes in sales might be spuriously associated with lost records in the general cross-section, but when records are lost in the healthcare sector sales takes a much greater and adverse turn since records are a salient measure of an individual's private medical history.

[14] Any value of α ("dispersion") above 1 tends to indicate over-dispersion.

4. Empirical Strategy

In our model, we consider regressions that relate firm outcomes, , with cyber security breaches through equations of the following form

$$\log(Y_{it}) = \beta X_{it} + \gamma \log(Breaches_{it}) + \phi_i + \lambda_t + \epsilon_{it} \qquad [2]$$

where X denote a vector of firm-level controls, and ϕ and λ denote fixed effects on firm and year. We also experiment with additional layers of fixed effects. Equation 2 provides a basic characterization of the association between cyber and firm outcomes through the estimated coefficient . We also consider regressions that relate firm outcomes with specific categories of cyber security incidents, in particular indicators for whether the attack constituted a breach in confidentality, integrity, or availability of information. An important advantage of these estimates is that they are conditional on a set of firm financial characteristics, which help control for omitted variables and selection.

Unfortunately, consistent identification of γ in Equation 2 requires that unobserved shocks to firm outcomes are uncorrelated with changes in cybersecurity outcomes. There are at least two plausible violations. The first identification concern is a static selection problem that arises from the fact that more productive firms might also be larger targets for cyber criminals---that is, because there is more to steal from these companies. It is also possible, however, that less productive firms are larger targets for cyber criminals---that is, because they are easier to breach. These two margins represent the marginal benefits and costs to cyber crime, requiring empirical evidence to shed light on the theoretically ambiguous effect. The second identification concern is a dynamic selection problem that arises from the fact that cyber breaches might respond to a rise in firm outcomes. That is, if a firm experiences a surge in sales or profitability, cyber criminals may respond by increasing their attacks against the company. While in theory we can address both concerns by including firm fixed effects to remove time-invariant heterogeneity across companies, in practice we found that fixed effects estimators failed due to a lack of variation. Our main identification strategy is to simplify condition on other relevant financial variables that proxy for factors that are correlated with omitted determinants of our residual and cyber breaches.

We also underscore the importance of functional form assumptions in these regressions. While functional form tends to be an innocuous issue, the distribution of cyber breaches is so heavily skewed that we are only able to generate traction in our models using logged breaches as the independent variable. We have used other functional forms, including polynomials and splines, none of which generated economically or statistically significant estimates. Splines may be an effective strategy, but they require sufficient numbers of observations within each partition of the distribution.

5. Results

We begin by estimating Equation 2 using a combination of the PRCD/Veris database, which contain cyber breach incidents spanning the entire economy. Table 4 documents these results. Although the financial variables, not surprisingly, have intuitive and reasonable interpretations, the coefficients on logged records breached are statistically and economically insignificant in every specification except the first, which represents the unconditional correlation between the logged records breached and logged firm outcome (revenue or cash). We subsequently examine specifications containing the firm-level

controls (column 2), industry fixed effects (column 3), the partial sample with industry fixed effects (e.g., only instances where the company is observed with a breach, column 4), and firm fixed effects (column 5).

[INSERT TABLE “Baseline Cyber Security Incidents and Firm Outcomes, Economy-wide” ABOUT HERE]

While lack of variation in the available data presents problems, it is not the sole problem. For example, when we implement a simple regression with controls, we still find a zero correlation between breaches and financial outcomes. To delve further into the potential phenomena at play, we now turn towards our alternative sample from the HHS. Table 5 documents these. We find two important facts. The first fact is that controlling for other firm characteristics, such as a firm's capital stock, qualitatively affects the point estimates on our logged breach variable. For example, when the dependent variable is breaches and no controls are included, we find that a 1% rise in breaches is associated with a 0.06% rise in cash. By contrast, our estimates suggest that 1 % rise in breaches is associated with a 0.17% decline in cash when we include property, plant, and equipment as a control. A similar story emerges when we examine the association between sales and intangible capital, although they are not statistically significant. The second fact is that including the years that the company does not appear in the cyber breach data---that is, in years they do not report breaches---we find highly economically and statistically insignificant estimates. We also omit additional specifications that contained firm fixed effects, but did not have enough variation to estimate any coefficients with precision.

[INSERT TABLE “Baseline Cyber Security Incidents and Firm Outcomes, Healthcare” ABOUT HERE]

We now turn to several other measures of cyber attacks, namely indicator variables for the type of attack within a given year. Table 5 document these results. Few of the conditional correlations are statistically significant. For example, a cyber attack that is considered espionage is associated with a 14 percent decline in revenues, but this effect is not statistically different from zero. In the case of “other” and “card fraud”, two of the estimates are statistically significant, but in the opposite direction. Our conclusion here is not that these estimates are credible, but rather that the data are deeply flawed.

[INSERT TABLE “Cyber Incident Type and Firm Outcomes” ABOUT HERE]

We finally turn towards regressions that distinguish among the different categories of cyber incidents, namely whether the breach constituted a violation of confidentiality, integrity, or availability of information. In theory, information security incidents categorized by their technical effects should matter for understanding the economic effects. Distinguishing among different categories of attacks is important since not all attacks have equal weight: some are more costly than others since some information is more important than others and certain information security incidents can either impair a firm's ability to properly function (e.g. denial of service attacks) or can destroy a firm's assets (e.g. wiper malware).

These results are documented in Table 6}. The results provide a slightly more optimistic interpretation of the data. Columns 1-6 (7-12) regress indicators for the category of the cyber attack on the firm's log cash flow (cost of goods sold) with two-digit industry and firm fixed effects, respectively. The results suggest that a breach in confidentiality is associated with a nearly 102% decline in cash flow, but the result is not statistically significant after controlling for firm fixed effects. Neither incidents that affect integrity nor availability have a statistically significant association with firm outcomes.

Interestingly, the coefficients associated with confidentiality are both significant when the dependent variable is cost of goods sold. In particular, incidents that compromise confidentiality are associated with a 21% decline in cost of goods sold, conditional on firm fixed effects, perhaps reflecting that firms may respond to cyber incidents by reducing their inventory and production line subsequent to a security failure. Broadly speaking, these results point towards the importance of heterogeneity in the type of cyber incident since crude measures of records lost treat all effects of information security failures as additively separable.

[INSERT TABLE "Cyber Incident Category and Firm Outcomes" ABOUT HERE]

6. Limitations

The data on which we have based our analysis is constrained in two ways. The first major constraint is the completeness of publicly available cybersecurity incident databases. Neither PRCD nor Veris contain the full universe---or anywhere near it---of attacks. In fact, it is likely that the public data represents only a very small fraction of overall attacks. To the extent that the missing observations and incomplete nature of the data is random, it will only produce larger standard errors. However, the companies that do not report, or those who do report simply a subset of the actual breaches that occurred, may do so systematically in ways that are correlated with their contemporaneous constraints and/or economic performance. Our results from the HHS sample are more reliable and likely driven by the fact that companies are required to report certain types of incidents under section 13402(e)(4) of the HITECH Act. This dataset is likely then to represent a more complete picture of the full universe of data breaches. With the European Union's Genreal Data Protection Regulation, which includes mandatory data breach notification rules, coming into effect in 2018 we hope this will provide a future data source with incidents across many industries.

We also are required to assume that records are additively separable. In other words, it imposes the assumption that each record breached or incident as an equal effect on the firm outcome. However, releasing confidential information about the CEO is much more likely to impact the firm value than releasing, or example, confidential information about entry-level workers.

The second major constraint is the limitations associated with restricting the sample to purely public traded firms. However, large publicly traded companies have many establishments, which increases the noise-to-signal ratio in causal inference since a cyber security incident might occur only at a single establishment, leaving the bulk of the firm unscathed. To the extent that security breaches affect the local establishment more than the overall firm, then focusing only on the large companies could add measurement error. Future analysis can match based on establishments using Dun and Bradstreet data, but the fact that our results were null on the Compustat panel of firmsraises the question of whether or not the PRCD or Veris datasets are even of any use for this purpose. A separate concern is that the cyber security incidents tend to reflect multiple sources of security failures. For example, an attack may involve not only lost records, but also fraud and a shock to the networks that bring company operations to a halt. While the solution is to simply condition on these different measures---that is, the continuous measure of records lost and the discrete measures of the type of attack---there is simply not enough within-firm variation in the available data to separately identify the coefficients, let alone on any single coefficient.

7. Conclusion

Despite the increasing concerns and perceived damages associated with emerging cyber security incidents, there is no causal evidence on their potential long-run economic effects. The only available studies that speculate over the costs use either survey data---which ask companies about their subjective view of the costs---or aggregate data---which tend to involve extrapolations of technical costs onto large populations. We address this empirical gap by producing the first panel dataset containing both financial and cyber security incident information at a firm-level. By manually matching companies appearing in the Veris, PRCD, and the US Department of Health and Human Services (HHS) publicly reported breach databases with Compustat, we constructed a panel of companies observed between 2005-2015. The dataset enables us to provide, to our knowledge, the first descriptive evidence to date on the operational and financial health (e.g., cash flow and assets) of companies joint with their histories of cyber incidents.

We began by documenting several stylized facts about cyber security incidents and firm outcomes. Firms with larger breaches tend to have greater assets, sales, and employment. One potential concern, however, is that unobserved differences across companies could bias our results. For example, larger companies might be bigger cyber targets. However, they may also be more equipped to handle security incidents. We examine these concerns by controlling for correlated firm characteristics and exploiting longitudinal variation---that is, by comparing changes in cybersecurity and financial outcomes within the same company over time.

Using purely the PRCD/Veris, our results suggests that cyber incidents are not related with firm financial outcomes regardless of whether we control for other observable characteristics (e.g., employment). And yet, our results from the US Department of Health and Human Services (HHS), containing breaches for a subset of healthcare companies suggest that a 1% rise of cyber breaches is associated with a 0.17% decline in productivity, which is very large given comparable estimates in the broader economics productivity literature (Syverson, 2011). Interestingly, given that the HHS sample is almost as large as the merged PRCD/Veris sample, despite the fact that it is only a narrow subset of the economy, pointed us towards an important sample selection problem---companies do not report all their cyber breaches and, given our contrasting estimates in the two datasets, their mis-reporting must be correlated with the firm's contemporaneous financial health. For example, companies may have fewer incentives to report their incidents when they are doing poorly, meaning we are less likely to observe breaches precisely when it might matter most. While our estimates remain noisy in most cases, our overall results point towards serious empirical challenges for the emerging literature on information security given the lack of comparability among datasets and sample selection issues.

Decision-makers in firms and policy makers in governments require evidence in order to make well-informed decisions regarding information security investments. However, the requisite evidence is not available for econometric analysis given the data deficiencies identified in this paper. Mandatory breach notification rules, such as those coming into effect in the EU in 2018, might provide future data sources that remedy these deficiencies. Until that point, data deficiencies will persist and, in turn, effective investment decision-making for information security will continue to be hampered.

References

Anderson, R., C. Barton, R. Bohme, R. Clayton, M. J. van Eeten, M. Levi, T. Moore, and S. Savage (2014): "Measuring the costs of cybercrime," Working paper.

Aral, S., E. Brynjolfsson, and M. W. Van Alystne (2009): "Information, technology, and information worker productivity," Information Systems Research, 23, 849–867.

Autor, D. H., F. Levy, and R. J. Murnane (2003): "The skill content of recent technological change: An empirical exploration," Quarterly Journal of Economics, 118, 1279–1333.

Bloom, N., R. Sadun, and J. Van Reenen (2012): "Americans do IT better: US multinationals and the productivity miracle," American Economic Review, 102, 167–201.

Bresnahan, T., E. Brynjolfsson, and L. Hitt (2002): "Information technology, workplace organization and the demand for skilled labor: firm-level evidence," Quarterly Journal of Economics, 117, 339–376.

Brynjolfsson, E., Y. Hu, and D. Simester (2011): "Goodbye Pareto Principle, Hello Long Tail: The Effect of Search

Costs on the Concentration of Product Sale," Management Science, 57, 1373–1386.

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou (2003): "The economic cost of publicly announced information

security breaches: Empirical evidence from the stock market," Journal of Computer Security, 1, 431–448.

Cavusoglu, H., B. Mishra, and S. Raghunathan (2004): "The effect of internet security breach announcements on

market value: Capital market reactions for breached firms and internet security developers," International Journal of

Electronic Commerice, 9, 69–104.

CSIS (2014): "Net losses: Estimating the global cost of cybercrime," Center for Strategic and International Studies.

Edwards, B., S. Hofmeyr, and S. Forrest (2015): "Hype and heavy tails: A closer look at data breches," Workshop on

Economics of Information Security.

Florencio, D. and C. Herley (2011): "Where do all the attacks go?" Workshop on Economics of Information Security.

Grossklags, J. and A. Acquisti (2007): "When 25 cents is too much: An experiment on willingnes to sell and willingness to protect information," Workshop on the Economics of Information Security. Herley, C. and D. Florencio (2011): "Sex, lies and cyber-crime surveys," Microsoft Research.

Kannan, K., J. Rees, and S. Sridhar (2007): "Market reactions to information security breach announcements: An empirical analysis," International Journal of Electronic Commerice, 12, 69–91.

Knight, R. F. and D. J. Pretty (1996): “The impact of catastrophes on shareholder value,” Oxford Executive Research Briefings, Sedgwick Group.

Kuypers, M. A., T. Maillart, and E. Pate-Cornell (2016): “An empirical analysis of cyber security incidents at a large organization,” Working paper.

Maillart, T. and D. Sornette (2010): “Heavy-tailed distribution of cyber-risks,” European Physical Journal B, 75, 357–364.

McAfee (2011): “Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency,” McAfee.

Ponemon, L. (2014): “2014 Cost of data breach study: Global analysis,” Ponemon Institute.

Soo Hoo, K. (2001): “Return on securing investment: Calculating the security investment equation,” Secure Business Quarterly.

Stiroh, K. J. (2002): “Information technology and the U.S. productivity revival: What do the industry data say?” American Economic Review, 92, 1559–1576.

Syverson, C. (2004): “Market Structure and Productivity: A Concrete Example,” Journal of Political Economy, 112, 1181–1222.

——— (2011): “What determines productivity?” Journal of Economic Literature, 49, 326–365.

Tambe, P., L. Hitt, and E. Brynjolfsson (2012): “The Extroverted Firm: How External Information Practices Affect Innovation and Productivity,” Management Science, 58, 843–859.

Van Alystne, M. W. and E. Brynjolfsson (2005): “Global village or cyberbalkans: Modeling and measuring the integration of electronic communities,” Management Science, 51, 851–868.

Verizon (2015): “2015 Data breach investigations report,” VERIS Community Group.

Wheatley, S., T. Maillart, and D. Sornette (2016): “The extreme risk of personal data breaches and the erosion of privacy,” European Physical Journal B, 89.

Global Digital Futures Policy Forum 2016: Issues Brief

Panel 4B: On Notice: The Coming Transformation of Key Economic Sectors

By Joah Sapphire

Introduction

Several vital economic sectors are currently undergoing significant disruption as a result of the advancement of digital technologies over the past decade. The emergence of digital technologies coincides with the convergence of smaller and faster chips embedded with sensors and actuators that are underpinning a multitude of devices. These devices are sending and receiving huge amounts of data over the high speed, global Internet. The storage and analytics of that data support limitless solutions and applications. Taken together this convergence is often referred to 'the Internet of Things (IoT)' and provides the backdrop for the next industrial revolution.

The financial sector faces the growth of Bitcoin and other cryptocurrencies and is now exploring adopting the underlying blockchains technology to gain efficiencies in their own operations. Automotives are rapidly incorporating sensors, artificial intelligence and data-driven operations in an attempt to develop autonomous vehicle solutions. The recent 'uberization' of several markets (e.g. hotels, taxis) is now moving into logistics.

Just as with the first industrial revolution, when governments were slow to react in understanding how to regulate international commerce driven by new technology, today the digitization of our economy is presenting a new set of policy challenges that maybe the most complex we have ever faced. While it is impossible to capture the multitude of issues surrounding this change, an examination of the impending policy needs presented by cryptocurrencies, blockchains, autonomous vehicles and urban transportation can serve to offer some important insights for the coming transformation of key economic sectors.

Problem Statement

The digitization of cryptography has given rise to the advent of cryptocurrencies and blockchains. The ability to transact on the internet in a simple and anonymous manner is creating new difficulties for policy makers and regulators that were never before imagined. With smart phones gaining prevalence across every corner of the globe how should governments balance allowing individuals to benefit from this technology through new ways to transact with one another while maintaining a consistent rule of law to control fraud and abuse? The stability of blockchains offers new ways to organize transactions and relationships but what mechanisms are in place to ensure the proper accounting of this new platform? All of these issues are important discussion points as connected devices become the common platforms for transacting in the global economy.

The development of autonomous vehicles has attracted huge investment from global automotive companies, auto parts suppliers and diverse technology companies that are new entrants in the automotive sector. While autonomous vehicles offer a tremendous profit opportunity, they present a multitude of policy challenges, with perhaps the greatest being how to regulate safety when the driver is now the vehicle. Governments have a responsibility to maintain the safety of the public especially on the roadways. In the case of autonomous vehicles and other emerging robotic devices how can the safety of the owner, user and general public be preserved when there is no human in the loop? Autonomous vehicles represent an immediate challenge to our current safety regulatory regime and that offers the opportunity for a demanding discussion of current international governmental approaches.

Finally, so-called sharing economy companies are very visibly disrupting numerous industries from hospitality to mobility. Urban transportation has experienced one of the fastest transformations and governments at all levels are facing new challenges as Uber, Lyft and others gain a greater share of markets. Ride sharing is quickly evolving into new logistics solutions and policy challenges around labor relations and liability among others are now front and center, requiring governments to adapt to keep pace.

Cryptocurrencies and Blockchains

Since the public release of Bitcoin in 2009, governments have worked vigorously to develop rules and regulations to govern this new way to transact. However, there is still great divergence between how different governmental organizations and agencies define and consider cryptocurrencies and blockchains.

The initial efforts aimed at users of cryptocurrencies highlight four distinct policy issues, relating to the definition of a cryptocurrency, that have broad and substantial fiscal, monetary and economic implications (for more detailed explanation of the definitions below, see Appendix 1):

- From the users perspective, the Financial Action Task Force (FATF) defines crytocurrencies as a **currency** so, for tax purposes, should profits from sales be taxed as ordinary income? [1]
- Or is it a capital **asset,** following the Internal Revenue Service (IRS) definition, and thus gains and losses should be subject to capital gains tax rates and losses should be used to offset other gains?[2]
- Could certain cryptocurrencies meet the '*Howey'* test and thus be treated as a **security**, implying treatment under federal securities laws and oversight by the Securities and Exchange Commission (SEC) in the U.S.?[3]
- Finally, do cryptocurrencies meet the U.S. Commodity Exchange Act's definition of a **commodity**, implying that that mining Bitcoin should be taxed in another form such as royalties on mineral rights?[4]

---

[1] FATF (2014), "Virtual Currencies Key Definitions and Potential AML/CFT Risks", available from: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, (accessed 4/12/16)

[2] IRS (2014), "IRS Virtual Currency Guidance:", available from: https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance, (accessed 4/12/16)

[3] U.S. Supreme Court, SEC v. Howey Co., 328 U.S. 293 (1946), available from: https://supreme.justia.com/cases/federal/us/328/293/case.html, (accessed 4/12/16)

Without proper policies in place the ambiguity of the treatment of cryptocurrencies impacts all of the actors in this sector from exchangers to miners of virtual currency. This lack of clarity limits that broad international adoption of cryptocurrencies.

At the same time, this also enables the potential for use of cryptocurrencies to support crime and tax evasion. Anti-money laundering and know your customer rules must now be applied to virtual currency. From a global policy perspective, are there sufficient regulatory bodies in place to ensure that cryptocurrencies are not being used to finance terrorism? Should these entities be satisfied with self-regulation by the financial industry or do governments need to step in the ensure that this new ability to transact is not exploiting weaknesses in the global payment system?

Cryptocurrencies provide the ability to transact. This differs from the underlying blockchains, which supports the shared ledger. The Australian Stock Exchange (ASX) in January of 2016 announced it was implementing a blockchain solution for equity trade processing. The new distributed ledger could reduce administrative costs and increase the efficiency of ASX's trading system. This is one of the first commercial applications of blockchains and many other finance entities are exploring the adoption of this new technology. Listed equity stock trading is a highly regulated market. Trading must be harmonized across the entire globe to ensure stable pricing and execution. Has there been enough testing of blockchains to ensure it is ready to go live? Who would be liable in the event of an incident and according to what standards? Numerous questions must be quickly studied and addressed.

Autonomous Vehicles

The United States Department of Transportation (USDOT) National Highway Traffic Safety Administration (NHTSA) defines vehicle automation as having five levels.[5] While each level of vehicle automation has numerous policy issues, this discussion will involve Level 4 or Full Self-Driving Automation. A Level 4 vehicle is designed to perform all safety critical driving functions and monitor roadway conditions for an entire trip. Such a design anticipates that the driver will provide destination or navigation input, but is not expected to be available for control at any time during the trip.[6] Governments have very recently ramped up discussions of how to approach this innovation.

In February of 2015, the United Nations Economic Commission for Europe (UNECE) was the first international body to discuss international regulatory steps concerning autonomous vehicles. Under the auspices of the World Forum for harmonization of vehicle regulations, the UNECE

---

[4] Commodity Futures Trading Commission (CFTC) (2015), Docket No. 15-29, Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, available from: https://supreme.justia.com/cases/federal/us/328/293/case.html, (accessed 4/12/16)

[5] No Automation (Level 0), Function Specific Automation (Level 1), Combined Function Automation (Level 2), Limited Self-Driving Automation (Level 3), and Full Self-Driving Automation (Level 4). For full definitions of each level of automation please see Appendix 2.

[6] NHTSA (2013), "Preliminary Statement of Policy Concerning Automated Vehicles Available", available from: http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf, (accessed 4/12/16)

Working Party on Brakes and Running Gear reviewed proposals covering semi-automated driving functions to pave the way for more highly-automated vehicles.[7]

The United States (US), United Kingdom (UK) and Japan among others have held hearings to discuss Level 4 vehicles but thus far have not enacted any new policies specifically governing autonomous vehicles. Within the US, at the state level, California, Michigan, Florida, Nevada, Tennessee and Washington D.C. have enacted legislation allowing limited driverless vehicle testing on public roadways.[8]

It is clear that policy makers are struggling with the best approach to address this new technology. The only approach that has been tried thus far is offering testing in controlled environments. Many technology companies feel this is insufficient because autonomous vehicles need to learn from real world environments. In the US, major autonomous vehicle players are increasingly growing frustrated with inaction at the federal level and complaining that US states are enacting a patchwork of laws that are not supportive of the commercialization of Level 4 vehicles.

In general, national or central governments need to update, establish and enforce policies and regulations around safety, privacy, data sharing, cybersecurity, manufacturing, vehicle design, infrastructure and data communications related to autonomous vehicles to enable state or provincial governments to then further tailor rules that meet distinct local needs.

- At the national level policy challenges include revising vehicle equipment requirements such as steering systems, braking systems, visual aids (side and rearview mirrors), seatbelts, and airbags, just to name a few. All of these current equipment specifications will have to be modified for Level 4 vehicles that use GPS, LiDAR[9] and radar for situational awareness.
- Roadway infrastructure requirements need to be revised in terms of signage and road striping for autonomous perception.
- In terms of liability does a human need to be in the loop? Should there be a human driver at all times or is there a need to require a human be available to override an autonomous vehicle system. If a human is not in the loop where does liability reside? With the vehicle owner? With the manufacturer? What standards or instructions should be required of the decision making of a Level 4 vehicle on the public roadways to ensure safety of the public?

At the state, provincial or local level policy challenges include vehicle permitting, infractions and infrastructure. With Level 4 vehicles, human error should be drastically reduced. This changes the paradigm for speeding tickets, traffic infractions and drunk driving laws, which are all administered at the state or local level. Other considerations include parking tickets,

---

[7] UNECE (2015), "UNECE to discuss first international regulatory steps concerning automated-driving", available from: http://www.unece.org/info/media/presscurrent-press-h/transport/2015/unece-to-discuss-first-international-regulatory-steps-concerning-automated-driving/unece-to-discuss-first-international-regulatory-steps-concerning-automated-driving.html, (accessed 4/12/16)

[8] Gabriel Weiner and Bryant Walker Smith, "Automated Driving: Legislative and Regulatory Action", available from http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action, (accessed 4/12/16)

[9] An acronym of Light Detection And Ranging, LiDAR is a surveying technology that measures distance by illuminating a target with a laser light.

incentives for high occupancy vehicles and support for public transportation. All of these policy regimes will need to be revisited and competitiveness of a nation may depend on ensuring that these emerging rules and regulations are consistent across jurisdictions.

The race is on globally. Despite President Obama proposing $4 billion over ten years for autonomous vehicle research and testing, Google has indicated it may look to the UK as its first deployment market. The UK has advanced limited regulation for autonomous vehicles and instead is supporting new private insurance for autonomous vehicles to enable deployment in the real world creating real global competition in this exciting new sector.[10] Dramatic cooperative action between nations is quickly taking shape as exemplified by transport ministers of all 28 European Union member states signing on April 14, 2016 the 'Amsterdam Declaration' that details steps necessary to establish rules and regulations to allow autonomous vehicle on the public roadways.[11]

Urban Transportation

After the launch of Uber in 2009 and Lyft in 2012, the growth of ride sharing applications has proliferated across the globe. There are numerous ways in which entrepreneurs are designing applications to support the tremendous need for mobility solutions in urban areas.

Historically, most governments regulated commercial vehicle for hire services at the local level. The primary policy goals often included transparent and standardized fares, licensed and safe drivers, and licensed and safe vehicles. More recently policies and regulations to ensure equitable services for the disabled, initiatives to reduce greenhouse gas emissions, and congestion pricing have been introduced in various jurisdictions. Overall, with hundreds of thousands of localities on every continent, there is currently a patchwork of fragmented policies and procedures regulating vehicle for hire services.

In spite of this fragmentation, Uber, Lyft and others have been able to grow rapidly and generate substantial revenue in developed and developing nations alike. As these new services have grown they are facing increasing opposition from existing local providers. In reaction to this opposition, some localities have banned these app-based services entirely and others are requiring onerous and inconsistent registration requirements. Beyond, the registration and licensing issues, individual safety for riders and drivers is an emerging issue. The unfortunate murder of six people by an Uber driver in Kalamazoo, Michigan in February of 2016 illustrates that there may be the need for federal or national legislation to ensure the safety of all participants in app based services.

As the ride share market becomes saturated in developed nations, large technology companies are seeking to leverage connected devices to transform logistics services especially in urban areas. From an environmental perspective fossil fueled ground transportation vehicles

[10] James Titcomb (2015), "Google's meetings with UK Government over driverless cars revealed", The Telegraph, available from: http://www.telegraph.co.uk/technology/2016/01/21/googles-meetings-with-uk-government-over-driverless-cars-reveale/, (accessed 4/14/16)

[11] Government of Netherlands (2016), "Europe wants to pick up the pace towards market introduction of self-driving vehicles", available from: https://www.government.nl/latest/news/2016/04/14/europe-wants-to-pick-up-the-pace-towards-market-introduction-of-self-driving-vehicles, (accessed 4/18/16)

contributed approximately one-quarter of energy-related global greenhouse gas emissions (GHGs) and was responsible for about one-fifth of energy use.[12] New technologies to better optimize last mile freight delivery in urban areas offers a unique opportunity to reduce GHGs and tap a very lucrative logistics market. New solutions for logistics may include autonomous air and ground vehicles teaming together to deliver good in an environmentally sound, cost effective manner. As firms look at these solutions, how can government provide the proper support to enable to improvements of urban areas? What standards must be put in place, regulations need to be changed, agencies need to take the lead to enforce the proper rules when the convergence of new technology transforming vast sectors of the economy?

Conclusion

There are myriad policy issues related to cryptocurrencies, blockchains, autonomous vehicles, and urban transportation. Cryptocurrencies face questions around their status as a currency, asset, security or resource. This can be viewed as a national or central government issue with important international considerations in terms of harmonizing with the global financial system. Whereas automotive vehicle regulation is a federal/central, state/provincial and local government issue where brand new policies and procedures must be developed and implemented as the vehicle as the driver becomes a reality. Urban transportation app based services on the other hand can be considered a local issue with logistics and vehicle for hire regulations needing to be tailored to the local community. And yet as new technology continues to converge any rule at the local level must be suitable to offer the interoperability required of the digital economy that knows no bounds.

As governments grapple with these new innovations many are beginning to recognize the dramatic ways in which applications and solutions related to digital technologies are transforming our global economy. It will be a requirement of policy makers at all levels of government to carefully balance the competing needs of various actors to ensure that the complexities of the 21st century are properly weighted and evaluated in order to support the increasing prosperity and quality of life that these new technologies have the potential to deliver.

Appendix 1

At an international level, through the Financial Action Task Force (FATF), general definitions of cryptocurrencies and blockchains have emerged to support regulation of this new innovation. The FATF defined cryptocurrency as "a math-based, decentralised **convertible virtual currency** that is protected by cryptography…Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof of work system to validate transactions and maintain the block chain."[13]

As a decentralized virtual currency, cryptocurrencies are distinct from FinCEN's definition of real currency as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a

[12] International Association of Public Transport (2014), Action Plan for 2014 UB Climate Change Summit, available from: http://www.un.org/climatechange/summit/wp-content/uploads/sites/2/2014/07/TRANSPORT-Action-Plan-UITC_revised.pdf, (accessed 4/18/16)
[13] FATF (2014), op cit.

medium of exchange in the country of issuance." Thus, in contrast to real currency, "virtual currency is a **medium of exchange that operates *like* a currency in some environments, but does not have all the attributes of real currency**. In particular, virtual currency does not have legal tender status in any jurisdiction."[14]

In the United States, in March of 2014, the Internal Revenue Service (IRS) detailed "that virtual currency is treated as **property** for U.S. federal tax purposes."[15] General tax principles that apply to property transactions apply to transactions using virtual currency, with tax consequences on wages or capital gains or losses derived in cryptocurrencies. A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property.

The Security and Exchange Commission may consider certain activities related cryptocurrencies as the exchange of **securities,** which would thus fall under federal securities laws. Such activities would have to pass the '*Howey'* test, which defines a security as a, "contract, transaction or scheme whereby a person [1] invests his money [2] in a common enterprise and [3] is led to expect profits [4] solely from the efforts of the promoter or a third party."[16] This may be applicable to certain instances where new cryptocurrencies are created or bought/sold on online marketplaces.

Finally, the Commodity Futures Trading Commission has labeled Bitcoin, one of many cryptocurrencies, as a **commodity**[17]. This decision was based on the potential for cryptocurrencies, like Bitcoin, to fall under the broad definition of a commodity in the Commodity Exchange Act as, "all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in".

Appendix 2

The United States Department of Transportation (USDOT) National Highway Traffic Safety Administration (NHTSA) defines vehicle automation as having five levels: No-Automation (Level 0): The driver is in complete and sole control of the primary vehicle controls at all times. Function-specific Automation (Level 1): Automation at this level involves one or more specific control functions. Examples include electronic stability control or pre-charged brakes. Combined Function Automation (Level 2): This level involves automation of at least two primary control functions designed to work in unison to relieve the driver of control of those functions. An example of combined functions enabling a Level 2 system is adaptive cruise control in combination with lane centering. Limited Self-Driving Automation (Level 3): Vehicles at this level of automation enable the driver to cede full control of all safety-critical functions under certain traffic or environmental conditions and in those conditions to rely heavily on the vehicle to monitor for changes in those conditions requiring transition back to driver

[14] FINCEN (2013), Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, available from: https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html, accessed (4/14/16)
[15] IRS (2014), op cit.
[16] U.S. Supreme Court (1946), op cit.
[17] CFTC (2015), op cit.

control. The driver is expected to be available for occasional control, but with sufficiently comfortable transition time. The Google car is an example of limited self-driving automation. Full Self-Driving Automation (Level 4): The vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for an entire trip. Such a design anticipates that the driver will provide destination or navigation input, but is not expected to be available for control at any time during the trip. This includes both occupied and unoccupied vehicles.[18]

[18] NHTSA (2013), op cit.

Section 4:
Activism, Rights and Civic Tech

Civic Tech for Inclusive Governance[1]

Hollie Russon Gilman,[2]

> The old saying that the cure for the ills of democracy is more democracy is not apt if it means that the evils may be remedied by introducing more machinery of the same kind as that which already exists, or by refining and perfecting that machinery. But the phrase may also indicate the need of returning to the idea itself, of clarifying and deepening our apprehension of it, and of employing our sense of its meaning to criticize and re-make its political manifestations.
>
> - John Dewey, *Public and Its Problems* (1954, p. 144).

Abstract

This article explores a unique subset of public sector innovations leveraging civic technology to achieve more inclusive and responsive governance. It argues that the growing field of civic technology ("civic tech") and its public sector applications offer an opportunity for more inclusive governance in the practice of public administration. The article provides a unique definition of civic tech and then employs four illustrative case studies of civic tech being used to further inclusive governance in the United States to inform a typology of how precisely civic tech can be used in public administration. It extends beyond applying technology for modernizing government ("e-government") or enhancing performance to articulate a framework for how technology can strengthen the democratic capacity of governance in order to engage a more diverse citizenry. Simply

---

[1] I am indebted to Hannah Acheson-Field, Erin Britton, Benjamin Dean, Aristodimos Dimitrios Iliopulos,Ester Fuchs, Jason Healey, Merit Janow, Dan McIntyre, Sabeel K. Rahman, Anya Schifrin, Andrea Batista Schlesinger, and the participants of the June 2015 Open Society Foundation research convening in New York City.

[2] Hollie Russon Gilman is a Postdoctoral Research Scholar at Columbia University School of International and Public Affairs (SIPA). She holds a Ph.D. from Harvard's Department of Government and is the former White House Open Government and Innovation Advisor in the Office of Science and Technology Policy.

employing technology is not sufficient–rather, public leaders must work to embed the technology within a more inclusive and responsive governance process.

Practitioner Points

- Public sector officials can leverage multi-sector partnerships to capitalize and harness the expertise of academia, civil society, industry and philanthropy to spur civic tech for governance.
- Creating centralized repositories of interested funders, open source digital tools, collaborations, and best practices for civic engagement can streamline multi-stakeholder partnerships in order to circumvent some of the current institutional barriers facing government officials eager to implement change.
- In order to incorporate civic tech for more inclusive governance, practitioners can start small by piloting civic tech experiments and then move to embed and institutionalize new practices into governance.
- Public officials in the United States can learn best practices from a variety of global examples. Lessons learned can be shared internationally.

Introduction

It is common today to bemoan the state of our democracy, including such phenomena as growing citizen disaffection and the increasing influence of money in politics. In surveys about the country's most serious problems, Americans continue to list government dysfunction over the economy. The 2015 Edelman Trust Barometer shows a global decline of trust in government, with numbers reaching historic lows.[3] Further, a recent Pew survey found that trust in government remains at historic lows.[4] Only 19% of Americans say they can trust the government always or most of the time. The majority of Americans (60%) think their government needs "major reform;" in the late 1990s, fewer than 40 percent of those surveyed thought so. Only 20% would describe government

[3] Edelman Trust Barometer, 2015.
[4] Pew Research Center, November, 2015, "Beyond Distrust: How Americans View Their Government."

programs as being well-run, and 55% of the public says that "ordinary Americans" would do a better job of solving national problems then elected officials.[5]

While these numbers are not conclusive, there is other data to suggest a weakening of the relationship between citizens and the State.[6] As Archon Fung writes, "According to many indicia, the bond between citizens and political institutions has weakened in the United States and other industrialized democracies" (for discussions, see Fung, 2015, p. 3). A growing body of empirical research underscores the degree to which state institutions are subverted by disparities in political and economic power, which contributes to this crisis of democratic legitimacy. Some scholars point to the decline in traditional membership organizations (Putnam, 2001; Skocpol, 1999). Others demonstrate that political elites are beholden to special interests (Lessig, 2011) or disproportionately responsive to viewpoints of those in the top ten percent of the income distribution and not all sensitive to the middle of the distribution or below (Gilens, 2012).

Partly in response to citizens' growing disaffection, however, a wave of participatory policy reform has emerged in America's largest cities, capitalizing on new technology and democratic experiments that aim to improve democracy. This typically includes local, place-based, community-driven interventions occurring both inside and outside of government. Often these approaches involve leveraging networks and digital tools. These instances of reform, collectively known as "open government," "inclusive governance,"

---

[5] *Ibid*.

[6] Throughout this article the term "citizen" denotes someone with the political standing to exercise voice or give consent to public decisions, not necessarily only someone with legal citizenship.

or "civic innovation," are engaging policymakers, citizens, and civil society and revivifying long-dormant democratic instincts.

One example of this push for more participatory policy reform includes the recent Sustainable Development Goals (SDGs) and the commitment for furthering inclusive and responsive institutions. In September 2015, the United Nations voted on its SDG framework, the follow-up international agenda to the Millennium Development Goals. SDGs aim to eradicate poverty, build sustainable cities, and combat climate change. Unlike the Millennium Development Goals, which were largely devised in a top-down manner in New York and Geneva, the SDGs were conceived more democratically after three years of deliberation by a group of representatives from 70 countries.[7] There was a high-level panel that included representatives from civil society, the private sector, and academia alongside local and national governments. In fact, the UN conducted the largest consultation in its history to shape SDGs.[8] These conversations included thematic and national discussions, in addition to door-to-door surveys that sought feedback from a variety of stakeholders.[9] There was also a *MyWorld* online.[10]

Perhaps as a result of this collaborative process, Goal 16.7 includes a commitment to:

---

[7] Liz Ford, "Sustainable Development Goals: all you need to know," *The Guardian*, January 19, 2015, retrieved from http://www.theguardian.com/global-development/2015/jan/19/sustainable-development-goals-united-nations

[8] Ford, 2015.

[9] Hollie Russon Gilman and Aristodimos Dimitrios Iliopulos, "The most sustainable development goal," *Al Jazeera America* September 25, 2014, retrieved from http://america.aljazeera.com/opinions/2015/9/the-most-sustainable-development-goal.html.

[10] See http://www.beyond2015.org/un-thematic-consultations

> Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels" to "ensure responsive, inclusive, participatory and representative decision-making at all levels.[11]

Collaborative Governance and Innovation

Governance innovations, unlike innovations in products or services, are concerned with "new forms of citizen engagement and democratic institutions" (Hartley, 2005, p. 28). Some have referred to a shift toward more "networked" or "citizen-centered" governance (Noveck, 2015; Benington &Hartley, 2001; Hartley, 2005).

Civic tech for governance differs from standard applications of technology to improve government efficiency or modernize systems ("e-government"). Civic tech used for governance is less focused on finding the next "killer app" than on employing technology in order to achieve more responsive and inclusive governance. As such, this article situates civic tech for democratic aims in dialogue with literatures examining innovative and collaborative governance (for discussions, see Moore &Hartley, 2008; Sørensen & Torfing, 2011; Ansell & Gash, 2007).

The innovation literature meant for both the public and private sectors helps set limited boundaries for what is and what is not an innovation. Sørensen & Torfing (2011) define innovation as an "intentional and proactive process that involves the generation and

[11] See https://sustainabledevelopment.un.org/focussdgs.html

practical adoption and spread of new and creative ideas, which aim to produce a qualitative change in a specific context" (2011, p. 849). Innovation is something new; it is not simply another name for the same thing (Lynn, 1997). For Moore and colleagues (1997), innovation must be "large enough, general enough and durable enough to appreciably affect the operations or character of the organization" (Moore and Hartley, 2008, p. 5). Importantly, innovation is context-specific (Sørensen & Torfing 2011; Zaltman, Duncan, & Holbek 1973). Even if a practice has already been instituted in a different institutional context, it can still be an innovation when applied in a new setting or manner.

There has been a resurgent interest in public-sector innovation (Altschuler & Behn, 1997; Borins, 2001, Moore & Hartley, 2008). Often the focus of these public innovations is intra-organizational, aiming to improve services, products, and processes. Public-sector innovation, in contrast with that in the private sector, is not "often seen as a virtue in itself" (Hartley, 2005, p. 23). Without clear new markets or a clear understanding of competition, public-sector innovation must show that it is advancing public value (Moore, 1997, & Moore, 2013, for definitions and discussions of "public value").

Scholars are pushing for more external-facing innovations, including public-private partnerships (Sørensen & Torfing, 2011, p. 852). Moore (1997; 2013) articulated an idea of creating *public value* that encouraged public managers to look outside their environment to gain a better sense of what was possible and valuable. A notable recent example is the Obama's Administration creation of 18F and the United States Digital

Service to deploy service-delivery teams throughout agencies to optimize user-centric service delivery.[12] These teams include designers, programmers, and digital experts whose task is to modernize service delivery in order to enhance the experience of everyday people.

Attempts to optimize government by using the latest technology do not necessarily lead to such democratic outcomes as more inclusive, responsive, participatory, or legitimate governance. In fact, there is a growing set of studies showing the limitations of technology in empowering citizens and, in particular, marginalized people (Rumbul, 2015; Peixoto & Fox, 2016).

Despite these limitations, there are two steps that must be taken to bring governance into the twenty-first century. Modernizing government is the first critical step. One example is creating digital interfaces members of the public can use to acquire driver's licenses or receive Veterans Affairs benefits. The second step works not only to modernize an individual process but also to ensure that technology creates the necessary channels to enhance the *relationship* between citizens and the State.

Within this second iteration, technology can be used for civic ends, *i.e.*, to empower people to take part in the process of governance. There are different terminologies—

[12] USDS and 18F are federal agencies with the goal of improving service delivery for citizens; they are comprised of teams of engineers, designers, coders, and policymakers. USDS is housed at the Office of Management and Budget (OMB) and is actively deploying USDS teams throughout agencies. 18F is housed at the General Services Administration (GSA); the building is physically located at 1800 F St., NW, Washington, D.C. See more at: https://www.whitehouse.gov/digital/united-states-digital-service and https://18f.gsa.gov/. These agencies grew out of the Presidential Innovation Fellows program, a fellowship to bring in technology experts for a rotation in the federal government. They reflect a general trend in the Obama administration to integrate technology into the federal government, which included implementing the positions of Chief Technology Officer and Chief Data Scientist.

including “inclusive” or “collaborative governance” and “participatory democracy”—used to describe processes that enhance civic opportunities in governance. These concepts have in common a push to re-engage everyday people in the policy decisions that impact their lives; “in the participatory conception, citizens engage directly with one another to fashion laws and policies that solve problems that they face together” (Fung, 2007, p. 450). For proponents of participatory democracy such as Benjamin Barber, common values include self-government, political equality, and reasoned rule (Fung, 2007; Barber, 1984, pp. 1988-89).

The literature on collaborative governance focuses on the types of institutional arrangements to engage citizens in decision making. Collaborative governance at its core “aims to ‘empower, enlighten, and engage citizens in the process of self-government’” (Sirianni, 2006, p. 39). One characteristic of collaborative governance is that it ensures that diverse stakeholders engage in a “collective decision-making process that is formal, consensus-oriented, and deliberative and that aims to make or implement public policy or manage public programs or assets” (Ansell & Gash, 2007, p. 544). Collaborative governance literature, then, is a body of work that could provide a theoretical framework to assess the types of institutional arrangements that could foster such civic opportunities.

Examples of institutional structures for more collaborative governance include minipublics and co-production. Scholarly work on “minipublics,” examines venues for direct citizen participation, such as the paradigmatic British Columbia Citizens’

Assembly (Fung, 2015; Fung, 2003; Smith & Ryan, 2014).[13] There is a related literature on the opportunity for citizens to be co-producers of public services (Kettl, 2015; Boyle and Harris, 2009). Ostrom and Baugh first used the term "coproduction" in 1973 to refer to citizens' more active roles in serving and improving government—and doing so more on par with the actions of elite professionals. An example of co-production includes Code for America's "adopt a hydrant" campaign, in which people in California sign up for a specific hydrant (or even a rain duct) and assume responsibility for its upkeep during bad weather conditions (Kettl, 2015, p. 225).[14]

This article aims to bring the nascent civic tech movement in dialogue with these more established frameworks on collaborative governance and innovation. Its goal is to conduct a rigorous inquiry that aims to understand the precise ways in which technology can affect public policy outcomes. The rise in access and availability of digital technology presents, at least in theory, an opportunity to deepen inclusive and collaborative governance. As a first wave of technological idealism adjusts to the realities of people, politics, and institutions, there is a need for more scholarly examination of the precise pathways by which digital technology can affect governance.

An initial wave of technologists was optimistic about the opportunity for information technology to transform democracy. Scholars examined the opportunity for new bloggers to enter into public discourse (Chadwick, 2006) with the promise of bringing about a

---

[13] For more information on this case, see Participedia.org. 2009, "British Columbia Citizens' Assembly on Electoral Reform," retrieved from http://participedia.net/en/cases/british-columbia-citizens-assembly-electoral-reform

[14] See Code For America "Adopt a Hydrant" retrieved from https://www.codeforamerica.org/products/adopt-a-hydrant/

newly networked public sphere (Benkler, 2006). In 2004 Joe Trippi noted, "The Internet is the most democratizing innovation we've ever seen–more so than even the printing press" (2004, p. 235). Clay Shirky outlined a vision of co-production in which the Internet enables people everywhere to work together: "These changes will transform the world everywhere groups of people come together to accomplish something, which is to say everywhere" (2008, p. 24).

However, the last decade has made manifest some of the challenges in implementing this utopian vision, in part due to the character of political incentives and institutional constraints. For example, Hindman's (2009, 104) research illustrates that the most popular political bloggers have elite resumes. Fung, Gilman, & Shkabatur (2013) have argued that Internet Communications Technologies (ICTs) are more likely to have an incremental, rather than a transformative, impact on politics. In particular, ICTs will be most successful when they work within existing political ecosystems and leverage traditional organizations, such as media outlets or NGOs.

This paper examines the opportunity within governance structures, primarily on the local level, for fostering more inclusive governance. Below it presents the current landscape of discussions of civic tech and provides a stylized definition of civic tech for governance innovation. Rather than being exhaustive, the definition aims to narrow the field of civic tech so that it encompasses only that area of the field aiming to further democratic goals such as inclusion and participation.

Civic Technology

Civic technology is an emerging field lacking a universally accepted definition. This causes confusion about its contours—particularly about to what extent it is public and to what extent it is private—but also provides opportunities for creativity. According to a Microsoft vice president, "Broadly defined, civic tech ranges from engagement between the city government and its population on social platforms, all the way to enterprise solutions that offer deep government IT problem-solving."[15]

Despite the lack of a coherent definition, civic tech continues to grow as a field. In 2014, a $23 million venture fund called GovTech launched to focus on technology to improve government services. According to a study by the International Data Corporation (IDC), sponsored by the software company Accela, civic tech investment will reach $6.4 billion in 2015 (Clarke, 2014).[16] This figure is just a piece of the $25.5 billion the government spends on external information technology (IT). The IDC report defines civic tech as merging "technology innovation with civic purpose" and cites its rapid growth, particularly in state and local government. One area of this form of civic tech is upgrading legacy government systems, generating citizen-facing services, and ensuring websites have mobile access. Another is creating greater access to, and transparency of, data and policy performance.

---

[15] Retrieved from http://blogs.microsoft.com/on-the-issues/2014/10/27/civic-tech-solutions-governments-communities-serve/

[16] This large investment represents just a fraction of the $25.5 billion expected to be spent on government IT services.

Further, contentiousness among stakeholders about definitions evidently has not dampened either the excitement or the funding in the civic sector. In 2013, the Knight Foundation released a report showing that the number of civic tech organizations had grown 23% in 2008, with a total investment of more than $431 million. The report cited two broad themes: community action and open government. Within these categories fell: collaborative consumption; government data; crowd funding, community organizing; and social networks. Some critiqued the report because of its inclusion of peer-to-peer sharing and other for-profit entities such as Airbnb (funded at $118.6 million) and Waze (funded at $30 million).[17]

The Knight Foundation's definition of civic tech is broad and includes projects that are not directly related to politics, such as: peer-to-peer sharing projects (e.g, Peerby, Lyft, Relayrides, Uber); neighborhood-level social networks (e.g. nextdoor); and data utility (e.g., textmybus). The Knight Foundation's $431 million figure limited civic tech to investments by foundations and corporations, thereby excluding government and public funding. But they still estimated that, as noted above, there has been 23% growth in this area from 2008 to 2013.

This paper proposes to narrow the definition to put democratic institutions front and center. It defines civic tech as: *technology that is explicitly leveraged to increase and deepen democratic participation*. This definition includes both the use of new digital tools specifically designed to promote democratic deepening and the repurposing of old

[17] See Nathaniel Heller "The Sharing Economy is Not Civic Tech," Global Integrity, retrieved from www.globalintegrity.org/2013/12/the-sharing-economy-is-not-civic-tech/

digital tools (e.g., webcam sit-in, mail campaigns) with the new objective of deepening democracy. By design, this is a stylized definition that excludes technology used solely for modernization or market gain.

Method

The purpose of this article is to begin a rigorous, detailed investigation into a particular application of civic technology. This type of civic technology is used for the more inclusive and collaborative governance that seem increasingly important for public policy, yet remain less well understood by political science and public policy literature. The method employs a small number of public-sector applications of civic technology (based on first-hand interviews, documentary evidence from case studies, and official reports) that fall within a broader set of civic technology for governance. These cases are not aimed at offering a complete evaluation of social impact or comprising a representative sample. Instead, they are offered as particular examples of innovations that are not currently accounted for by existing theories. They are valuable cases in the opportunity they provide to change conceptual understanding. The cases illustrate the opportunity to reframe the discussion of civic tech around promoting democratic outcomes such as enhanced citizen engagement with governance. The cases lead to a set of public policy recommendations to inform researchers and practitioners.

Civic Tech for Inclusive Governance: Important Paradigms

Boston New Urban Mechanics

In 2010, at the beginning of Mayor Menino's fifth term, Boston launched the first Mayor's Office of New Urban Mechanics (MONUM).[18] The office was designed to pilot experiments and work directly with entrepreneurs. The goal was leveraging technology and innovation to improve the quality of City services and to strengthen the relationship between citizens and the City to promote "peer-produced governance."[19] Menino had long been interested in the process of tinkering with tools, which gave him the nickname "The Urban Mechanic." Since 2010, the office quickly gained momentum, with the two co-heads receiving an award as the Public Officers of the Year from *Governing Magazine*.[20] MONUM has been recognized as a global example, including by the UK Innovation Unit NESTA, and recently received $1.3 million as part of the Bloomberg Philanthropies Innovation Team program aimed at developing solutions to the middle-income-housing challenge.

MONUM grew out of a desire to leverage technology to modernize government services and to enable the overworked staff of City Hall to run innovation projects, often with international policy experts and external entrepreneurs. A core principle was to more deeply engage residents with City Hall. Though only an initial team of five, the team was able to permeate the city culture and create a test environment for civic experiments. Prior to officially launching MONUM, its co-founders took advantage of the momentum and distribution of smart phones to develop a cutting-edge application, *Citizens Connect*,

---

[18] Retrieved from http://newurbanmechanics.org/boston/

[19] See Ben Schreckinger, "Boston: There's an App for That," *Politico Magazine*, June 10, 2014.

[20] See Steve Goldsmith, "An Old-School Mayor on the Forefront of Innovation," *Governing*, September 6, 2012.

in 2009 (Crawford & Walters, 2013). The app creates a streamlined process for residents to report local issues directly to the right municipal agency, empowering them to improve the condition of their neighborhoods. It has been used by over 70,000 residents across multiple platforms, including a web-based interface and Android. The app now accounts for one-fifth of all city service requests, or roughly 10,000 per year.[21]

Since its launch, the project, now called *Commonwealth Connect*, has expanded from Boston to encompass over forty Massachusetts communities. The latest version of *Connect* includes a mini Customer Relationship Management (CRM) system with a call center, visible city worker completion of a task, and the capacity to generate reports (Crawford & Walters, 2013). Residents may even "thank" city workers for completing a task. As Crawford and Walters write, "Boston may be the best in the country in late 2013 at engaging people and building relationships that further the aims of city government, but it is not clear what will happen to this culture when the key people leave the building in January 2014 (2013, p. 25)."

Since Boston's new mayor took office, the MONUM have moved from a pilot initiative to become more embedded and institutionalized within government. Importantly, from the start, MONUM has been focused on civic engagement—not only on modernizing performance management—and is currently using its expertise in civic engagement to address several core policy areas for City Hall. This includes: enabling Boston to be a premier digital school district by 2020; increasing access to city services with a refurbished truck, *City Hall to Go*, that delivers services directly to the people; and

[21] Schreckinger, 2014

running a Housing Innovation Lab committed to attracting small business and retaining affordable housing. The support of Bloomberg Philanthropies has enabled increased staff capacity as well.

The MONUM model has spread to Philadelphia and Salt Lake City and continues to serve as an international paradigm for cities. The success of MONUM illustrates the opportunity for digital technology to alter institutional culture, making it more amenable to experimentation and focused on residents. MONUM takes the needs of the citizens as users very seriously—even conducting a thorough ethnographic study to understand housing needs for lower-income communities. Throughout these endeavors, MONUM has worked to produce the types of tools and technologies that can be easily accessed by residents. Further, MONUM's ability to become more embedded in the structure of City Hall provides a promising model for transforming experiments from ad hoc processes to core governance functions.

Participatory Budgeting in New York City

While participatory budgeting (PB) is just now taking root in the United States, it traces its origins to a unique initiative started in 1989 in Porto Alegre, Brazil, by the leftist Partido dos Trabalhadores (Workers' Party, henceforth PT). Participatory budgeting gives citizens the opportunity to learn about government practices and to come together to deliberate, discuss, and substantively have an effect on budget allocations (Shah, 2007). In its original campaign for participatory budgeting, the PT outlined four basic principles guiding PB: (1) direct citizen participation in government decision-making

processes and oversight; (2) administrative and fiscal transparency as a deterrent against corruption; (3) improvements in urban infrastructure and services, especially in aiding the indigent; and (4) a renewed political culture in which citizens serve as democratic agents. Recent research convincingly demonstrates that in the last twenty years PB has enhanced the quality of democracy in Brazil, improving governance and empowering citizens. Other positive outcomes linked to specific uses of PB in Brazil include increased municipal spending on sanitation and health, increased numbers of CSOs, and decreased rates of infant mortality (Touchton & Wampler 2014, p. 1444); Goncalves (2014).

Since then, PB, often supported by the World Bank or foundations and civil society, has spread across the globe to over 2,500 localities The process first came to the United States in 2009 in Chicago, where an alderman used $1.3 million of his discretionary funds to make American civic history.[22] Since then, the process has continued to expand with political support from the White House, with over $50 million in local based public funds being allocated. In New York City, the Participatory Budgeting Project has worked closely with Community Voices Heard, a local membership-based organization that focuses on women of color and low-income families, to support and expand the process. In 2011, New York City launched the largest domestic project with bi-partisan support and four City Council members implementing PB. Since then, the process has grown to over half the City Council, with 27 of 51 Council members implementing PB

[22] Newcombe, 2012; See Weeks, 2000, for large-scale deliberative processes in the early 1990s that engaged citizens to address municipal-budget concerns in Eugene, OR, and Sacramento, CA. For other examples of U.S.-based citizen engagement on budgeting, see Center for Priority Based Budgeting 2015 (retrieved from http://www.pbbcenter.org/).

for 2015-2016. NYC's PB has been effective at ensuring that PB voters represent a larger percentage of previously marginalized residents than do voters in traditional elections. In 2014-2015, 51,000 residents voted. The majority of PB voters (57%) identified as people of color, in comparison to 47% of local election voters and 66% of the total population of the twenty-four districts participating.[23]

New York City is experimenting with a range of digital tools to engage people in the PB process, exporting successful examples from other countries. For example, Belo Horizonte, Brazil, has solely online PB, through which roughly 10 percent of the city's eligible voters participate (Sampaio & Peixoto, 2014). Online participation was between three to five times higher than participation rates in face-to-face rounds of PB occurring in the same year (IBM Center, 2011, p. 36).

In 2015 New York's PB used electronic ballot counting and a partnership with Textizen, which started as a Code for America project.[24] The City Council has created a web-based mapping tool for gathering crowdsourced public input for project submissions. The geo-

[23] Community Development Project at Urban Justice Center with the PBNYC Research Team: "A People's Budget: A Research and Evaluation Report on Participatory Budgeting in the New York City," Cycle 4: Key Research Findings October 20, 2015, retrieved from: https://cdp.urbanjustice.org/sites/default/files/CDP.WEB.doc_Report_PBNYC_cycle4findings_20151021.pdf

[24] Alex Yule, "New York City Brings Budgeting to the People," The Textizen Blog, May 5, 2015, retrieved from http://blog.textizen.com/nyc-participatory-budgeting-20150505/); Aseem Mulji, "Participation Lab: Developing New Engagement Tools for Transformative Democratic Participation," submitted as the Participatory Budgeting Project's entry to the Knight News Challenge, "How Might We Better Inform Voters and Increase Civic Participation before, during and after Elections?" March 19, 2015, retrieved from http://newschallenge.org/challenge/elections/entries/participation-lab

targeted maps enable people to drop a pin on a map and provide ideas, suggestions, and comments. The maps are powered by OpenPlans open source technology.[25]

In the 2015 PB vote, New York City, in partnership with Stanford University's Crowdsourced Democracy Team and Democracy 2.1, tested alternative ways of voting with the goal of making voting "as easy an ATM."[26] New York City employed a digital ballot experiment, with both iPads for mobile kiosks and computers for in-person voting. In 2016, New York's PB is slated to conduct the first-ever remote online voting with an integrated online/offline ballot. Researchers from universities across the world are partnering with Public Agenda, a New-York-based non-profit, and the Participatory Budgeting Project, to conduct research on the process and its impact.

The rise of the PB process and civic tech experiments in New York illustrate the opportunity for cross-national learning to engage citizens in governance. While it started in Brazil, PB continues to grow and change shape based on the specific context in which it is deployed. Similarly, the precise application of digital tools also varies among specific communities. Sharing these lessons learned, including obstacles, creates an opportunity for illustrative civic tech to translate across borders in order to inform a deeper practice of innovation.

---

[25] New York City Council, "Participatory Budgeting: Suggest a Project Idea," retrieved from http://council.nyc.gov/html/pb/ideas.shtml.

[26] Jessica McKenzie, "New York City Test Digital Ballot in Participatory Budget Vote," June 18, 2015, retrieved from http://civichall.org/civicist/new-york-city-tests-digital-ballot-in-participatory-budget-vote/

Chicago OpenGrid

Chicago has created OpenGrid to provide an open source, situational awareness system to that enables people to easily access a centralized open source repository of public information.[27] OpenGrid reflects one of the most advanced deployments of government data to empower citizens.[28] It also reflects the latest project in Chicago to build open source data efficiency that is scalable.[29] Chicago's WindyCity platform integrated seven million pieces of data from city departments every day and paired it with a powerful analytics tool to create data visualization to equip managers with new insights on city operations in real time.[30] It won $1 million from Bloomberg Philanthropies Mayor's Challenge.[31]

OpenGrid also includes a series of data installments led by the Chicago city government. An earlier project, WindyGrid, provided an open-source situational awareness system for government employees, which Chicago helped roll out in other cities. WindyGrid led to internal efficiency that, in turn, informed the building of a public facing interface. The

---

[27] See also "Chicago Tech Plan," City of Chicago, retrieved from http://techplan.cityofchicago.org/

[28] See Sean Thornton, "Chicago Launches OpenGrid to Democratize Open Data," *Harvard Data-Smart City Solutions*, January 20, 2016, retrieved from http://datasmart.ash.harvard.edu/news/article/chicago-launches-opengrid-to-democratize-open-data-778?utm_content=buffere195b&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

[29] Jason Sheuh, "3 Reason's Chicago's Analytics Could be Coming to Your city" *Government Technology,* April 1, 2014, retrieved from http://www.govtech.com/data/3-Reasons-Chicagos-Analytics-Could-be-Coming-to-Your-City.html

[30] "Chicago Uses MongoDB To Create A Smart and Safer City," retrieved from https://www.mongodb.com/customers/city-of-chicago.

[31] Amina Elahi, "Bloomberg Awards Chicago $1 M for Real-Time Analytics Platform" *Built in Chicago*, March 13, 2013, retrieved from http://www.builtinchicago.org/blog/bloomberg-awards-chicago-1m-real-time-analytics-platform.

earlier processes to modernize government have directly led to a more engagement-oriented design.

Now Chicago has moved beyond internal efficacy to create an external situational awareness interface that allows everyday people to engage with the city's information. Even with open data portals in many major cities across the globe, it can be difficult for a layperson to quickly find the relevant data in a sea of information. OpenGrid is a map-based application made by Chicago's Department of Innovation and Technology (DoIT) that provides an intuitive visual so that residents may understand complex municipal data and use that understanding to interact with their community.

The city is partnering with outside collaborators whom they see as key beneficiaries, including the University of Chicago's Urban Center for Computation and Data and the Smart Chicago Collaborative, comprised of local civic organizations including MacArthur and the Chicago Community Trust. According to Chicago CIO and DoIT Commissioner Brenna Berman, "At the Department of Innovation and Technology, our clients are the residents and businesses of Chicago. We're driven by what they need, and how we can serve them."[32] For example, prospective entrepreneurs can use OpenGrid to identify nearby permits and licenses. Residents, researchers, or community organizations can understand the pulse of the city, ranging from crime and environmental inspections to 311 calls.

[32] Thornton, 2016.

OpenGrid reflects the latest version of open data being released to spur civic education, agency, and industry. For example, in the 1970's the United States' National Oceanic and Atmospheric Administration began releasing its daily weather data to the public. That data, in turn, helped spawn the modern weather industry and is used by hundreds of companies, from Weather.com to countless smartphone apps. Similarly, the government's releasing GPS data in the 1980's led to the creation of an entire industry, from car GPS devices to Google Maps.

In contrast to the older examples, in which data was simply released without an engagement strategy, OpenGrid is designed for participation, collaboration, and replicability. Chicago's Civic User Testing Group is comprised of residents from across the city who test civic websites and apps and then provide direct feedback. The Grid is engaging these users to understand how residents can most benefit from the information. The coding and user documentation is publically available on the file-sharing site GitHub. In theory, other cities can leverage the code for their own databases. OpenGrid won Amazon's "Dream Big" award in its City on a Cloud innovation Challenge. Now, Amazon Web Service is providing support that can also enable other cities to leverage this model.

OpenGrid illustrates that opening up data alone will not necessarily lead to more democratic outcomes. Citizens are living in a supersaturated data environment that does not inescapably lead to more informed or empowered citizenry. Cities across the country,

nevertheless, are taking lessons from Chicago in order to implement experiments with their own platforms to democratize access to open data.

Rhode Island Civic Crowd Funding

Central Falls, Rhode Island, is a densely populated community in a small geographic area, with Rhode's Island only majority-Hispanic community. In 2011, Central Falls declared chapter 9 bankruptcy, marking the first time a city in Rhode Island had declared bankruptcy. In this socio-political climate, the city government decided to try something new to engage the community around a shared project.[33] They partnered with Citizinvestor,[34] a crowdfunding and civic engagement site similar to a Kickstarter for governments, to launch a civic crowdfunding campaign, one of the first in the United States. Municipalities post a project with a funding goal. Citizens donate online. If the goal is met, the municipality receives the funds minus fees. It's an all-or-nothing model—in order for the entity to receive the funds, the fundraising goal must be met.

Central Falls hosted town halls about the funding proposal in order to gauge where community interest lay. The community responded by talking about the lack of proper trash bins in the central park of the city. Central Falls launched a Citizinvestor campaign that hit their goal of $10,044. Local residents were active participants in every part of the process: identifying the area for fundraising; pledging their own dollars; and collaboratively designing artistic trash cans, working directly with local arts nonprofit

[33] Retrieved from http://citizinvestor.com/project/clean-up-cf-new-bins-in-jenks-park
[34] Retrieved from http://citizinvestor.com/

The Steel Yard. Community members even came out to directly place the trashcans and paint them. The project invigorated the community in a way that was both functional and led to direct improvements in public life.

What precisely is civic crowdfunding? Rodrigo Davies provides a definition: "Civic crowdfunding projects can therefore be defined as projects that produce some non-rival benefits that serve either the non-excludable public or broad sections of it" (Davies 2014, p. 29). According to Davies the most popular civic crowdfunding projects involve parks.

Several cities across the United States have been experimenting with civic crowdfunding, and they are learning from one another. Philadelphia was the first city to partner with Citizinvestor in a campaign to fund TreePhilly.[35] While they did not meet their $13,000 funding goal, their lessons learned have shaped further civic crowdfunding experiments. This includes launching more focused projects that are applicable to specific communities and ensuring that crowdfunding does not become a substitute for existing public resources. Instead, it should be used to supplement public funding.

Some states are starting to develop laws to govern crowdfunding. One such state is Oregon, which allows Oregon-based companies to raise up to $250,000 from Oregon Investors to start new businesses or fund existing operations. No single investor can invest more than $2,500 in any one project.

---

[35] Sarah Glover, "Philadelphia Uses 'Crowdfunding' to Complete Civic Projects," March 26, 2013, , retrieved from http://www.nbcphiladelphia.com/news/local/Philly-Projects-Crowdfunding-200081891.html#ixzz3yTGS1W33

Civic crowdfunding is concerned with distributional equity, more specifically with ensuring that it is not only wealthier residents who can afford specific amenities for their communities. Civic crowdfunding has been limited to specific projects and can help generate immediate gratification for citizens.[36] Each project can also generate larger lessons—insight from Philadelphia helped inform future efforts in Central Falls. As the process continues to spread, each experiment creates a valuable model that can help generate a set of best practices and considerations to inform future projects.

Initial Inquiries and Limitations

These applications of technology seem to warrant their own classification and further inquiry. How can we understand these civic tech applications? They seem to inform a more comprehensive toolkit for re-engaging citizens in governance and policy decision-making. In this article, I have limited the discussion specifically to civic tech used within a governmental capacity. There is additional research needed both to assess implementation in organized civil society and to do a deeper assessment of how civic tech can better strengthen the interface between government and people. I have also only focused on "positive" examples that fall into the schema I have outlined. There are methodological limitations to this approach. The four cases above are, however, valuable because they can change people's conceptual understanding of how technology can be employed in governance. These cases show that the conversation about technology need

[36] See also Rodrigo Davies, "Civic Crowdfunding: A New Way of Spending Down?" September 16, 2014, *Stanford Social Innovation Review.* retrieved from http://ssir.org/articles/entry/civic_crowdfunding_a_new_way_of_spending_down

not be limited to its potential to modernize government performance; in fact, technology can also enhance the democratic capacity of governance to engage a more diverse citizenry. Outlined below are three unique characteristics of civic tech for governance with relevant policy recommendations.

Lessons Learned: Civic Tech for More Inclusive Governance

Leveraging Multi-Sector Partners

Each of the examples took advantage of a wide range of talent and expertise—from technologists and entrepreneurs in the MONUM to well-organized membership-based civil society in PB in New York City. Each of these initiatives has had a partnership with external experts, such as the Citizinvestor platform, and external entities such as the Amazon Web Services in Chicago, from which OpenGrid leveraged resources. MONUM now has more staffing capacity because of Bloomberg Philanthropies. PB has spread across the United States with the backing both of philanthropies such as Omidyar Network's Democracy Fund and grassroots-level support. OpenGrid has partnered with the Smart Chicago Collaborative, which is funded by the MacArthur Foundation, and the Chicago Community Trust.

The civic tech examples here also utilized university expertise. This could take the form of fellowships (e.g. MONUM), computing power (e.g. OpenGrid), or research support (PBNYC). The methods employed enabled public-private partnerships and created entry points for the public sector to leverage external resources.

These cases show that policy makers can think more expansively about the resources at their disposal and structure civic tech experiments with the deliberate intent to engage multi-sector stakeholders. The result is securing more resources to fund public projects and harnessing experts who may not typically be associated with governance. Structuring projects to include diverse stakeholders is a key strategy for more inclusive governance.

The Embedding and Institutionalization of Pilot Programs

Many of these examples started as pilots and went on to become more embedded in institutionalized structures. When they started, the Boston New Urban Mechanics were able to create prototypes of several kinds of programs in a lean and agile way. Because their work gained momentum and won support from citizens, they now are being asked to solve critical problems for the city systematically. PB also began as a pilot with $1 million in public funds, and now upwards of $50 million is being allocated through the process. In Central Falls, Rhode Island, city managers explored new ways of engaging citizens in decision-making regarding precisely where and how to fund public programs. Considerable improvisation was needed, as the city had never before used civic crowdfunding. Citizens were involved in identifying projects, spending their own dollars, and even setting up the trash bins ultimately paid for by the crowdfunding.

The leaders of these projects were able to take otherwise impossible risks because they were starting out with small and nimble programs. This fact produced both less pressure from the outset and the ability to think more creatively about implementation. Learning

from mistakes, leaders and participants were able to refine processes and gain external validation. As the projects gained traction and support, they could become more embedded into institutional processes.

Policy makers can see a certain type of freedom in pilot projects, in which the stakes are lower than usual, creating less pressure. Experiments offer an opportunity to reach citizenry in non-traditional ways, which is particularly helpful for outreach to traditionally marginalized communities, as well as to expand the traditional public service delivery model of citizen as mere customer. Instead, citizens can be empowered to participate in more inclusive decision-making through well-structured pilots.

Learned Lessons Across Contexts

Because civic tech is not bound to one geographic region, many of these examples take a more networked and global approach. Such networks enable project developers and participants to apply lessons learned from various contexts. Participatory budgeting first began in the Global South and is quickly spreading across the North. Philadelphia was the first city to experiment with a Citizinvestor public funding campaign, and, though they did not reach their goal, valuable insights from their process directly improved the processes in other cities. The Chicago DoIT ensures that all the code for the city is open source and available on GitHub. Other cities, in turn, can use this code for their own public interfaces, which creates more open and democratic data.

In several of these examples, prior experiments and pilots in different locations generated shared lessons. Best practices from global experiments can be adapted to fit specific

contexts and local needs. These experiments do not need to be viewed in isolation from one another; rather, each can serve as a useful breeding ground for ideas for further implementations.

Policy makers can learn lessons from many types of actors across diverse contexts. The result can be a more expansive approach to innovation, which is inclusive of diverse cultures and backgrounds. But it is critical to apply these lessons in context and in a way that is sensitive to the local socio-political context and environment.

Can Civic Technology Really Enhance Democracy?

The article's examples illustrate a new way of doing business, one in which citizens themselves are put front and center in discussions of technology. Although there will be many debates on how to measure and deploy digital tools, there are certain questions specific to the realm of civic tech for inclusive governance. Consider the following three:

First, what are the incentives for government officials to implement these civic tech innovations? These processes are labor-intensive by design. Engaging citizens for more inclusive governance requires resources, time, and intentionality. In times of spending cuts and austerity, how can government prioritize citizen engagement? This is especially true given normative views of a less robust democracy, in which voting is considered sufficient for participation.[37] While I have outlined the potential for multi-stakeholder partnerships to buttress these programs, government buy-in and support are still required

[37] There are more minimalist conceptions of democracy, such as aggregative democracy. For discussions, see Fung, 2007. Throughout this paper I am arguing for a more participatory approach to democracy.

to structure the partnerships. Getting officials to agree to these projects will require building a robust evidence base of what works and why. Even well-intentioned public administrators may face ossified political structures that prevent them from fully engaging with citizens (Peixoto & Fox, 2016). Creating centralized repositories of interested funders, open source digital tools, collaborations, and best practices for civic engagement can streamline multi-stakeholder partnerships in order to circumvent some of the current institutional barriers facing government officials eager to implement change. For those officials more reluctant to take the risk of innovating, successful examples in other localities across the globe may provide necessary political cover for further experimentation. In all of these cases, external support can accelerate implementation and serve as a public endorsement.

The second, related, challenge is, how can we measure the impact of nebulous concepts such as inclusive governance? How can we measure feedback loops from civic participation back to the people? Is it simply the number of people who participated or the type of people who engage (including their demographic diversity as well as prior levels of civic engagement)? Or should we be measuring the quality and efficacy of their engagement? These processes may take a long time to show results. Positive community indicators from deploying Participatory Budgeting in Brazil, for example, are only evident after many years. We need to do longitudinal studies of impact in a political environment that rewards instant gratification and success. As evidenced in Chicago, simply providing open data is not enough. Metrics on government's releasing of data are insufficient on their own. Rather, this data must be strategically deployed to engage

citizens when and where they need information the most. Textured measures combining quantitative and qualitative metrics are therefore more valuable than numbers alone. A metric that simply captures the number of open data sets will not tell the whole story.

Finally, how do we balance one-time experiments with the need for institutionalization? As mentioned earlier, there is a certain type of power that comes from pilot and ad hoc experiments. There is greater willingness to explore and take risks during these types of pilots. Citizens can serve as true co-producers when the bureaucratic rules are not yet fully formed. There is a tension, however, between conducting small pilots and building more inclusive governance institutions. Smaller pilots are more likely to get off the ground quickly within a climate of at least some bureaucratic constraints. However, if pilots are limited to engaging citizens to solve only small-scale problems, citizens may become disillusioned with a process they view as trivial (Fung, 2015, p. 9). Archon Fung describes this as "the park bench problem" (Fung, 2015, p. 9). If pilots are viewed as trivial in the sense of pertaining only to small-stakes politics, such as whether there are enough park benches, they will lose their ability to bring about lasting change. Smaller-scale experiments within government institutions, therefore, should be viewed as vehicles for achieving quick victories and fostering more institutionalized forms of inclusive governance. A one-time small pilot, however, is not enough to transform citizen engagement, which is why longer-term institutionalization is so important. Once projects are embedded within agencies and institutional structures, they are less vulnerable to leadership turnover and may, as a result, be able to expand in scope. Embedding pilots within government agencies has its own challenges, including securing a continuous

pipeline of leadership and resource support. Showing the quick victories from initial small pilots can be very helpful in overcoming these obstacles.

Conclusions

This article has tried to show that the conversation about civic tech need not be divorced from discussions on governance innovation and collaboration. On the contrary, civic tech can be used precisely to support more inclusive and responsive governance. Incorporating these techniques into a broader public administration toolkit requires an understanding of the lessons learned from prior implementations as well as dedicated leadership, structured multi-sector partnerships, and shared learning across contexts to deepen these processes. It will not happen overnight. However, democracy at its core has always been about experimentation and adaptation. Now is the time for public administrators to put these principles to the test.

References

Altschuler, A., & Behn, R. (1997). *Innovations in American government.* Washington, DC: The Brookings Institution.

Ansell, C., & Gash, A. (2007). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory,18*, 543-571. doi: 10.1093/jopart/mum032

Barber, B. R. (1984). *Strong democracy: Participatory politics for a new age*. Berkeley: University of California Press.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom.* New Haven, CT: Yale University Press.

Borins, S. (2001). Encouraging innovation in the public sector. *Journal of Intellectual Capital, 2*, 310-319.

Boyle, D. and Harris, M. (2009). *The challenge of co-production: How equal partnerships between professionals and the public are crucial to improving public services*. London: New Economics Foundation.

Chadwick, A. (2006). *Internet politics: State citizens, and new communication technologies.* Oxford: Oxford University Press.

Davies, R. (2014). *Civic crowdfunding: Participatory communities, entrepreneurs, and the political economy of place*. (Unpublished master's thesis). MIT, Cambridge, MA. doi: 10.2139/ssrn.2434615

Dewey, J. *Public and its problems*. (1954 [1927]). Athens, OH: Swallow Press/Ohio University Press.

Fung, A. (2003). Recipes for public spheres: Eight institutional design choices and their consequences. *Journal of Political Philosophy, 11*(3), 338–67. doi: 10.1111/1467-9760.00181

Fung, A. (2007). Democratic theory and political science: A pragmatic method of constructive engagement. *American Political Science Review, 101*(3), 443-458. doi: 10.1017/S000305540707030X

Fung, A. (2015). Putting the public back into governance: The challenges of citizen participation and its future. *Public Administration Review*, *75*(4), 513-522. doi: 10.1111/puar.12361. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/puar.12361/abstract

Fung, A., Russon Gilman, H., & Shkabatur, J. (2013). Six models for internet + politics. *International Studies Review, 15*, 20-47. doi: 10.1111/misr.12028

Gilens, M. (2012). *Affluence and influence: Economic inequality and political power in America.* Princeton, NJ: Princeton University Press.

Gonçalves, S. (2014). The effects of participatory budgeting on municipal expenditures and infant mortality in Brazil. *World Development, 53*, 94–110. doi:10.1016/j.worlddev.2013.01.009

Hartley, J. (2005). Innovation in governance and public service: Past and present. *Public Money & Management*, *25*, 27-34. doi: 10.1111/j.1467-9302.2005.00447.x

IBM Center for the Business of Government. (2011). *Using online tools to engage—and be engaged by—the public*. Washington, DC: Matt Leighninger. Retrieved from http://businessofgovernment.org/report/using-online-tools-engage-public

Kettl, D. (2015). The job of government: Interweaving public functions and private hands. *Public Administration Review, 75*(2)*, 219-229.* doi: 10.1111/puar.12336.

Knight Foundation. (2012). "Digital citizenship: Exploring the field of tech for engagement." Miami, FL. Retrieved from: http://www.slideshare.net/knightfoundation/knight-civictech

Lessig, Lawrence. (2011). *Republic, lost: How money corrupts Congress—And a plan to*

stop it. New York, NY: Twelve.

Moore, M. H. (2007). *Creating public value: Strategic management in government*. Cambridge, MA: Harvard University Press.

Moore, M. H. (2013). *Recognizing public value*. Cambridge, MA: Harvard University Press.

Moore, M., & Hartley, J. (2008). Innovative in governance. *Public Management Review,10*(1), 3-20.

mySociety. (2015). Who benefits from civic technology? Demographic and public attitudes research into the users of civic technologies. UK: Rebecca Rumbul.

Noveck, B. S. (2015). *Smart citizens, smarter state: The technologies of expertise and the future of governing*. Cambridge, MA: Harvard University Press.

Ostrom, E., & Baugh, W. H. (1973). *Community organization and the provision of police services*. Beverly Hills, CA: Sage Publications.

Peixoto, T., & Fox, J. (2016). When does ICT-enabled citizen voice lead to government responsiveness? In Duncan Edwards and Rosie McGee (Eds.), *Opening governance*. Institute of Development Studies.

Putnam, R. D. (2001). *Bowling alone: The collapse and revival of American Community*. New York, NY: Simon & Schuster.

Sampaio, R. C., & Peixoto, T. (2014). Electronic participatory budgeting: False dilemmas and true complexities. In Nelson Dias (Ed.), *Hope for democracy: Twenty-five years of participatory budgeting* (413-425). São Brás de Alportel, Portugal: In Loco. Retrieved from http://buergerhaushalt.org/sites/default/files/downloads/Studie_Hope_for_democracy_-_25_years_of_participatory_budgeting_worldwide.pdf

Shah, A. (2007). *Participatory budgeting*. Washington, DC: World Bank.

Shirky, C. (2008). *Here comes everybody: The power of organizing without organizations*. New York, NY: Penguin Group.

Sirianni, C. (2006). *Reinvesting in democracy*. Washington, DC: Brookings Institution Press.

Skocpol, T. (1999, July). Associations without members. *The American Prospect*.

Smith, G., & Ryan, M. (2014). Defining mini-publics: Making sense of existing conceptions. In Kimmo Grönlund, André Bächtiger, & Maija Setälä (Eds.), Deliberative mini-publics: Involving citizens in the democratic process. Colchester, UK: ECPR Press.

Sørensen, E., & Torfing, J. (2011). Enhancing collaborative innovation in the public sector. *Administration and Society, 43*(8), 842-868. doi: 10.1177/0095399711418768

Toyoma, Kentaro (2015) *"Geek Heresy: Rescuing Social Change from the Cult of Technology"* New York: Public Affairs.

Touchton, M., & and Wampler, B. (2014). "Improving Social Well-Being through New Democratic Institutions." *Comparative Political Studies* 47, no. 10, pp. 1442–69. doi:10.1177/0010414013512601.

Trippi, J. (2004). *The revolution will not be televised: Democracy, the Internet, and the overthrow of everything*. New York, NY: HarperCollins.

Semantic Analysis of One Million #GamerGate Tweets Using Semantic Category Correlations

Phillip R. Polefrone
PhD Candidate, Department of English and Comparative Literature
Columbia University
August 2016

Abstract

This paper develops a methodology for describing the contents of a controversy on a microblogging platform (Twitter) by measuring correlations in broad semantic categories. Over one million tweets were gathered daily from November 2015 to June 2016 using Tweepy and the Twitter API, over 280,000 of which were not retweets and thus contained unique data. Using a Python implementation of Roget's hierarchy of semantic categories, these tweets were collected in bins of one thousand and analyzed using a "bag of categories" model, or a categorized bag of words. The linear correlation of each category with the "WOMAN" category was measured and compared with a control group. The categories concomitant with "WOMAN" in the test corpus include some noise, but over all present a meaningful description of the conversation that adheres to its known qualities. This result suggests that a more developed version of this methodology could be used to detect conversational trends on social media platforms more easily and with less human labor than other similar methods.

Acknowledgements

This project received funding from Columbia's School of International and Public Affairs (SIPA) and the Carnegie Corporation of New York.

Introduction

At present, the common methodologies used to perform semantic analysis of social media content present many limitations. Much of the existing work on the topic of online harrassment uses network analysis (Baio 2014) or sentiment analysis (Wofford 2014), neither of which takes the specific semantic meaning of the posts themselves into account. Although the possibilities afforded by network analysis are exciting, it derives conclusions primarily from who is connected to whom, not the contents of any message sent. Sentiment analysis abstracts word meanings into a numeric value of positive or negative sentiment from a dictionary of human-

supplied sentiment ratings. While widely utilized, reducing semantic content to a single vector limits the meaningfulness and scope of the conclusions that can be drawn from it. By far the most promising of the common methods is the application of machine learning and statistical modeling techniques (Ostrowski 2015; Burnap & Williams 2015), but the requirements of these methods are at odds with the nature of many social media platforms. The need for large samples is inconsistent with the medium's usual brevity, while the need for human-generated training corpora makes keeping up with rapidly evolving conversations impractical. There is, then, a disconnect between methods that are flexible enough to keep up with the medium and those that are robust enough to provide meaningful conclusions.

This presents a potentially existential problem for social media platforms and their users. Platforms such as Twitter intends to give all users an equal platform, but ungoverned usage limits the ability of many women as well as racial, religious, and sexual minorities to enter these forums without fear of harassment or worse. The difficulty that faces a company trying to semantically classify posts automatically while keeping up with shifting topics means that a culture of harassment is able to persist and keep some users from the freedoms others enjoy. A method to provide more meaningful semantic analysis of posts in real time could ease the governance of these forums and ultimately help protect the right of all users to express themselves online.

The purpose of this paper is to outline and begin developing a method that uses broad semantic categories, derived from a hierarchy introduced in Roget's thesaurus, to detect the semantic content of social media trends. I will evaluate this method based on its ability to describe the content of the Twitter conversation marked by the #GamerGate hashtag, which has notoriously led to harassment and silencing of marginalized groups in the video gaming

community. I will analyze the raw counts of these categories using a “bag of categories” model in which a bag of words derived from a bin of one thousand tweets is replaced with the categories that describe each word. After normalizing these counts according to the total number of words in each bin, I will calculate the linear correlation of each word category with the “WOMAN” category. Finally, I will evaluate the resulting correlations by comparing them with a control group of 1.6 million tweets gathered by Stanford’s Sentiment140 group (2009).

I expect this approach to yield a sense of how a certain topic is being discussed by identifying correlative categories, or in other words, categories that covary according to shifts in the conversation. This study uses a much-discussed controversy so that its known features can be used to evaluate two factors: the extent to which the method is descriptive and the manner of its description. Because the method is still naive in ways described below, I expect some correlative categories to be descriptive and some to either qualify as noise or be difficult to interpret. In particular, I expect the categories that correlate with the “WOMAN” category to illustrate the harassment and denigration that has characterized the discussion, as well as the recourse to “freedom of speech” rhetoric that pro-GamerGaters are known to use as a smokescreen.

This approach rests on several basic assumptions. The first is that #GamerGate is a movement devoted to maintaining gaming culture’s domination by white heterosexual males, and that it achieves its goals by harassing, threatening, and overwhelming its opponents. This interpretation is consistent with most examinations of the movement beyond the pro-#GamerGate contingent itself, but those within the movement frequently claim it is about “media ethics.”[1] Some might claim that this assumption constitutes question-begging, but as I am

1 This claim is undercut by one of their key pieces of evidence. The movement began with a campaign against Zoe Quinn, a game developer best known as the creator of *Depression Quest*. Future participants in the movement began harrassing Quinn, alleging that she exchanged sex for favorable reviews for her games. It appears, however, that these claims

evaluating the method's effectiveness according to its ability to detect this trend rather than using the method to prove the existence of the trend, it should not present an issue. My second assumption is that Roget's word categories correspond meaningfully to a human understanding of language. This assumption is supported by findings that methods built on a Roget framework perform at a success rate similar to that of human users (Jarmasz & Szpakowicz 2012; McHale 1998; Klingenstein, Hitchcock, & DeDeo 2014).

Several methodological difficulties persist that will limit my findings. First, the tool I built to incorporate Roget's framework into a natural language processing suite is based on the 1911 edition of Roget's thesaurus (Roget 1991), meaning that fewer of the words will match the word-category dictionary than would be the case with a more recent version. The need for a digitized, plain text version for automatic processing restricted me to editions that had gone out of copyright, however, so without additional resources, this problem will persist. Second, no edition of the thesaurus has kept up with the rapidly changing contours of language on Twitter, meaning that much semantically meaningful and relevant content has been excluded from the model. Third, the rate of correspondence between the words in the corpus and those in the thesaurus could be improved by more sophisticated stemming and lemmatization. Finally, and perhaps most significantly, the project is hindered by Twitter's restrictive licensing policy, which has prevented me from obtaining the most relevant data from the beginning of the hashtag's lifespan. My data covers the second year of this lifespan, a period marked by self-referentiality and rehashing of previous arguments, while the ideal dataset would include data from the most

---

began with a post by a gilted ex-boyfriend, Eron Gjoni, which led to a cascade of misogynistic comments and threats that have characterized the discourse since (Parkin 2014).

volatile period (in the first month, before the bulk of the press coverage had occurred) when threats and harassment were at their most extreme.

Several terms that require more explicit definition. A **category** will refer to a numbered section in Roget's Thesaurus (1911). All categories refer to the lowest level of abstraction in the category hierarchy, unless otherwise indicated. (The full hierarchy is reconstructed in my "Roget Tools" based on the headings and subheadings above each category, and other levels of abstraction can be used.) A **mention** refers to a tweet that tags a user's screen name with the "@" sign, which causes notifications to be sent to that user and the tweet to appear in the user's timeline. A **hashtag** refers to a word or words preceded by a "#" and not separated by white space; it is a common convention on Twitter for linking tweets to an ongoing conversation. A **supertweet** is a term coined by [grant_online_2011] to describe the process of aggregating multiple tweets into bins for modeling and analysis. Supertweets in this paper contain one thousand tweets unless otherwise specified. A **bag of words** indicates a set of words to which order is irrelevant.

Review of Related Literature

Two categories predominate in the literature relevant to this study: computational studies of GamerGate and other instances of online harassment, and semantic analysis of text using Roget's or other word categories.

Studies of Online Harassment

Andy Baio's "72 Hours of #GamerGate" (2014) collects and analyzes the statistics of three days' worth of tweets using the "#GamerGate" hashtag and the associated users. He finds that ~69% of the tweets are retweets, which is reflected in my dataset. He also found that many

of the accounts responsible have a very low “age,” pointing out that “[r]oughly 25% of all Gamergate activity is coming from accounts created in the last two months [as of October 2014]” while the average account age for a general sample has a more even distribution (Baio 2014). Significantly, the #GamerGate hashtag is used ten times more frequently by pro-Gamergate users than anti-Gamergate users, meaning that findings using his hashtag disproportionately describe the pro-Gamergate side of the debate.

Taylor Wofford and Newsweek’s “Is Gamergate about Media Ethics or Harassing Women? Harassment, the Data Shows” (2014) uses sentiment analysis performed by the company BrandWatch to analyze a corpus of tweets representing the hashtag from September 1, 2014 to October 23, 2014. They found that a female game developer (Zoe Quinn) was mentioned in fourteen times as many tweets as a male game journalist (Nathan Grayson) despite both facing the same accusation. The same trend was found when comparing male and female journalists (Stephen Totilo and Leigh Alexander) writing in similar contexts. Although tweets directed at Grayson and Totilo were classified as more negative than those directed at Quinn, Alexander, and others, a greater number of negative tweets were found to be directed at the female users studied. The quantity of negative sentiment, then, taking into account the relative volume of tweets, was found to be greater in the tweets received by the female users studied.

Pete Burnap and Matthew L. Williams analyze the proliferation of hate speech following triggering events in “Cyber Hate Speech on Twitter: An Application of Machine Classification and Statistical Modeling for Policy and Decision Making” (Burnap & Williams 2015). The authors demonstrate the applicability of machine learning to social media contexts in which hate speech is present, using syntactical pattern recognition and a human-tagged training corpus.

Previous Applications of Roget's Categories for Semantic Analysis

I was introduced to Roget's category hierarchy as a methodology at a talk by Simon DeDeo on (Klingenstein et al. 2014), which uses these categories and latent Dirichlet allocation to map the "civilizing" trend in verdicts from London's Old Bailey legal archive. This study uses Roget's categories to "coarse grain" the language of trial transcripts, studying the shifting logic according to which crimes are classified as violent or non-violent. Latent Dirichlet allocation has been an effective method of topic modeling in other semantic studies of social media content as well, e.g. (Grant, George, Jenneisch, & Wilson 2011). I adopted their method of coarse-graining as well as adapting the method into an open-source tool for this study.

Jarmasz and Spakowicz (2012) and McHale (1998) have both demonstrated Roget-based methods' ability to detect word similarity comparable to human users. The latter also finds that the method compares favorably with WordNet, a similar tool. Stan Spakowicz has done extensive additional studies of using Roget's thesaurus as a natural language processing tool, including an exploration of automatic updating (Kennedy & Szpakowicz 2014).

Methodology

My methodology can be divided into three main steps:

1. Gathering test and control data
2. Classifying words by Roget's categories
3. Determining category correlation coefficients for test and control data

Gathering test and control data

I collected a live stream of tweets to create a corpus of test data by scheduling a daily automatic query of Twitter's API. Using Tweepy (2009), a Twitter API wrapper for Python, I gathered as many tweets as possible that use the "#GamerGate" tag between November 18, 2015

and June 30, 2016, a total of 1,049,890 tweets. Scrubbed of retweets, the total was 281,449 tweets. To clean the data, I eliminated all tokens with non-alphanumeric characters, including mentions and hashtags.

My control data is taken from Sentiment140's corpus, a Stanford University project that facilitates brand- and trend-based sentiment analysis (Sentiment140 2009). Using a range of queries, they gathered 1.6 million tweets, which I split into bins of 100,000 for comparison with the test data.

Classifying words by Roget's categories

To classify the words by category, Roget's thesaurus first had to be adapted for use in a natural language processing environment. I transformed the 1911 edition of the text from Project Gutenberg (1991) into a set of nested Python dictionaries, creating a catalog of words in the thesaurus according to the category or categories that describe them. In total, there are 1044 categories. Each of these categories can be traced up the hierarchy to categories at a higher level of abstraction if desired, though only the lowest level was used in this study.

After a "bag of words" was made out of each bin of one thousand tweets, each word was replaced by the category or categories that apply to it, resulting in a "bag of categories" containing where applicable and null categories where none applied. If a word fell into multiple categories, its ambiguity was preserved by including all relevant categories in the bag.

A frequency distribution was created for each bag of categories, providing a count for each category, which was then normalized for the total word count (categorized or not) for each bag. These normalized frequencies were recorded in a spreadsheet for correlation calculation.

This process was applied to both the test and control corpora, except that the test data used bins of 10,000 tweets and the control data used bins of 100,000 tweets. There were 282 bins for the test data and 108 bins for the control.

Determining category correlation coefficients for test and control data

For each set of data, I calculated the linear correlation of each word category with the "WOMAN" category across all the bags of categories derived from the bins of one thousand tweets. I then isolated the categories that were statistically significant ($p<.05$) for the number of samples. In the case of the control data, I chose the top twenty-five categories, all of which correlated to a degree that was statistically significant for the number of samples.

Analysis of Data

Table 1 shows the categories that correlate with "WOMAN" in the test data, and Table 2 shows these categories with the words in that category for additional interpretive context. Many of the category names in themselves are meaningful—"PENALTY" seems to point to calls for retribution by one side against the other, while "OSTENTATION" could either indicate criticism of the rhetoric of the other side of the argument or a common trope in criticizing women for attention to appearances (hardly unique to GamerGate in the history of misogyny). Other categories appear to be noise until the list of category words is inspected carefully. The baffling "HORIZONTALITY," for example, comes into focus when one considers that any instances of the word "lie" are being interpreted quite literally as "making oneself horizontal" when classification as an accusation of dishonesty would be more appropriate and meaningful.

Trends can be detected in this list of category correlations:

Words of Conflict

These are words that might appear as features of an argument regardless of the context of that argument, particularly a bitter argument between two clear sides that is defined by acrimony. Categories include:

- PENALTY, DECREMENT, DISCORD, INCREDULITY, PHYSICAL INSENSIBILITY, REGRESSION, VIRTUE, DECEIVER, RELINQUISHMENT, HELL, NOBILITY, REPETITION, TROPHY, TRUTH, INELEGANCE, HASTE, ENVY, MALEDICTION

Misogynistic Tropes

Like "OSTENTATION," discussed above, these categories are familiar in the history of vilifying women as a group. They include categories that, in context, seem to imply a reduction of a person to appearance or physicality, deemphasis of intellect, and implications of deception, dishonesty, or manipulation. Categories include:

- MATERIALITY, OSTENTATION, HORIZONTALITY/DECEIVER, ORNAMENT, DIMNESS, DECEIVER, PRODUCTIVENESS/PRODUCTION (birth, procreate, etc.), INGRATITUDE, JEWELRY, APPEARANCE, JEWELRY

Sexual Language

This list is self-explanatory, but there are several categories that I am including because the best explanation for the correlation with "WOMAN" is miscategorization of modern sexual slang. (In these instances, I will include the word in parenthesis.) Categories include:

- STREAM ("blow"), CARRIER ("ass"), SEXUALITY

These categories are almost entirely absent from the control group, as can be seen in Figure 3. Indeed, the contrast is surprisingly clear: the categories that most strongly correlate

with women in the control group are almost uniformly positive, so much so that there may be cause to look for experimental error. The top four categories, ‘FRIENDSHIP,’ ‘FAVORITE,’ ‘LOVE,’ ‘BENEVOLENCE,’ tell the tale of the distribution, and none of the categories at the top of the test distribution appear high up in the control group’s list. It appears that the category correlations exposed in the #GamerGate tweets are unique to that dataset.

Conclusions

As expected, this method of semantic analysis yielded results that are both descriptive and legible—even more legible than expected. There is a clear trend in these category correlations. In GamerGate’s corner of Twitter, women are discussed in terms of their material form and appearance, with reference to common misogynistic tropes, and in an inflammatory manner characteristic a bitter disputes. There is also a proliferation of sexual language that accompanies these categories. The mixture of these broad categories describes the trend that is visible to the human eye, but on a scale that exceeds what a human user can parse in a comparable amount of time.

Nevertheless, this is a naive instantiation of the methodology that leaves much more room for improvement. I did not deal with n-grams in this experiment, despite the presence of n-grams in Roget’s word dictionary. I also did not stem or lemmatize the words, which could have reduced the number of words that fell into a null category. Perhaps most important, I have not removed the archaic entries or attempted to update the word dictionary in any way. This introduces more noise into the system, but it also prevents the method from picking up many more modern terms. Some means of implementing a more modern version of the thesaurus, a

means of manipulating WordNet data to add entries to the dictionary, or a protocol for manual addenda could aid the process considerably.

Confidence in my interpretations is impossible without broadening the study to include other known controversies that are similarly acrimonious and have a clear target of abuse. There is sadly no shortage of misogynistic hashtags on Twitter, so replicating the results in other contexts should not present a challenge. Doing so requires being able to get to the epicenter of a controversy, though, and studying it from beginning to end. This will remain difficult as long as Twitter's licensing agreements and terms of use remain as obstructive as they currently are, so it is advisable to begin collecting data as early as possible when a useful topic emerges.

Finally, a word on the purpose of this study. Developing automatic semantic analysis is not meant as a first step in automatically blocking, punishing, or censoring users. Rather, it is meant as a way of flagging certain topics for monitoring by the governing bodies of a given social media forum. And contrary to what a pro-Gamergater would surely say, the intention is not to censor the speech of some users, but to make sure that everyone can participate in the modern public forum online without fear of threats or harassment. In a forum as huge as a platform like Twitter, some degree of automation is required to bring content to the attention of human arbiters.

Categories	Statistically Significant Correlations with "Woman" by Category (p < .05)
('WOMAN', 'cat0374')	1
('PENALTY', 'cat0974')	0.2165915529
('MATERIALITY', 'cat0316')	0.206136624
('OSTENTATION', 'cat0882')	0.1931942794
('DECREMENT', 'cat40.a')	0.175721327
('HORIZONTALITY', 'cat0213')	0.1661889801
('DISCORD', 'cat0414')	0.164865744
('SIMPLENESS', 'cat0042')	0.1579639682
('RESPECT', 'cat0928')	0.1572288105
('LEARNING', 'cat0539')	0.1561260369
('INCREDULITY', 'cat0487')	0.1536853448
('CARRIER', 'cat0271')	0.1493326214
('STREAM', 'cat0347')	0.1420658763
('ORNAMENT', 'cat0577')	0.139249848
('ARRIVAL', 'cat0292')	0.1370752301
('TEACHING', 'cat0537')	0.1364858972
('PHYSICAL INSENSIBILITY', 'cat0376')	0.1340969768
('REGRESSION', 'cat0283')	0.1334929839
('DISUSE', 'cat0678')	0.1316266895
('VIRTUE', 'cat0944')	0.1303371881
('DIMNESS', 'cat0422')	0.125913392
('MESSENGER', 'cat0534')	0.1242361704
('VALUE', 'cat812.a')	0.1238270939
('DECEIVER', 'cat0548')	0.1231316459
('DRYNESS', 'cat0340')	0.1210036872
('PUBLICATION', 'cat0531')	0.1204010077
('RELINQUISHMENT', 'cat0782')	0.1194993812
('LINING', 'cat0224')	0.1193638456
('ARTLESSNESS', 'cat0703')	0.119336499
('NECESSITY', 'cat0601')	0.1185088886

Figures:

Figure 1:

Category

Correlations

with

"WOMAN" in

Test Group

Figure 2: Correlating Category Words with “WOMAN” in Test Group

Roget Categories	Words	Correlation with “WOMAN”
WOMAN	['bachelor girl', 'betty', 'bitch', 'consanguinity', 'cotquean', 'cow', 'dame', 'doe', 'dowager', 'dyke', 'effeminate', 'estrogen', 'ewe', 'fair sex', 'female', 'feminality', 'feminine', 'feminist', 'feminize', 'frow', 'gammer', 'girl', 'good wife', 'good woman', 'goody', 'grisette', 'gynaecic', 'gynecaeum', 'gynecic', 'hen', 'henhussy', 'her', "hers.'", 'lady', 'ladylike', 'lesbian', 'lioness', 'madam', 'madame', 'maidenly', 'mare', 'matron', 'matronage', 'matronhood', 'matronly', 'mistress', 'mollycoddle', 'Mrs', 'muff', 'muliebrity', 'Nanny goat', 'new woman', 'nymph', 'oestrogen', 'old woman', 'paternity', 'petticoat', 'Pron', 'rani', 'roe', 'she', 'she-', 'she goat', 'sissy', 'softer sex', 'sow', 'squaw', 'suffragette', 'suffragist', 'tabita', 'the fair', 'the sex', 'tigress', 'unmanly', 'vixen', 'Vrouw', 'weaker vessel', 'wench', 'wife', 'wifely', 'woman', 'woman is the	1

	lesser man', 'womanhood', 'womanish', 'womankind', 'womanly']	
PENALTY	['amerce', 'amercement', 'confiscate', 'confiscation', 'damages', 'deodand', 'escheat', 'estreat', 'fine', 'forfeit', 'forfeiture', 'mulct', 'pain', 'pains and penalties', 'penalty', 'penance', 'retribution', 'sconce', 'sequester', 'sequestrate', 'sequestration', 'the devil to pay', 'weregild', 'wergild']	0.2165915529
MATERIALITY	['article', 'bodily', 'body', 'brute matter', 'corporal', 'corporality', 'corporeal', 'corporeity', 'corpus', 'element', 'experimental philosophy', 'flesh and blood', 'frame', 'hyle', 'impersonal', 'material', 'materialism', 'materialist', 'materialistic', 'materiality', 'materialness', 'materials', 'matter', 'natural philosophy', 'neuter', 'nonsubjective', 'object', 'objective', 'pabulum', 'palpable', 'parenchyma', 'physical', 'physical condition', 'physical science', 'physicism', 'physicist', 'physics', 'plenum', 'ponderable', 'principle', 'sensible', 'somatic', 'somatics', 'somatism', 'somatist', 'somatology', 'somatoscopic', 'something', 'still life', 'stocks and stones', 'stuff', 'substance', 'substantial', 'substantiality', 'substantialness', 'substratum', 'tangible', 'thing', 'unspiritual']	0.206136624

OSTENTATION	['all decked out', 'array', 'attitudinarian', 'attract attention', 'ball dress', 'be ostentatious', 'blazon forth', 'brandish', 'ceremonial', 'ceremonious', 'ceremony', 'chic', 'claptrap', 'come forward', 'coup de theatre', 'court dress', 'cry up', 'cut a dash', 'cut a figure', 'cut a splash', 'cut a splurge', 'dangle', 'dangle before the eyes', 'dash', 'dashing', 'decjed out', 'demonstration', 'display', 'dramatic', 'dress', 'dressed to kill', 'dressed to the nines', 'emblazon', 'endimanch_e', 'equipage', 'etiquette', 'evening dress', 'exhibit', 'exhibition', 'exposition', 'f=ete', 'fancy dress', 'field day', 'figure', 'figure away', 'flaming', 'flashing', 'flaunt', 'flaunting', 'flourish', 'flourish of trumpets', 'flying colors', 'fop', 'foppery', 'form', 'formal', 'formality', 'frippery', 'full dress', 'fuss', 'gairish', 'gala', 'garish', 'gaudy', 'gaudy as a butterfly', 'gaudy as a peacock', 'gaudy as a tulip', 'gay', 'glitter', 'glittering', 'grand', 'grand doings', 'grand function', 'hand out', 'have framed and glazed', 'high-sounding', 'hold up', 'in best bib and tucker', 'in Sunday best', 'insubstantial pageant', 'janty', 'jaunty', 'magnificence', 'magnificent', 'majestic', 'make a dash', 'make a display', 'make a show', 'make a splash', 'make a splurge', 'man millinery', 'march past', 'millinery', 'mount', 'mouth honor', 'mummery', 'ostentation', 'ostentatious', 'pageant', 'pageantry', 'palatial', 'parade', 'pomp', 'pomposity', 'pompous', 'pretense', 'pretensions', 'pretentious', 'prink', 'procession', 'promenade', 'punctilio', 'punctilious', 'punctiliousness', 'put a good face upon', 'put a smiling face upon', 'put forward', 'put oneself forward', 'review', 'ritual', 'set off', 'set out', 'show', 'show off', "show off one's paces", 'showing off', 'showy', 'solemn', 'solemn mockery', 'solemnity', 'spectacle', 'spectacular', 'splash', 'splendid', 'splendor', 'splurge', 'sport', 'stage effect', 'stage trick', 'star it', 'starched', 'starched stateliness', 'state', 'stateliness', 'stately', 'stiff', 'strut', 'sumptuous', 'tailoring', 'theatrical', 'tomfoolery', 'tour de force', 'trot out', 'turgid', 'turn out', 'with beat of drum', 'with flourish of trumpet', 'with flying colors']	0.1931942794
DECREMENT	['afterglow', 'decrement', 'deduction', 'defect', 'discount', 'eduction', 'loss', 'waste']	0.175721327

HORIZONTALITY	['accubation', 'accumbent', 'alluvial', 'azimuth', 'be horizontal', 'billiard table', 'bowling green', 'butte', 'calm', 'calm as a mill pond', 'couch', 'couchant', 'cricket ground', 'croquet ground', 'croquet lawn', 'dead flat', 'dead level', 'decumbence', 'decumbency', 'decumbent', 'discumbency', 'esplanade', 'estrade', 'even', 'fell', 'flat', 'flat as a billiard table', 'flat as a bowling green', 'flatness', 'flatten', 'floor', 'horizontal', 'horizontality', 'horizontally', 'jacent', 'knock down', 'lay down', 'lay out', 'ledge', 'level', 'level plane', 'lie', 'lie down', 'lie flat', 'lie prostrate', 'loll', 'lying', 'lying down', 'mesa', 'on all fours', 'on its beam ends', "on one's back", 'parterre', 'plain', 'plane', 'plateau', 'platform', 'procumbent', 'prone', 'proneness', 'prostrate', 'prostration', 'reclination', 'recline', 'recubant', 'recumbency', 'recumbent', 'render horizontal', 'resupination', 'sit down', 'smooth', 'smooth as glass', 'spirit level', 'sprawl', 'stratum', 'supination', 'supine', 'table land', 'terrace']	0.1661889801
DISCORD	['ajar', 'altercation', 'apple of discord', 'at cross purposes', 'at daggers drawn', 'at feud', 'at high words', 'at issue', 'at loggerheads', 'at odds', 'at sixes and sevens', 'at variance', 'barney', 'battle ground', 'be discordant', 'bear garden', 'bicker', 'bone of contention', 'bone to pick', 'brabble', 'brand of discord', 'brangle', 'brawl', 'breach', 'breach of the peace', 'break squares with', 'break with', 'breeze', 'broil', 'cat-and-dog life', 'clash', 'come amiss', 'commotion', 'conflict', 'contentious', 'contentiousness', 'controversial', 'controvert', 'cross purposes', 'declaration of war', 'declare war', 'demel_e', 'differ', 'difference', 'disaccord', 'disagree', 'disagreeing', 'disagreement', 'discord', 'discordant', 'disputant', 'disputatious', 'dispute', 'disputed point', 'disruption', 'dissension', 'dissent', 'dissentient', 'dissidence', 'dissonance', 'disturbance', 'disunion', 'disunite', 'disunited', 'division', 'division in the camp', 'Donnybrook', 'Donnybrook Fair', 'embranglement', 'embroil', 'embroiled', 'embroilment', 'enmity', 'entangle', 'faction', 'factious', 'fall foul of', 'fall out', 'family jars', 'fasten a quarrel on', 'feud', 'fish in troubled waters', 'fracas', 'get into hot water', 'gladiatorial', 'ground of quarrel', 'hate', 'have a bone to pick', 'have a crow to pluck with', 'have no measures with', 'have words', 'high words', 'hubbub', 'imbroglio', 'in hot water',	0.164865744

	'jangle', 'jar', 'jarring', 'join issue', 'jostle', 'jostling', 'kick up a dust', 'kick up a row', 'Kilkenny cats', 'litigant', 'litigate', 'litigation', 'litigious', 'live like cat and dog', 'misunderstand one', 'misunderstanding', 'nag', 'no love lost between them', 'odds', 'on bad terms', 'open rupture', 'out of tune', 'outbreak', 'part company with', 'pettifogging', 'pick a quarrel', 'pit against', 'polemic', 'polemics', 'pull different ways', 'put in issue', 'quarrel', 'quarrelsome', 'question at issue', 'racket', 'riot', 'rixation', 'row', 'rumpus', 'rupture', 'schism', 'screw loose', 'scrimmage', 'set against', 'set at odds', 'set together by the ears', 'shock', 'snarl', 'snip-snap', 'sow dissension', 'spar', 'spat', 'split', 'squabble', 'squall', 'stir up dissension', 'strange bedfellows', 'strife', 'subject of dispute', 'tiff', 'together by the ears', 'torn', 'towrow', 'tracasserie', 'troublous times', 'try conclusions', 'unpacific', 'unpacified', 'unreconciled', 'up in arms', 'variance', 'vexed question', 'warfare', 'widen the breach', 'with', 'words', 'wrangle', 'wrangling']	
SIMPLENESS	['bolt', 'clear', 'disentangle', 'elementary', 'eliminate', 'elimination', 'exclude', 'exclusive', 'exempt from', 'free from', 'get rid of', 'homogeneity', 'homogeneous', 'incomplex', 'neat', 'only', 'pure', 'purification', 'purify', 'purity', 'render simple', 'sheer', 'sift', 'sifting', 'simple', 'simpleness', 'simplify', 'single', 'unadulterated', 'unalloyed', 'unblended', 'uncombined', 'uncompounded', 'undecomposed', 'unfortified', 'uniform', 'unmingled', 'unmixed', 'unsophisticated', 'untinged', 'winnow']	0.1579639682
RESPECT	['admiration', 'all Hail!', 'approbation', 'attention', 'awe', 'bareheaded', 'bear respect for', 'bend the knee to', 'bow', 'bow to', 'cap in hand', 'ceremonious', 'command respect', 'consideration', 'courtesy', 'dazzle', 'decorous', 'defer to', 'deference', 'deferential', 'devoirs', 'devotion', 'do homage to', 'do honor to', 'do the honors', 'duty', 'egards', 'emeritus', 'entertain respect for', 'esteem', 'estimation', 'fall down before', 'fealty', 'genuflection', 'hail', 'hail!', 'hallow', 'have a high opinion of', 'hold a high opinion of', 'hold in reverence', 'homage', 'honor', 'honor pricks me on', 'impose', 'in deference to', 'in high esteem', 'in high estimation', 'inspire awe', 'inspire respect', "keep one's distance", 'kneel to', 'kneeling prostration', 'kowtow',	0.1572288105

	'look up to', 'make room', 'obeisance', 'obsequious', 'obsequiousness', 'observe due decorum', "on one's knees", 'overawe', 'pay attention', 'pay homage to', 'pay respect', 'pay tribute to', 'present arms', 'presenting arms', 'prostrate', 'prostrate oneself', 'regard', 'regards', 'render honor to', 'respect', 'respected', 'respectful', 'respecting', 'respects', 'revere', 'reverence', 'reverential', 'salaam', 'salute', 'saving your grace', 'saving your presence', 'show courtesy', 'stand upon ceremony', 'think much of', 'time-honored', 'to', 'venerable', 'venerate', 'veneration', 'with all due respect', 'with all respect', 'with due respect', 'with submission', 'with the highest respect', 'worship']	
LEARNING	['acquaint oneself with', 'acquire knowledge', 'acquired knowledge', 'acquirement', 'acquisition of knowledge', 'acquisition of skill', 'apprenticeship', 'apt', 'aptitude', "at one's books", 'attainment', 'be dismissed', 'be informed', 'be studious', 'be taught', 'burn the midnight oil', 'coach up', 'collect knowledge', 'con over', 'consume the midnight oil', 'cram', 'dip into', 'dismiss', 'docile', 'docility', 'drink in knowledge', 'drop out', 'edification', 'erudition', 'expel', 'flunk out', 'gain knowledge', 'gather knowledge', 'get knowledge', 'get up', 'glean information', 'glean knowledge', 'glean learning', 'go to college', 'go to school', 'go to the university', 'graduate', 'grind', 'imbibe knowledge', 'in statu pupillari', 'industrious', 'inquiry', 'kick out of school', 'learn', 'learn by heart', 'learn by rote', "learn one's trade", 'learning', 'leave school', 'lore', 'make oneself master of', 'master', 'matriculate', 'matriculation', "mind one's book", 'novitiate', 'obtain knowledge', 'perusal', 'peruse', 'pick up knowledge', 'pore over', 'prenticeship', 'pupilage', 'pupilarity', 'quit school', 'read', 'reading', 'receive knowledge', 'run the eye over', 'run the eye through', 'scholarly', 'scholarship', 'scholastic', 'self-instruction', 'serve an apprenticeship', "serve one's time", 'spell', 'studious', 'study', 'take a leave', 'take in knowledge', 'teachable', 'thumb over', 'transfer', 'turn over the leaves', 'tutelage', 'wade through', 'wide information']	0.1561260369

INCREDULITY	['be incredulous', 'cynic', 'cynical', 'cynicism', 'disposed to doubt', 'distrust', 'distrustful', 'hard of belief', 'heretic', 'hold aloof', 'ignore', 'inconvincible', 'incredulity', 'incredulous', 'incredulousness', 'indisposed to believe', 'misbeliever.a', 'mistrust', 'pyrrhonism!', 'pyrrhonist', 'refuse to believe', 'scrupulosity', 'scrupulous', "shut one's ears to", "shut one's eyes to", 'shy of belief', 'skeptic', 'skeptical', 'skepticism', 'suspicion', 'suspicious', 'suspiciousness', 'turn a deaf ear to', 'unbeliever', 'unbelieving', 'want of faith']	0.1536853448
CARRIER	['Arab', 'asinine', 'ass', 'barb', 'bayard', 'bearer', 'beast', 'beast of burden', 'bidet', 'blood horse', 'brace', 'broncho', 'bronco', 'Bucephalus', 'burro', 'camel', 'cargador', 'carriage', 'carrier', 'carrier pigeon', 'cart', 'cart horse', 'cattle', 'charger', 'cob', 'colt', 'conductor', 'conveyer', 'coolie', 'courser', 'cow pony', 'creature', 'critter', 'cuddy', 'dolley', 'donkey', 'draft horse', 'dray horse', 'dromedary', 'elephant', 'equine', 'express', 'expressman', 'filly', 'foal', 'fork lift', 'galloway', 'garran', 'garron', 'gelding', 'genet', 'goer', 'hack', 'hinny', 'horse', 'hunter', 'jackass', 'jade', 'jennet', 'jument', 'ketch', 'llama', 'locomotive', 'mare', 'motor', 'mule', 'mustang', 'nag', 'Narraganset', 'pack horse', 'pad', 'palfrey', 'pallet', 'Pegasus', 'pony', 'porter', 'post horse', 'punch', 'racehorse', 'racer', 'reindeer', 'roadster', 'roan', 'Rocinante', 'sheltie', 'shelty', 'Shetland pony', 'ship', 'stallion', 'stevedore', 'stud', 'sumpter horse', 'sumpter mule', 'support', 'thoroughbred', 'tit', 'tranter', 'waler']	0.1493326214
STREAM	['blow', 'flow', 'flowmeter', 'stream']	0.1420658763
ORNAMENT	['Alexandrine', 'alliteration', 'alliterative', 'altiloquence', 'altiloquent', 'antithesis', 'antithetical', 'artificial', 'beautified', 'big-sounding', 'big-sounding words', 'bombast', 'bombastic', 'declamation', 'declamatory', 'elegance', 'euphemism', 'euphemist', 'euphemistic', 'euphuism', 'euphuist', 'euphuistic', 'figurative', 'figurativeness', 'fine writing', 'flaming', 'flashy', 'florid', 'floridness c', 'flourish', 'flowers of rhetoric', 'flowers of speech', 'flowery', 'frills of style', 'frothy', 'fustian', 'grandiloquent', 'grandiose', 'high flowing', 'high flown', 'high-sounding', 'high-sounding words', 'inflated', 'inflation', 'inversion', 'Johnsonian', 'macrology', 'magniloquent', 'Minerva press', 'mouthy',	0.139249848

	'ornament', 'ornate', 'orotund', 'orotundity', 'overcharge', 'overlay with ornament', 'paronomasia', 'pedantic', 'phrasemonger', 'pompous', 'pretension', 'prose run mad', 'rant', 'rhetorical', 'rich', 'sententious', 'sesquipedal', 'sesquipedalian', 'sesquipedality', 'smell of the lamp', 'sonorous', 'stilted', 'swelling', 'teratology!', 'tumid', 'turgescence', 'turgescent', 'turgid', 'turgidity', 'well-rounded periods']	
ARRIVAL	['advent', 'airport', 'alight', 'all Hail!', 'anchorage', 'any port in a storm', 'arrival', 'arrive', 'arriving', 'attain', 'be in at the death', 'bounce upon', 'bunder', 'burst upon', 'cast anchor', 'come', 'come across', 'come at', 'come back', 'come home', 'come in', 'come in contact', 'come to', 'come to hand', 'come up to', 'come up with', 'come upon', 'complete', 'completion', 'debark', 'debarkation', 'de-orbit', 'deplane', 'destination', 'detrain', 'disembark', 'disembarkation', 'dismount', 'drop in', 'encounter', 'fetch', 'get back', 'get home', 'get to', 'go ashore', 'goal', 'goalpost', 'good morrow!', 'good-day', 'hail!', 'halting ground', 'halting place', 'harbor', 'haven', 'here', 'hit', 'hither', 'home', 'homeward bound', 'join', "journey's end", 'land', 'landing', 'landing place', 'landing stage', 'landing strip', 'light', 'light upon', 'make', "make one's appearance", 'make the land', 'meet', 'meeting', 'outspan', 'overtake', "pitch one's tent", 'pitch upon', 'plump upon', 'pop upon', 'port', 'put in', 'put into', 'reach', 'reception', 'recursion', 'rejoin', 'remigration', 'rencounter', 'resting place', 'return', 'runway', 'sit down', 'spaceport', 'terminal', 'terminus', 'visit', 'welcome', 'welcome!']	0.1370752301
TEACHING	['A,B,C,D,E,F', 'A.B.C.', 'academic', 'advise', 'apologue', 'beat into', 'beat into the head', 'book', 'book exercise', 'break', 'break in', 'breed', 'bring forward', 'bring up', 'bring up to', 'brute memory', 'calisthenics', 'chalk talk', 'classical education', 'coach', 'college education', 'collegiate education', 'convince', 'cooperative learning', 'course', 'course of study', 'cram', 'curriculum', 'denominational education', 'didactic', 'direct', 'direct attention to', 'direction', 'disciplinal', 'discipline', 'discourse', 'disseminate', 'doctrinal', 'drill', 'drynurse', 'edification', 'edify', 'educate', 'education', 'educational', 'elementary education', 'enlarge the mind', 'enlighten', 'exam', 'examination', 'excitation',	0.1364858972

	'exercise', 'exercise book', 'exercise for the student', 'explanation', 'expound', 'fail', 'familiarize with', 'final exam', 'form', "gentleman's C", 'give a discourse', 'give a lecture', 'give a lesson', 'give a sermon', 'give new ideas', 'given an idea of', 'graft', 'grammar', 'ground', 'guidance', 'guide', 'gymnastics', 'habituate', 'hold forth', 'homework', 'imbue', 'implant', 'impregnate', 'impress upon the memory', 'impress upon the mind', 'improve', 'incept', 'incomplete', 'inculcate', 'inculcation', 'indoctrinate', 'indoctrination', 'infiltrate', 'infix', 'infuse', 'ingraft', 'initiate', 'initiation', 'inoculate', 'inoculation', 'instill', 'instruct', 'instruction', 'instructional', 'instructive', 'inure', 'lecture', 'lesson', 'liberal education', 'marks', 'mid-term exam grade', 'military education', 'Montessori method', 'moral education', 'moral tuition', 'moralize', 'nurture', 'open the eyes', 'opsimathy', 'parable', 'pass', 'persuasion', 'phonics', 'physical drill', 'physical education', 'point a moral', 'practice', 'preach', 'preach to the converted', 'preach to the wise', 'preachment', 'preinstruct', 'preparation', 'prepare', 'primary education', 'prime', 'project', 'prolection', 'propaedeutic', 'propaedeutical', 'propaedeutics', 'propaganda', 'propagandism', 'proselytism', 'put in the way of', 'put to nurse', 'put up to', 'qualification', 'qualify', 'read a lesson', 'rear', 'religious education', 'rote', 'rote memorization', 'scholastic', 'school', 'schooling', 'score', 'secondary education', 'secular education', 'send to school', 'sermon', 'sermonize', 'set right', 'sharpen the wits', 'sloyd', 'sow the seeds of', 'take in hand', 'take-home lesson', 'tame', 'task', 'taught', 'teach', 'teach granny to suck eggs', 'teaching', 'technical education', 'test', 'the schoolmaster abroad', 'theme', "three R's", 'train', 'training', 'tuition', 'tutelage', 'tutor', 'tutorage', 'ungraded classes', 'university education', 'workbook']	
PHYSICAL INSENSIBILITY	['anaesthesia', 'anaesthetic', 'anaesthetic agent', 'anaesthetize', 'be insensible', 'benumb', 'blunt', 'callous', 'case hardened', 'chloral', 'chloroform', 'coma', 'comatose', 'dead', 'dull', 'ether', 'exhilarating gas', 'hard', 'hardened', 'have a rhinoceros hide', 'have a thick skin', 'hemiplegia', 'impercipient', 'insensibility', 'insensible', 'laughing gas', 'motor paralysis', 'nitrous oxide', 'numb', 'obtund', 'obtuse', 'obtuseness', 'opium', 'pachydermatous', 'pall',	0.1340969768

	'palsied', 'palsy', 'paraesthesia', 'paralysis', 'paralytic', 'paralyze', 'physical insensibility', 'proof', 'protoxide of nitrogen', 'refrigeration', 'render insensible', 'senseless', 'sleep', 'stun', 'stupefy', 'thick-skinned', 'unfeeling', 'vegetable state']	
REGRESSION	['as you were', 'back', 'back down', 'back out', 'backsliding', 'backtrack', 'backward movement', 'backwards', 'backwater', 'balk', 'balky', 'beat a retreat', 'come back', 'counter march', 'counter motion', 'counter movement', 'countermarch', 'crab-like', 'crab-like motion', 'crawl', 'dance the back step', 'deterioration', 'double', 'draw back', 'drop astern', 'ebb', 'fall', 'fall astern', 'fall back', 'flip-flop', 'get back', 'go back', 'go home', 'hark back', 'jib', 'lose ground', 'motion in reverse', 'put about', 'put back', 'reactionary', 'rebound', 'recede', 'receding', 'recess', 'recession', 'recidivation', 'recidivism', 'recidivity', 'recidivous', 'reculade', 'reflex', 'reflexively', 'refluence', 'refluent', 'reflux', 'regrade', 'regress', 'regression', 'regressive', 'regurgitate', 'regurgitation', 'relapse', 'remigration', 'resilience reflection', 'resilient', 'retire', 'retirement', "retrace one's steps", 'retreat', 'retroaction', 'retrocede', 'retrocession', 'retrograde', 'retrograde motion', 'retrograduation', 'retrogression', 'retrogressive', 'return', 'reversal', 'revert', 'run back', 'shrink', 'shy', 'sound a retreat', 'take the back track', 'tergiversation', 'to the right about', 'turn back', "turn one's back upon", 'turn round', 'turn tail', "turn upon one's heel", 'turning point', 'veer round', 'veering', 'wheel', 'withdraw', 'withdrawal']	0.1334929839
DISUSE	['abstain', 'abstinence', 'cast overboard', 'cast to the dogs', 'cast to the winds', 'desuetude', 'discard', 'dismantle', 'dismiss', 'dispense with', 'disusage', 'disuse', 'disused', 'do without', 'done with', 'forbear', 'forbearance', 'give warning', 'have done with', 'heave overboard', 'keep back', 'keep on the shelf', 'lay aside', 'lay by', 'lay on the shelf', 'lay up', 'lay up in a napkin', 'lay up in ordinary', 'leave off', 'let alone', 'lie unemployed', 'make away with', 'neglect', 'not required', 'not touch', 'not use', 'not used', 'put aside', 'relinquishment', 'remain unemployed', 'reserve', 'set aside', 'shelve', 'spare', 'supersede', 'throw aside', 'throw overboard', 'unapplied', 'uncalled for',	0.1316266895

	'unculled', 'undisposed of', 'unemployed', 'unessayed', 'unexercised', 'ungathered', 'unspent', 'untouched', 'untrodden', 'waive']	
VIRTUE	['above all praise', 'acquit oneself well', "act one's part", 'act well', 'admirable', 'angelic', "be on one's best behavior", "be on one's good behavior", 'be virtuous', 'beyond all praise', 'cardinal virtues', "command one's passions", 'commendable', 'correct', 'credit', 'creditable', 'desert', 'desertful', 'deserving', 'discharge of duty', "discharge one's duty", "do one's duty", 'duteous', 'dutiful', 'ethics', 'excellence', 'excellent', 'exemplary', 'fight the good fight', "fulfill one's duty", 'fulfillment of duty', 'godlike', 'good', 'good actions', 'good behavior', 'heaven-born', 'innocence', 'innocent', 'integrity', 'keep in the right path', "keep one's promise", 'laudable', "master one's passions", 'matchless', 'merit', 'meritorious', 'moral', 'moral rectitude', 'morality', 'morals', 'noble', 'nobleness', 'peerless', "perform one's duty", 'performance of duty', 'practice virtue', 'praiseworthy', 'pure', "redeem one's pledge", 'right', 'righteous', 'right-minded', 'saint-like', 'saintly', 'self-control', 'self-denial', 'seraphic', 'set a good example', 'set an example', 'sterling', 'virtue', 'virtuous', 'virtuously', 'virtuousness', 'virtus laudatur et alget', 'well-doing', 'well-intentioned', 'well-spent life', 'whole-souled', 'worth', 'worthy']	0.1303371881
DIMNESS	['aurora', 'be dim', 'bedim', 'blear', 'break of day', 'candlelight', 'cloud', 'cloudy', 'cockshut time', 'confused', 'crepuscular', 'crepuscule', 'dark', 'darken', 'darkish', 'darkness', 'dawn', 'daybreak', 'demi-jour', 'dim', 'dimness', 'dingy', 'dirty', 'dull', 'dun', 'dusk', 'eclipse', 'fade', 'faint', 'farthing candle', 'firelight', 'flicker', 'fuliginous', 'glassy', 'gliming', 'glimmer', 'grow dim', 'half light', 'lackluster', 'leaden', 'loom', 'looming', 'lower', 'lurid', 'misty', 'moonbeam', 'moonglade', 'moonlight', 'moonshine', 'muddy', 'muggy', 'nebular', 'nebulosity', 'nebulous', 'obnubilated', 'obscure', 'overcast', "owl's light", 'pale', 'pale its ineffectual fire', 'paleness', 'partial eclipse', 'partial shadow', 'render dim', 'rushlight', 'shades of evening', 'shadow of a	0.125913392

	shade', 'shadowed forth', 'shorn of its beams', 'starlight', 'tone down', 'twilight', 'twinkle']	
MESSENGER	['ambassador', 'apparitor', 'Ariel', 'bellman', 'cable', 'carrier pigeon', 'chore boy', 'courier', 'crier', 'dak', 'delivery service', 'emissary', 'envoy', 'errand boy', 'estafette', 'express mail', 'Federal Express', 'Fedex', 'flag bearer', 'gentleman of the press', 'herald', 'informer', 'internuncio', 'Iris', 'legate', 'letter bag', 'mail', 'marshal', 'Mercury', 'messenger', 'newsboy', 'next-day delivery', 'nuncio', 'overnight mail', 'own correspondent', 'penny-a-liner', 'post', 'post office', 'pursuivant', 'reporter', 'runner', 'scout', 'special correspondent', 'spy', 'telegraph', 'telephone', 'trumpeter', 'United Parcel Service', 'UPS', 'wire']	0.1242361704
VALUE	['appraisal', 'appraise', 'appraisement', 'appreciate', 'assess', 'assessment', 'cost', 'esteem', 'estimable', 'evaluate', 'fair price', 'full of worth', 'going price', 'intrinsic value', 'market price', "money's worth", 'par value', "penny's worth", 'precious', 'price current', 'quality', 'quotation', 'rate', 'valuable', 'valuation', 'value', 'what it will fetch', 'what the market will bear', 'worth', "worth a king's ransom", 'worth the price', 'worthwhile', 'worthy']	0.1238270939
DECEIVER	['actor', 'adventurer', "ass in lion's skin", 'Cagliostro', 'charlatan', 'cheat', 'cockatrice', 'conjuror', 'crimp', 'deceiver', 'decoy', 'decoy duck', 'dissembler', 'empiric', 'faker', 'false witness', 'Fernam Mendez Pinto', 'four flusher', 'fraud', 'gypsy', 'horse coper', 'humbug', 'hypocrite', 'imposter', 'Janus', 'Jesuit', 'jilt', 'jobber', 'jockey', 'Joseph Surface', 'Judas', 'juggler', 'knave', 'liar', 'man of straw', 'Mawworm', 'medicaster', 'mountebank', 'Pecksniff', 'perjurer', 'Pharisee', 'prestidigitator', 'pretender', 'quack', 'quacksalver', 'ringer', 'rogue', 'Rosicrucian', 'saltimbanco', 'saltimbanque', 'Scapin', 'serpent', 'shuffler!', 'snake in the grass', 'sophist', 'spieler', 'stool pigeon', 'story-teller', 'swindler', 'Tartufe', 'trickster', "wolf in sheep's clothing"]	0.1231316459

DRYNESS	['adust', 'anhydrous', 'arefaction', 'arescent', 'arid', 'aridity', 'be dry', 'be fine', 'blow dry', 'clothes drier', 'clothesline', 'dehydrate', 'dehydrated', 'dephlegmation', 'desiccate', 'desiccation', 'desiccative', 'dessicated', 'dessicator', 'drain', 'drainage', 'dried', 'drier', 'drought', 'dry', 'dry as a biscuit', 'dry as a bone', 'dry as a mummy', 'dry as a stick', 'dry as dust', 'dry up', 'drying oven', 'dryness', 'ebb tide', 'electric drier', 'exsiccate', 'exsiccation', 'fine', 'gas drier', 'hair drier', 'hang out to dry', 'hold up', 'husky', 'juiceless', 'kiln', 'kiln dry', 'low water', 'lyophilizer', 'mummify', 'oven dry', 'parch', 'rainless', 'render dry', 'sapless', 'sear', 'siccity', 'soak up', 'sponge', 'swab', 'undamped', 'vacuum dry', 'vacuum oven', 'water proof', 'water tight', 'wipe', 'without rain']	0.1210036872
PUBLICATION	['acquire currency', 'ad.', 'advertise', 'advertisement', 'affiche', 'arrant', 'bandy about', 'be public', 'be published', 'become public', 'bill', 'blaze about', 'blaze abroad', 'blazon', 'blow about', 'bring before the public', 'broach', 'broadside', 'bruit', 'bruit about', 'buzz about', 'circular', 'circular letter', 'circulate', 'circulation', 'come out', 'cry', 'currency', 'current', 'daily', 'diffuse', 'disseminate', 'drag before the public', 'drag into the open day', 'edit', 'edition', 'emit', 'encyclic', 'encyclical', 'evulugate', 'exoteric', 'find vent', 'flagrancy', 'flagrant', 'fly about', 'gazette', 'get about', 'get abroad', 'get afloat', 'get out', 'get wind', 'give forth', 'give out', 'give to the world', 'give tongue', 'go about', 'go forth', 'go the rounds', 'hawk about', 'herald', 'hue and cry', 'hype', 'imprint', 'in circulation', 'in open court', 'indiction', 'issue', 'journal', 'lay before the public', 'make known', 'make public', 'manifesto', 'newspaper', 'noise abroad', 'notice', 'notice is hereby given', 'notice!', 'notoriety', 'notorious', 'O yes!', 'open', 'Oyez!', 'pass current', 'pass from mouth to mouth', 'placard', 'post', 'post up afficher', 'poster', 'proclaim', 'proclaim at Charing Cross', 'proclamation', 'promulgate', 'promulgation', 'promulgatory', 'propagate', 'propagation', 'public', 'public announcement', 'public press', 'publication', 'publicity', 'publicly', 'publish', 'publish in the Gazette', 'published', 'publisher', 'put about', 'put forth', 'put forward', 'raise a cry', 'raise a hue and cry', 'raise a report', 'report', 'rumor', 'run like wildfire', 'see the light', 'send forth', 'send round the crier', 'set news	0.1204010077

	afloat', 'sound a trumpet', 'speak of', 'spread', 'spread abroad', 'spread like wildfire', 'take air', 'talk of', 'telegraphy', 'the press', 'these are to give notice', 'this is to give', 'thunder forth', 'trumpet forth', 'trumpet-tongued', 'utter', 'voice', 'vox populi', 'whisper about', 'with open doors']	
RELINQUISHMENT	['abandon', 'abandonment', 'away with!', 'be quit of', 'be rid of', 'cast aside', 'cast away', 'cast behind', 'cast off', 'cast overboard', 'cast to the dogs', 'cast to the winds', 'cede', 'cession', 'culls', 'derelict', 'dereliction', 'disburden oneself of', 'discard', 'discards', 'dismiss', 'dispensation', 'dispose of', 'dispossess oneself of', 'divest oneself of', 'drop', 'eject', 'expropriate!', 'expropriation!', 'fling aside', 'fling away', 'fling overboard', 'fling to the dogs', 'forego', 'foundling', 'garbage', 'get quit of', 'get rid of', 'give away', 'give notice to quit', 'give up', 'give warning', 'jetsam', 'jettison', 'lay apart', 'lay aside', 'lay down', 'lay on the shelf', 'left', 'let go', 'let slip', 'make away with', 'maroon', 'part with', 'pitch aside', 'pitch away', 'pitch overboard', 'pitch to the dogs', 'put aside', 'put away', "quit one's hold", 'quitclaim', 'quitclaim deed', 'refuse', 'reject', 'rejects', 'relinquish', 'relinquished', 'relinquishment', 'renounce', 'renunciation', 'resign', 'resignation', 'rid oneself of', 'riddance', 'rubbish', 'set aside', 'spare', 'supersede', 'surrender', 'sweep away', 'sweep to the winds', 'throw aside', 'throw away', 'throw overboard', 'throw to the dogs', 'throw to the winds', 'turn away', 'unappropriated', 'unculled', 'unowned', 'waif', "wash one's hands of", 'yield']	0.1194993812
LINING	['coating', 'fill', 'filling', 'incrust', 'inner coating', 'line', 'lined', 'lining', 'pad', 'padding', 'stalactite', 'stalagmite', 'stuff', 'stuffing', 'wad', 'wadding', 'wainscot', 'wall']	0.1193638456

ARTLESSNESS	['abandon', 'aboveboard', 'Arcadian', 'artless', 'artlessness', 'be artless', 'be free with one', 'blunt', 'bonhomie', 'call a spade a spade', 'candid', 'candor', 'confiding', 'direct', 'downright', 'frank', 'frank-hearted', 'free-spoken', 'guileless', 'honest', 'honesty', 'in plain English', 'in plain words', 'inartificial', 'ingenu', 'ingenuous', 'innocence', 'innocent', 'lain', 'look one in the face', 'matter of fact', 'matter of fact man', 'naive', 'naivete', 'native', 'natural', 'nature', 'not to mince the matter', 'open', 'open as day', 'open-hearted', 'outspoken', 'plain speaking', 'plain-spoken', 'pure', 'rough diamond', 'simple', 'simple-hearted', 'simple-minded', 'simplicity', 'sincere', 'sincerity', 'single-hearted', 'single-minded', 'singleness of heart', 'singleness of purpose', "speak one's mind", 'speak out', 'straightforward', 'think aloud', 'unaffected', 'undesigning', 'unflattering', 'unpoetical', 'unreserved', 'unsophisticated', 'unsuspicious', 'untutored']	0.119336499
NECESSITY	['adverse necessity', 'astral influence', 'automatic', 'automaton', 'avoidless', 'be destined', 'be doomed', "be one's fate", 'befated', 'blind', 'blind impulse', 'book of fate', 'by stress of', 'cast a spell', 'compel', 'compulsion', 'destination', 'destine', 'destined', 'destiny', 'devote', 'dire necessity', 'doom', 'elect', 'election', 'fatalism', 'fatalist', 'fatality', 'fate', 'fated', 'Fates', 'foredoom', 'foreordination', "God's will", 'hard necessity', 'have no alternative', 'have no choice', "Hobson's choice", 'Ides of March', 'if need be', 'imperious necessity', 'impulsive', 'in for', 'inborn proclivity', 'inevitable', 'inevitableness', 'inexorable', 'inexorable necessity', 'innate proclivity', 'instinct', 'instinctive', 'involuntariness', 'involuntary', 'iron necessity', 'irresistible', 'irrevocable', 'it cannot be helped', 'it is written', 'it must be', 'it must be so', 'it needs to be', 'it will be', 'it will have its way', 'kismet', 'last resort', 'last shift', 'lie under a necessity', 'lot fortune', 'mechanical', 'native tendency', 'natural impulse', 'natural tendency', 'necessarian', 'necessaries', 'necessarily', 'necessary', 'necessitarian', 'necessitate', 'necessitation', 'necessity', 'needful', 'needs must', 'obligation', 'of course', 'of necessity', "one's days are numbered", "one's fate is sealed", 'Parcae', 'perforce', 'pis aller', 'planet', 'planets', 'predestination', 'predestine', 'predetermination', 'preordain', 'preordination', 'resistless', 'Sisters three', 'sky', 'spell', 'spellbound	0.1185088886

	compulsory', 'star', 'stars', 'stern necessity', 'subjection', 'the die is cast', 'there is no help for', 'there is no helping it', 'to be unable to help', 'unavoidable', 'unconscious', 'uncontrollable', 'under the necessity of', 'unintentional', 'unthinking', 'unwitting', 'what must be', 'wheel of Fortune', 'will he nil he', 'will of Heaven', 'willing or unwilling', 'willy nilly']	
PRODUCTIVENESS	['aftercrop', 'aftergrowth', 'aftermath', 'arrish', 'conceive', 'eddish', 'fecund', 'fecundate', 'fecundify', 'fecundity', 'fertile', 'fertility', 'fertilization', 'fertilize', 'fructification', 'fructify', 'frugiferous', 'fruit-bearing', 'fruitful', 'generate', 'generative', 'hydra', 'impregnate', 'life-giving', 'luxuriance', 'luxuriant', 'make productive', 'milch cow', 'multiparous', 'multiplication', 'multiply', 'omnific', 'parturient', 'pregnancy', 'pregnant', 'procreant', 'procreate', 'procreation', 'procreative', 'produce', 'productive', 'productiveness', 'profitable', 'prolific', 'propagable', 'propagation', 'protoplasm', 'pullulation', 'rabbit', 'rowen', 'second crop', 'seed plot', 'spermatic', 'spermative', 'superfetation', 'teem', 'teemful', 'teeming', 'uberous', 'uberty', 'warren']	0.1182832252
HELL	['Abaddon', 'abyss', 'bottomless pit', 'Cocytus', 'Domdaniel', 'eternal damnation', 'everlasting fire', 'everlasting torment', 'gehenna', 'Hades', 'hell', 'hell fire', 'hellish', 'infernal', 'infernal regions', 'inferno', 'jahannan', 'limbo', 'Pandemonium', 'pit of Acheron', 'place of torment', 'Pluto', 'purgatory', 'realms of Pluto', 'Rhadamanthus', 'shades below', 'sheol', 'stygian', 'Stygian creek', 'Styx', 'Tartarus', 'Tophet', 'worm that never dies']	0.1154839513
NOBILITY	['ameer', 'aristocracy', 'aristocrat', 'aristocratic', 'armiger', 'atheling', 'banneret', 'baron', 'baronet', 'baronetcy', 'be noble', 'begum', 'better sort magnates', 'big bug', 'big gun', 'bigwig', 'birth', 'blood', 'blue blood of Castile', 'boyar', 'celebrity', 'chevalier', 'condition',	0.1151248159

	'count', 'countess', 'courtly', 'dame', 'distinction', 'Do$a', 'don', 'donship', 'duchess', 'duke', 'earl', 'effendi', 'elite', 'emir', 'esquire', 'every inch a king', 'exalted', 'fashionable world', 'genteel', 'gentility', 'gentlefolk', 'gentleman', 'gentlemanlike', 'gentry', 'grandee', 'great folks', 'great gun', 'great man', 'hidalgo', 'high-', 'high descent', 'high life', 'highly respectable', 'house of lords', 'house of peers', 'in high quarters', 'king', 'knight', 'knighthood', 'lady', 'laird', 'laureate', 'Lord', 'lordling', 'lords', 'magnate', 'maharaja', 'maharani', 'man of distinction', 'man of mark', 'man of rank', 'marchioness', 'margrave', 'marquis', 'marquisate', 'memsahib', 'nawab', 'nobility', 'noble', 'nobleman', 'noblesse', 'notabilities', 'notables', 'of gentle blood', 'of rank', 'optimacy', 'optimates', 'order', 'palsgrave', 'pantisocracy', 'pasha', 'patrician', 'peer', 'peerage', 'personage of distinction', 'personage of mark', 'personage of rank', 'primates', 'prince', 'princely', 'princess', 'quality', 'rajah', 'rani', 'rank', 'sahib', 'scherif', 'seignior', 'sharif', 'signior', 'squirarchy', 'squire', 'squireen', 'star', 'superstar', 'swell', 'thane', 'three-tailed bashaw', 'titled', 'upper classes', 'upper ten thousand', 'vavasour', 'viscount', 'waldgrave', 'wali', 'well-born']	
REPETITION	['a number of times', 'above-mentioned', 'above-said', 'aforenamed', 'aforesaid', 'afresh', 'again', 'again and again', 'anew', 'another', 'battologize', 'battology', 'begin again', 'bis', 'burden of a song', 'chimes', 'chiming', 'cuckoo', 'cut and come again', 'day by day', 'de novo', 'diffuseness', 'din in the ear', 'ding-dong', 'ditto', 'do over again', 'drum', 'drum in the ear', 'drumming', 'echo', 'encore', 'ever recurring', 'frequent', 'frequently', 'full many a time', 'go over the same ground', 'go the same round', 'habitual', 'hammer', 'harp on the same string', 'harp upon', 'harping', 'incessant', 'iterate', 'iteration', 'iterative', 'many a time', 'many times', 'many times over', 'mocking', 'monotonous', 'monotony', 'never hear the last of', 'new edition', 'often', 'old song', 'old story', 'once more', 'over again', 'over and over', 'over and over again', 'periodicity', 'pleonasm', 'pleonastic', 'reappear', 'reappearance', 'recapitulate', 'recapitulation', 'recur', 'recurrence', 'recurrent', 'recurring', 'recurse', 'recursion', 'recursive', 'recursively', 'redouble', 'redundancy', 'redundant',	0.1151155849

	'reecho', 'refrain', 'rehearsal', 'rehearse', 'reiterate', 'reiteration', 'renew', 'renewal', 'repeat', 'repeated', 'repeatedly', 'repetend', 'repetition', 'repetitional', 'repetitionary', 'reproduce', 'reproduction', 'resume', 'retold', 'return', 'return to', 'reverberation', 'revert', 'reword', 'rhythm', 'ring the changes on', 'ritornello', 'run', 'say over again', 'second edition', 'several times', 'succession', 'tautology', 'tautophony', 'thick coming', 'time after time', 'time and again', 'twice-told tale', 'unvaried', 'year after year']	
TROPHY	['award', 'bays', 'chaplet', 'civic crown', 'crown', 'decoration', "feather in one's cap", 'flying colors', 'for valor', 'garland', 'insignia', 'Iron Cross', 'laurel', 'laurels', 'medal', 'monumentum aere', 'palm', 'prize', 'triumph', 'triumphal arch', 'trophy', 'Victoria Cross', 'wreath']	0.1148663446
EXCLUSION	['exclusion']	0.1142314335
INGRATITUDE	['be ungrateful', 'benefits forgot', 'et tu Brute!', 'forget benefits', 'forgotten', 'ill-requited', 'ingrate', 'ingratitude', 'insensible of benefits', 'oblivion of benefits', 'thank you for nothing!', 'thankless', 'thankless office', 'thankless task', 'thanklessness', 'thanks for nothing!', 'unacknowledged', 'ungrateful', 'unmindful', 'unrequited', 'unrewarded', 'unthanked', 'unthankful', 'unthankfulness', 'wanting in gratitude']	0.1127440083
TRUTH	['accuracy', 'accurate', 'actual', 'actually', 'at all events', 'at any rate', 'authentic', 'authenticity', 'be the case', 'be true', 'categorically true', 'certain', 'certainly', 'chapter and verse', 'clean-cut', 'clear-cut', 'clockwork precision', 'close', 'conformity to rule', 'constant', 'correct', 'correctitude', 'correctness', 'curious', 'definite', 'definitively true', 'delicacy', 'delicate', 'empirically true', 'ex officio', 'exact', 'exact truth', 'exactitude', 'exactly', 'exactness', 'experimentally verified', 'fact', 'faithful', 'fine', 'genuine', 'get at the truth', "God's honest truth", 'gospel', 'gospel truth', 'have the true ring', 'hold good', 'hold true', 'hold water', 'honest truth', 'in all respects', 'in effect', 'in every respect', 'in its true colors', 'in reality', 'indeed',	0.1114875163

	'intrinsic truth', 'just', 'just so', 'just the thing', 'legitimate', 'literal', 'literally', 'mathematical', 'mathematical precision', 'naked truth', 'natural', 'nature', 'neither more nor less', 'nice', 'nicety', 'not an illusion', 'official', 'orthodox', 'orthodoxy', 'orthology', 'particular', 'plain fact', 'plain matter of fact', 'plain truth', 'precise', 'preciseness', 'precision', 'prove true', 'proven', 'pukka', 'punctual', 'punctuality', 'pure', 'real', 'real Simon Pure', 'realism', 'realistic', 'reality', 'really', 'religiously exact', 'render true', 'right', 'rigid', 'rigor', 'rigorous', 'rigorously true', 'sand the test', 'scientific', 'scrupulous', 'severe', 'sic', 'so', 'sober truth', 'solid', 'sound', 'sterling', 'stern truth', 'strict', 'strictly speaking', 'substantial', 'substantially true', 'substantiate', 'substantiated', 'tangible', 'the fact is', 'the truth is', 'the very thing', 'to a hair', 'to a nicety', 'to a T', 'to a tittle', 'to a turn', 'to an inch', 'to the letter', 'true', 'true as gospel', 'true by definition', 'true to the letter', 'truly', 'truth', 'unadulterated', 'unaffected', 'unalloyed', 'unalloyed truth', 'uncolored', 'unconfuted', 'undisguised', 'undistorted', 'unerring', 'unexaggerated', 'unflattering', 'unideal', 'unimagined', 'unimpeachable', 'unqualified truth', 'unquestionably true', 'unreconfuted', 'unromantic', 'unsophisticated', 'unvarnished', 'unvarnished tale', 'unvarnished truth', 'valid', 'veracious', 'veracity', 'verbatim', 'verified', 'verily', 'veritable', 'verity', 'well founded', 'well-defined', 'well-grounded', 'with truth', 'word for word']	
SIMPLICITY	['bald', 'bare', 'be simple', 'chaste', 'chastity', 'dull', 'flat', 'free from affectation', 'free from ornament', 'homeliness', 'homely', 'homespun', 'household', 'ingenuous', 'inornate', 'ordinary', 'plain', 'plainness', 'render simple', 'severe', 'simple', 'simplicity', 'simplify', 'sincere', 'unadorned', 'unaffected', 'unarranged', 'uncomplicate', 'undecked', 'undress', 'ungarnished', 'unornamented', 'untrimmed', 'unvarnished']	0.1113601904
DISAPPEARANCE	['avaunt', 'avaunt!', 'be gone', 'be lost to view', 'departure', 'disappear', 'disappear!', 'disappearance', 'disappearing', 'dissolve', 'dissolving views', 'eclipse', 'efface', 'evanescence', 'evanescent', 'evaporate', 'exit', 'fade', 'get lost!', 'get out of here', 'go', 'go off the stage', 'gone', 'leave no trace', "leave 'not a rack behind'", 'lose sight of', 'lost', 'lost to sight', 'lost to view', 'melt away',	0.1107975112

	'missing', 'occultation', 'pass', 'pass out of sight', 'retire from sight', 'suffer an eclipse', 'undergo an eclipse', 'vanish', 'vanish!', 'vanishing point', 'vaporize']	
DEPUTY	['ablegate', 'accredit', 'accredited to', 'acting', 'alter ego', 'answer for', 'appear for', 'archon', 'badli', 'be deputy', 'champion', 'chancellor', 'commissioner', 'consul', 'delegate', 'deputy', 'eight', 'eleven', 'hold a brief for', 'in behalf of', 'lieutenant', 'locum tenens', 'minister', 'next friend', 'plenipotentiary', 'prefect', 'premier', 'proconsul', 'provost', 'proxy', 'regent', 'represent', 'representative', 'secondary', 'stand for', 'stand in the shoes of', 'stand in the stead of', 'substitute', 'surrogate', 'team', 'Tsung-li Yamen', 'vicar', 'vice', 'vice regal', 'viceregent', 'viceroy', 'vizier', 'Wai Wu Pu', 'walk in the shoes of', 'warden']	0.1103944717
EXTRINSICALITY	['accident', 'accidental', 'adscititious', 'adventitious', 'apparent', 'appearance', 'ascititious', 'contingent', 'derived from without', 'extraneous', 'extraneousness', 'extrinsic', 'extrinsical', 'extrinsicality', 'extrinsically', 'fortuitous', 'implanted', 'incidental', 'inculcated', 'infused', 'ingrafted', 'modal', 'non ego', 'nonessential', 'objective', 'objectiveness', 'outward', 'phenomenon']	0.110272255
LANGUAGE	['Babel', 'betacism', 'bilingual', 'chrestomathy', 'classics', 'comparative grammar', 'confusion of tongues', 'current', 'dead languages', 'dialect', 'dialectic', 'diglot', 'express by words', 'genius of language', 'glossology', 'glottology', 'hexaglot', 'household words', 'humanities', "King's English", 'language', 'letters', 'lexicology', 'lingo', 'lingual', 'linguistic', 'linguistics', 'literary', 'literature', 'mimmation', 'mother tongue', 'muses', 'myatism', 'native tongue', 'nunnation', 'onomatopoeia', 'paleography', 'paleology', 'pantomime', 'pasigraphie', 'pasigraphy', 'philology', 'phraseology', 'polite literature', 'polyglot', "Queen's English", 'republic of letters', 'scholarship', 'speech', 'tongue', 'vernacular', 'vulgar tongue']	0.1101934587

JEWELRY	['agate', 'alexandrite', 'amethyst', 'anklet', 'balais', 'bejeweled', 'beryl', 'bijou', 'bijoutry!', 'bloodstone', 'bracelet', 'brilliant', 'broach', 'carbuncle', 'carcanet', "cat's eye", 'chain', 'chalcedony', 'charm bracelet', 'chatelaine', 'chrysolite', 'coral', 'costume jewelry', 'cubic zirconia', 'cultured pearl', 'diamond', 'earring', 'emerald', 'fine jewelry', 'fresh-water pearl', 'garnet', 'gem', 'gemmology', 'gemological', 'gemologist', 'gemology', 'gemstone', 'girasol', 'girasole', 'heliotrope', 'hematite', 'hyacinth', 'jacinth', 'jasper', 'jewel', 'jeweler', 'jewellery', 'jewelry', 'junk jewelry', 'lapel pin', 'lapidarian', 'lapidary', 'lapis lazuli', 'locket', 'minerologist', 'minerology', 'moonstone', 'mother of pearl', 'necklace', 'onyx', 'opal', 'oriental', 'oriental topaz', 'pearl', 'pendant', 'peridot', 'pin', 'pinky ring', 'plasma', 'precious stone', 'ring', 'rock', 'ruby', 'sapphire', 'sard', 'sardonyx', 'shine like a diamond', 'spinel', 'spinelle', 'sunstone', 'synthetic ruby', 'torque', 'tourmaline', 'trinket', 'turquois', 'turquoise', 'zircon']	0.1081389002
PRODUCTION	['abiogenesis', 'accomplish', 'accouchement', 'achieve', 'achievement', 'acquire', 'albumen', 'archebiosis', 'archegenesis', 'architectonic', 'architecture', 'assimilation', 'authorship', 'be brought to bed of', 'bear', 'bear fruit', 'beget', 'big with', 'biogenesis', 'biogeny', 'birth', 'birth-throe', 'breed', 'bring forth', 'bring into being', 'bring into existence', 'bring up', 'bringing forth', 'brought to bed of', 'build', 'building', 'call into being', 'carve', 'cause', 'childbirth', 'chisel', 'coin', 'coinage', 'compose', 'confinement', 'constitute', 'construct', 'construction', 'contrive', 'create', 'creation', 'creative', 'delivery', 'develop', 'development', 'diaster', 'digenesis', 'digenetic', 'dissogeny', 'do', 'drop', 'dysmerogenesis', 'ean', 'ectogenous', 'edification', 'edifice', 'edify', 'enceinte', 'engender', 'entelechy', 'epigenesis', 'erect', 'erection', 'establish', 'establishment', 'eumerogenesis', 'evolution', 'evolve', 'fabric', 'fabricate', 'fabrication', 'farrow', 'fecundate', 'fecundation', 'fertilization', 'flower', 'flowering', 'forge', 'form', 'formation', 'formative', 'frame', 'fraught with', 'fructification', 'fructify', 'fruit', 'gamic', 'gar', 'gemination', 'generate', 'generation', 'genesis', 'genetic', 'genial', 'genital', 'geniture', 'germination', 'gestation', 'get', 'give birth to', 'growth', 'haematobious', 'hatch', 'heterogamy', 'heterogenesis', 'heterogenetic', 'homogenesis', 'impregnate',	0.1077672931

	'impregnation', 'in the family way', 'in the straw', 'induce', 'inflorescence', 'institute', 'kindle', 'kitten', 'labor', 'lay', 'lie in', 'make', 'make productive', 'manufacture', 'merogenesis', 'metogenesis', 'midwifery', 'monogenesis', 'obstetrics', 'oeuvre', 'oogenesis', 'oogenetic', 'operate', 'opus', 'organization', 'organize', 'parthenogenesis', 'parturient', 'parturition', 'perform', 'performance', 'pile', 'pregnant', 'procreate', 'procreation', 'produce', 'produced', 'producing', 'production', 'productive of', 'progenerate', 'progeneration', 'prolific', 'propagate', 'propagation', 'publication', 'puerperal', 'puerperous', 'pullulate', 'pup', 'put together', 'putting together', 'raise', 'rear', 'run up', 'set up', 'spontaneous generation', 'sporogenous', 'sporophorous', 'structure', 'superinduce', 'suscitate', 'teem', 'teeming', 'tocogony', 'tower', 'travail', 'usher into the world', 'vacuolization', 'weave', 'whelp', 'workmanship', 'works', 'xenogenesis1', 'xenogenetic', 'xenogeny', 'yean']	
INELEGANCE	['abrupt', 'affected', 'artificial', 'awkward', 'barbarism', 'barbarous', 'be inelegant', 'cacophony', 'cramped', 'crude', 'dry', 'euphuism', 'euphuistic', 'forced', 'formal', 'fustian', 'graceless', 'grotesque', 'halting', 'harsh', 'inelegance', 'inelegant', 'labored', 'mannered', 'mannerism', 'marinism', 'offensive to ears polite', 'ponderous', 'rude', 'slang', 'solecism', 'stiff', 'stiffness', 'turgid', 'uncourtly', 'uncouth', 'ungraceful', 'unlettered Muse', 'unpolished']	0.1063138159
APPEARANCE	['air', 'angle', 'apparent', 'apparently', 'appear', 'appearance', 'as it seems', 'aspect', 'assume the appearance', 'assume the semblance of', 'at first sight', 'at the first blush', 'be visible', 'bear the appearance of', 'bear the semblance of', 'become visible', 'biograph', "bird's-eye view", 'carriage', 'carry the appearance of', 'carry the semblance of', 'cast', 'cast of countenance', 'cinematograph', 'color', 'complexion', 'contour', 'cosmorama', 'countenance', 'coup de theatre', 'cut a figure', 'cut of one s jib', 'demeanor', 'diorama', 'display', 'dissolving views', 'exhibit the appearance of', 'exhibit the semblance of', 'exposure', 'expression', 'face', 'face of the thing', 'figure', 'first blush', 'gallanty-show', 'georama', 'guise', 'have the appearance of', 'have the semblance of', 'image', 'in the eyes of',	0.1059099484

	'insignia', 'landscape', 'light', 'look', 'look like', 'lookout', 'magic lantern', 'metoposcopy', 'mien', 'moving pictures', 'on the face of it', 'on view', 'ostensible', 'ostensibly', 'outline', 'outlook', 'outside', 'pageant', 'pageantry', 'panorama', 'peep-show', 'perspective', 'phantasm', 'phantasmagoria', 'phantom', 'phase', 'phasis', 'phenomenon', 'phiz.', 'physiognomy', 'picture', 'point of view', 'port', 'premonstration', 'presence', 'present the appearance of', 'present the semblance of', 'present to the view', 'profile', 'prospect', 'raree-show', 'rising of the curtain', 'scene', 'scenery', 'seem', 'seeming', 'seemingly', 'shape', 'show', 'sight', 'species', 'spectacle', 'tableau', 'take on the appearance of', 'take on the semblance of', 'take the appearance of', 'take the semblance of', 'to all appearance', 'to all seeming', 'to the eye', 'tournure', 'view', 'visage', 'vista', 'wear the appearance of', 'wear the semblance of']	
GASEITY	['aeration', 'aerial', 'aerification', 'aeriform', 'aerodynamics', 'aerostatics', 'air', 'air bladder', 'airy', 'ammonia', 'ammoniacal gas', 'cloud', 'diffuse', 'effluvium', 'elastic fluid', 'emit vapor', 'essence', 'ether', 'ethereal', 'evanesce', 'evaporable', 'evaporate', 'flatulence', 'flatulency', 'flatulent', 'flatus', 'fume', 'gas', 'gaseity', 'gaseous', 'gasify', 'gasmeter', 'gasometer', 'partial vacuum', 'pneumatics', 'pneumatostatics', 'reek', 'sound', 'steam', 'swimming bladder', 'vacuum', 'vapor', 'vaporize', 'vaporous', 'vaporousness', 'volatile', 'volatile alkali', 'volatility']	0.1055835732
AIR	['aerial', 'aeriform', 'aerography', 'aerology', 'aerometer', 'aerometry', 'aeronaut', 'aeronautics', 'aeroscope', 'aeroscopy', 'aerosphere', 'aerostation', 'air', 'airy', 'al fresco', 'aneroid', 'atmosphere', 'atmospheric', 'atmospheric air', 'barometer', 'baroscope', 'blue sky', 'climate', 'climatology', 'cloud', 'common air', 'containing air', 'effervescent', 'eudiometer', 'eudioscope', 'exposure to the air', 'exposure to the weather', 'fan', 'flatulent', 'in the open air', 'isobar', 'meteorological', 'meteorology', 'open air', 'pneumatics', 'sky', 'ventilate', 'ventilation', 'weather', 'weather cock', 'weather gauge', 'weather glass', 'weatherwise', 'welkin', 'windy']	0.1048508442
SEXUALITY	['adultery', 'arousal', 'attractiveness', 'autoeroticism',	0.1046325482

	'become aroused', 'beefcake', 'bisexual', 'bisexuality', 'boner', 'buggery', 'carnal', 'carnal knowledge', 'cheesecake', 'climax', 'coitus', 'come', 'concupiscence', 'copulate', 'copulation', 'deviation', 'do it', 'ejaculate', 'ejaculation', 'erection', 'erotic', 'esquire', 'estrus', 'female', 'femininity', 'fetish', 'fetishism', 'fornicate', 'fornication', 'fuck', 'gay', 'gender', 'get hot', 'get it up', 'hardcore pornography', 'hard-on', 'have an erection', 'have intercourse', 'have sex', 'have the hots', 'heat', 'homosexual', 'homosexuality', 'horns', 'horny', 'hot', 'hot-blooded', 'hots', 'hunk', 'hustler', 'in the mood', 'incest', 'jack off', 'jerk off', 'lesbian', 'lesbianism', 'libidinous', 'libido', 'lovemaking', 'lust', 'lusty', 'make love', 'male', 'maleness', 'marital relations', 'masculinity', 'masochism', 'masturbate', 'masturbation', 'mate', 'mating', 'oestrus', 'onanism', 'one-night stand', 'orgasm', 'passionate', 'pederasty', 'perversion', 'pin-up', 'play the field', 'play with oneself', 'Playboy', 'porn', 'porno', 'pornography', 'randy', 'rut', 'rutting', 'Sadism', 'sado-masochism', 'self-abuse', 'self-gratification', 'sensual', 'sensuality', 'sex', 'sex drive', 'sex goddess', 'sex instinct', 'sex symbol', 'sexiness', 'sexual', 'sexual abnormality', 'sexual intercourse', 'sexual union', 'sexuality', 'sexy', 'sleep around', 'sleep together', 'sleeping together', 'sodomy', 'softcore pornography', 'stud', 'tumescence', 'up', 'voluptuousness']	
MORNING	['a.m.', 'at sunrise', 'aurora', 'break of day', 'cockcrow', 'cockcrowing', 'crepuscule', 'dawn', 'daybreak', 'dayspring', 'first point of Aries', 'foreday', 'forenoon', 'matin', 'matutinal', 'meridian', 'midday', 'midsummer', 'morn', 'morning', 'noon', 'noonday', 'nooning', 'noontide', 'noontime', 'peep of day', 'prime', 'prime of the morning', 'spring', 'summer', 'sunrise', 'sunup', 'the small hours', 'twilight', 'vernal', 'vernal equinox', 'when the morning dawns', 'with the lark', 'with the sun']	0.1036872099
BLINDNESS	['ablepsia', 'ablepsy', 'amaurosis', 'avert the eyes', 'be blind', 'be blind to', 'blind', 'blind as a bat', 'blind as a beetle', 'blind as a buzzard', 'blind as a mole', 'blind as an owl', 'blinded', 'blindfold', 'blindfolded', 'blindly', 'blindness', 'blink at', 'Braille', 'Braille-type', 'cataract', 'cecity', 'close the eyes', 'dark', 'darkly', 'dazzle', 'dimsighted', 'dim-sightedness', 'excecation', 'eyeless',	0.1031696651

	'grope in the dark', 'guttaserena', 'have the eyes bandaged', 'hoodwink', 'look another way', 'lose sight of', 'noctograph', 'not look', 'not see', 'prestriction', "put one's eyes out", 'render blind', 'sand-blind', 'screen from sight', 'shut the eyes-', 'shut the eyes to', 'sightless', 'stark-blind', 'stone-blind', 'teichopsia', 'turn away the eyes', 'undiscerning', 'visionless', 'wall-eyed', 'wink', 'wink at']	
HASTE	['a word and a blow', 'accelerate', 'acceleration', 'all at once', 'amain', 'apace', 'at short notice', 'barrel along', 'be in a hurry', 'be in haste', 'be precipitate', 'bestir oneself', 'boisterous', 'breathless', 'brusque', 'brusquerie', 'bundle on', 'bustle', 'by cable', 'by express', 'by fits and starts', 'by forced marches', 'by spurts', 'by telegraph', 'cursory', 'dart to and fro', 'dash', 'dash off', 'dash on', 'despatch', 'devil take the hindmost', 'dispatch', 'drive', 'expedite', 'express', 'feverish', 'fidget', 'flurry', 'flutter', 'forced march', 'full drive', 'full-tilt', 'furious', 'fuss', 'fussy', 'hard pressed', 'haste', 'haste makes waste', 'hasten', 'hastily', 'hasty', 'have no time', 'have not a moment to lose', 'head and shoulders', 'headlong', 'heels over head', 'helter-skelter', 'holus-bolus', 'hop skip and jump', 'hotheaded', 'hurried', 'hurry', 'hurry on', 'hurry-skurry', 'immediately', 'impetuosity', 'impetuous', 'in a hurry', 'in all haste', 'in haste', 'in hot haste', 'jump at', 'lose no time', 'lose not a moment', 'lose not an instant', 'make a dash', 'make haste', 'make short work of', 'no sooner said than done', 'no time to be lost', 'plunge', 'plunge headlong', 'posthaste', 'precipitancy', 'precipitate', 'precipitately', 'precipitation', 'precipitousness', 'press forward', 'press on', 'pressed for time', 'push on', 'pushing', 'put on', 'quicken', 'railroad', 'rush', 'scramble', 'scrambling', 'scuttle along', 'skurry', 'slap-bang', 'slapdash', 'speed', 'spirt', 'splutter', 'spurt', 'urge', 'urgency', 'urgent', 'velocity', 'whip', 'whip on', 'with all haste', 'with breathless speed', 'with haste', 'work against time']	0.1029272255
ENVY	['burst with envy', 'covet', 'covetous', 'envious', 'enviousness', 'envy', 'illwill', 'invidious', 'rivalry', 'spite']	0.1020089863

MALEDICTION	['a plague upon!', 'abuse', 'accurse', 'anathema', 'anathematize', 'aroynt!', 'aspersion', 'bad language', 'ban', 'beshrew', 'beshrew!', 'billingsgate', 'blast!', 'bold up to execration', 'commination', 'confound!', 'confusion seize!', 'curse', 'curse and swear', 'curse!', 'cursed', 'cursing', 'damn', 'damn it!', 'damn you to hell!', 'damn you!', 'damn!', 'denounce', 'denunciation', 'devil take!', 'devote to destruction', 'disparagement', 'evil speaking', 'excommunicate', 'excommunication', 'execrate', 'execration', 'fall a cursing', 'foul invective', 'foul language', 'fulminate', 'fulmination', 'go to blazes!', 'go to hell!', 'hang!', 'ill betide', 'imprecate', 'imprecation', 'invective', 'malediction', 'malison', 'maranatha', 'more bark than bite', 'oath', 'out upon!', 'out with!', 'profane swearing', 'proscribe', 'proscription', 'rap out an oath', 'ribaldry', 'rude reproach', 'sauce', 'scold', 'scurrility', 'strong language', 'swear', 'swear at', 'swear like a trooper', 'threat', 'threaten', 'thunder against', 'thunders of the Vatican', 'unparliamentary language', 'vilification', 'vituperation', 'woe betide', 'woe to!']	0.1014076768

Figure 3: Category Correlations with “WOMAN” in Control Group

Category	Correlation with Woman (p<.05)
('WOMAN', 'cat0374')	1
('FRIENDSHIP', 'cat0888')	0.8187368148
('FAVORITE', 'cat0899')	0.8178576227
('LOVE', 'cat0897')	0.8143562779
('BENEVOLENCE', 'cat0906')	0.8127995009
('TASTE', 'cat0850')	0.8090154668
('COURTESY', 'cat0894')	0.804339191
('WIT', 'cat0842')	0.7963906449
('DEMONSTRATION',	0.7744655093

'cat0478')	
('COLOR', 'cat0428')	0.7729662166
('SWEETNESS', 'cat0396')	0.7681858842
('ACCOMPANIMENT', 'cat0088')	0.7655875014
('MELODY CONCORD', 'cat0413')	0.7645980458
('REJOICING', 'cat0838')	0.758464961
('REFRIGERATION', 'cat0385')	0.7575741773
('RIDICULOUSNESS', 'cat0853')	0.7515830737
('OBSERVANCE', 'cat0772')	0.7485614912
('APPROBATION', 'cat0931')	0.747918816
('CAUTION', 'cat0864')	0.74605189
('GRATITUDE', 'cat0916')	0.7459885554
('PLEASURE', 'cat0827')	0.7418700094
('OSCILLATION', 'cat0314')	0.7375353036
('MEASUREMENT', 'cat0466')	0.7375224685
('DISINTERESTEDNESS', 'cat0942')	0.7371969715
('DEFENSE', 'cat0717')	0.737184811
('DISSUASION', 'cat0616')	0.7359037372

Bibliography

Baio, Andy (2014). 72 Hours of #Gamergate: Digging through 316,669 tweets from three days of Twitter’s two-month-old trainwreck, There’s little overlap between communities., The top RTed users are pro-GG, the top RTed tweets are against., Gamergate supporters use the

#gamergate hashtag more often. *Medium*. Online: https://medium.com/message/72-hours-of-gamergate-e00513f7cf5d#.b77envpa3; accessed 3 August 2016.

Burnap, Pete & Williams, Matthew L. (2015). Cyber Hate Speech on Twitter: An Application of Machine Classification and Statistical Modeling for Policy and Decision Making. *Policy & Internet* 7(2):223–42. Online: http://onlinelibrary.wiley.com.ezproxy.cul.columbia.edu/doi/10.1002/poi3.85/abstract; accessed 11 August 2016.

Grant, Christian; George, Clint P.; Jenneisch, Chris; & Wilson, Joseph N. (2011). Online Topic Modeling for Real-Time Twitter Search. In, *The Twentieth Text REtrieval Conference (TREC 2011) Proceedings*. Gaithersburg, Maryland: NIST.

Jarmasz, Mario & Szpakowicz, Stan (2012). Roget's Thesaurus and Semantic Similarity. *arXiv:1204.0245 [cs]*. Online: http://arxiv.org/abs/1204.0245; accessed 11 August 2016.

Kennedy, Alistair & Szpakowicz, Stan (2014). Evaluation of automatic updates of Roget's Thesaurus. *Journal of Language Modelling* 2(1):1. Online: http://jlm.ipipan.waw.pl/index.php/JLM/article/view/78; accessed 12 August 2016.

Klingenstein, Sara; Hitchcock, Tim; & DeDeo, Simon (2014). The civilizing process in London's Old Bailey. *Proceedings of the National Academy of Sciences* 111(26):9419–24. Online: http://www.pnas.org/content/111/26/9419; accessed 11 August 2016.

McHale, Michael (1998). A Comparison of WordNet and Roget's Taxonomy for Measuring Semantic Similarity. *arXiv:cmp-lg/9809003*. Online: http://arxiv.org/abs/cmp-lg/9809003; accessed 11 August 2016.

Ostrowski, D. A. (2015). Using latent dirichlet allocation for topic modelling in twitter. In, *2015 IEEE International Conference on Semantic Computing (ICSC)*, 493–97.

Parkin, Simon (2014). Zoe Quinn's Depression Quest. *The New Yorker Online*. Online: http://www.newyorker.com/tech/elements/zoe-quinns-depression-quest; accessed 11 August 2016.

Roget, Peter Mark (1991). *Roget's Thesaurus*. Online: https://www.gutenberg.org/ebooks/22; accessed 12 August 2016.

Sentiment140 (2009). Sentiment140 - A Twitter Sentiment Analysis Tool. *Sentiment140*. Online: http://help.sentiment140.com/home; accessed 6 August 2016.

Tweepy (2009). Tweepy. *Tweepy*. Online: http://www.tweepy.org/; accessed 12 August 2016.

Wofford, Taylor (2014). Is GamerGate About Media Ethics or Harassing Women? Harassment, the Data Shows. *Newsweek*. Online: http://www.newsweek.com/gamergate-about-media-ethics-or-harassing-women-harassment-data-show-279736; accessed 3 August 2016.

Why and How to Build Civic Tech Hubs in Emerging Markets
A Case Study of Phandeeyar: A Myanmar Innovation Lab

By Danielle Tomson
October 2016

Executive Summary: Myanmar is undergoing a connectivity revolution, going from 1% to over 80% of the population online since 2011. Phandeeyar is a civic tech hub in downtown Yangon taking advantage of growing enthusiasm for all things Internet by facilitating the growth and projects of the technology, social impact, and entrepreneurship communities. It and one of its primary investors, Omidyar Network, are part of a global movement of civic tech that has recently received more funding and positive metrics in recent years largely due to its holistic approach to economic, social and civic development. This case study narrates Phandeeyar's origins and successes, while also offering key reasons, concepts, and best practices to build a civic tech hub in an emerging economy.

Table of Contents

I. Overview and Summary

In 2011, only 1% of Myanmar's citizens had access to the Internet. After the country opened up that year, that number skyrocketed to over 80% today.[1] People are flocking to be part of the connectivity revolution and with that comes an interest in technology and innovation.

In a short amount of time, the international development community has had to adjust to the quick pace of social change fueled by telecommunications growth and foreign investment in Myanmar. Given that many country plans and grant timelines move slower than rates of Facebook adoption, trying to develop meaningful tech projects in the social and civil impact spaces is not easy for the development community.

Rather than developing stand-alone tech products or programs, one organization developed a model to cultivate a civic-minded technology ecosystem. That organization is Phandeeyar, a self-described "Innovation Lab" in downtown Yangon. It acts as a community center, accelerator, training center and event space for entrepreneurs, technologists, social impact professionals, and the media. Many of the values Phandeeyar holds are mirrored in the global movement of "civic tech," described as "the use of technology for the public good."[2] Civic tech is more than a product; it is a community, a movement, a culture. To this end, Phandeeyar as a civic tech hub[3] is helping to create a foundation for social, technological and economic growth by connecting those often non-connected communities in order to meaningfully collaborate.

While quantitative impact metrics are still emerging, the qualitative success of Phandeeyar is evident in talking to local leaders in telecom, entrepreneurship, civil society, investment, and media. As theory and empirical evidence suggests, civic tech hubs offer a platform for economic, civic, and cultural development to grow by connecting communities and giving them financial resources to begin building solutions to big problems. The growth of civic tech investment is a testament to the belief in civic tech's economic and social impact. Funding for civic tech projects up 119% and affiliation with "civic tech" went up 107% between 2013-2015.[4]

While Phandeeyar's success might sound like a unicorn to some international development practitioners, this paper is here to spread the good news: there is a model for building civic tech hubs with some clear principles for best practices. Those include:

- *Independence*: In funding, location, decision-making, and reputation
- *Accessibility*: In physical space and local language
- *Inclusivity*: In hiring, community-building and project facilitation
- *Platform Driven*: In organizational model and leadership

---

[1] "Land of temples and tech: The startup culture germinates in an unlikely place," *The Economist*, 18 March 2015. http://www.economist.com/news/business/21647318-startup-culture-germinates-unlikely-place-land-temples-and-tech

[2] From Matt Stempeck of Microsoft, Micah Sifry and Erin Simpson of Civic Hall Labs at "The Impacts of Civic Technology

[2] From Matt Stempeck of Microsoft, Micah Sifry and Erin Simpson of Civic Hall Labs at "The Impacts of Civic Technology
Conference on 27 April 2016. Also available here: https://blogs.microsoft.com/on-the-issues/2016/04/27/towards-taxonomy-civic-technology/#sm.001aipwe5te4ehz11p21znc67usop

[3] "Civic Tech Hub" is the term in this paper to describe a community, event, and training center that brings together the tech, civic, social impact and entrepreneurial communities. Instead of using "innovation lab" as Phandeeyar calls itself, the term civic tech hub also connects itself to a global trend. Other terms for this have been "innovation hub," "innovation lab," "iHub," or "social innovation center." It should not be confused with just a co-working space, accelerator, or incubator though it might include those things.

[4] Omidyar Network and Purpose, "Engines of Change: What Civic Tech Can Learn From Social Movements." June 2016. https://www.omidyar.com/sites/default/files/file_archive/Pdfs/Engines%2520of%2520Change%2520-%2520Final.pdf p. 12.

- *Distributive*: In finances, resources, and knowledge

In offering a case study of Phandeeyar, this paper is a narrative best practices guide designed for practitioners of international development who want to understand "why" and "how" to build such civic tech ecosystems. Much of the information presented here has been gathered through ethnography and live interviews with the Phandeeyar team, funders, and Myanmar technology community.[5] With the exception of Phandeeyar's founder, names are not reported to respect to interviewees' privacy.

To present the community-feel Phandeeyar offers the style of this study is a bit unorthodox, part academic-style and part narrative. The research is based on a larger forthcoming academic study tracing the emergence of the narrative of "innovation" and "civic tech" in international development. The project is generously funded by Columbia's School of International and Public Affairs Tech and Policy Initiative and the Carnegie Corporation of New York.

II. The Story of Phandeeyar: Origins and Structure

In order to demonstrate the best practices for building civic tech hubs, one must also first understand a little bit about Phandeeyar and its founding, its early programming, and organizational structure.

Origins

If there is any takeaway from the story of Phandeeyar's early days, it is the importance of being community-driven before being technology-driven. The result is an organization that puts people and their needs first—technology just facilitates.

Phandeeyar was founded in 2014 out of a series of Code for Change Myanmar hackthons. The organizer was David Madden, an Australian youth organizer, Internet entrepreneur, and founder of GetUp.org (an Australian equivalent of Change.org) and Purpose (a consultancy that helps organizations leverage Internet-based platforms for community building and campaigning). Madden describes arriving in Yangon in mid-2012 when the mobile and Internet penetration rate was "less than North Korea" and a "SIM card could sell for $250." The telecommunications sector had just opened up to foreign companies and the people of Myanmar were eager to connect with the world. As a serial community builder and global technology enthusiast, Madden had been inspired by the Nigerian Co-Creation Hub in Lagos, also a self-described "social innovation centre dedicated to accelerating the application of social capital and technology for economic prosperity."[6]

To see if such an "innovation hub" might catch on in Myanmar, Madden tested the concept by putting on the first Code for Change Myanmar hackathon. A hackthon is typically a 48-hour weekend event where computer programmers get together to "hack" technology-based solutions to a set of posed problems. Technology enthusiasts were easy to find; in January 2013, Myanmar had the largest ever BarCamp (a user-generated technology conference made popular by tech entrepreneur, Tim O'Reilly) with over 6,400 attendants.[7] The government-sponsored Myanmar Computer Federation (MCF) organized these events. Yet, aside from BarCamps and a

[5] Quoted and non-cited material comes from interviews done by the author.
[6] From Co-Creation Hub Website, http://cchubnigeria.com/
[7] Anh-Minh Do, "The World's Largest Barcamp is in Myanmar," *TechinAsia*, 29 Jan 2013, https://www.techinasia.com/worlds-largest-barcamp-myanmar

few trainings at a tech park far from downtown, there weren't many places for enthusiasts to go. To get the first hackathon off the ground, Madden enlisted the new Qatari telecomm provider, Ooredoo, to provide a space and wireless Internet—a service offering that the company had yet to launch to the public. Madden wanted to involve civil society in the event. His question was, "What was the willingness of non-technical groups to embrace technology?" He reached out to local civil society organizations and NGOs to source problems for the hackathon.

Madden recalled a key moment from the first hackathon "when everyone was red-bulled up." Population Services International (PSI) had posed two unique problems to the hackathon teams: how could tech be used to help women with birth spacing, and how could tech be used to reach sex workers with health needs? A young doctor from PSI refused to leave that night, going around to all of the teams hacking together solutions. That is when Madden knew he had his proof of concept for a space connecting techies and social do-gooders. "I'm completely familiar with all the writing on hackathons [referring to research questioning their utility] and I'm well versed in their limitations and all those things, but as a means of testing out a bunch of ideas and beginning to build a community around this stuff, [the hackathon] was very, very effective."

Madden continued to connect the tech and social impact communities and decided to have a second hackathon in September 2014, bringing in USAID and the World Bank. He also solicited space and Internet from Ooredoo, which had just launched its 3G service and was interested in an ecosystem that could build apps for this new service. The hackathon had a practical purpose of solving local business challenges, but the other larger objective was always visible to the public: the hackathon was "to help the growth and the development of the technology community."[8]

Around this time, Madden had secured philanthropic investment to build a civic tech hub from eBay founder Pierre Omidyar's philanthropy and venture capital organization, the Omidyar Network. Omidyar Network also partly funds other tech hubs like Co-Creation Hub in Lagos and Civic Hall in New York,[9] both of which had launched or were in the process of launching at nearly the same time. Indicative of the role information, news, and civic engagement would play in its future, Phandeeyar was fiscally sponsored by InterNews, an organization dedicated to empowering local media. With support in place, Phandeeyar leased a space on the top floor of a building overlooking Sule Pagoda in the heart of downtown Yangon.

Early Programming

With a space in place, Madden and his small, diverse team of entrepreneurs, social impact enthusiasts and recent graduates started their work. In the first year of 2015 alone, Phandeeyar held over 100 events, including 36 MeetUps, 21 seminars, 42 workshops and 10 major events (like hackathons). Work fell into three thematic areas: technology and the election, entrepreneurship and product development, and technology for social impact. LGBT groups, feminist organizations, religious pluralism groups, Maker enthusiasts and Linux fans found common ground at Phandeeyar. Facebook hosted events and Google sponsored a "Election Create-a-thon" to bring together creative to tackle civic education challenges for 48 hours. Civic engagement was in the DNA as much as tech and entrepreneurship were.

One of the most impactful events in Phandeeyar's first year was the MaePaySoh ("Let's Vote") Hack Challenge in September 2015 in which 137 developers in 30 teams participated.

---

[8]Catherine Trautwein, "Yangon's second 'hackathon' scheduled for September," *Myanmar Times*, 11 August 2014. http://www.mmtimes.com/index.php/business/technology/11337-yangon-s-second-hackathon-scheduled-for-september.html

[9] Full disclosure, the author of this paper was on the founding team of Civic Hall.

Myanmar would have its first national vote in November 2015 since the country had introduced nominal civilian government after almost 50 years of military rule. Phandeeyar partnered with the Asia Foundation and the International Foundation of Electoral Systems (IFES) to hold a two-week competition to see who could build the best election app using the candidate information API. The Asia Foundation had worked with the Myanmar Union Election Commission to create the API. The API offered dataset access to biographical information for 6,074 candidates and also parliamentary records obtained from the Open Myanmar Initiative for existing officials up for election. Additionally, the hack challenge urged hackers to answer three common questions: are you registered to vote and if not, where can you? Who can you vote for? How do you vote?[10] Though the information sounds basic, easy civilian access to it was *unprecedented*. The winning team received membership to the Accelerate Track of Facebook's FBStart Program and $80,000 worth of services for technology entrepreneurs.[11] Ultimately the winning app, MVote, had over 211,000 downloads, had been viewed in 87% of Myanmar's 330 townships, and had over 58,000 active viewers on election day alone.

Given the dearth of digital information, local and international journalists relied on the app for reliable data about candidates. It was the first "Civic App" in Myanmar. One journalist described this as the first digital Burmese news tool she ever used: "MP lists were never published on the Internet. I had to rely on a friend from Voice of America to supply me lists of the names of MPs. Normal people never knew the name of their MP in military times unless [the MP] went to their villages to give speeches."

The benefits of a civic API trickled outside of just the winning app. One former official from the Asia Foundation described seeing printouts of screenshots of the app with information about candidates running for office in a small village. As one local media insights and search startup in Yangon that participated described, "We couldn't miss the opportunity of participating and putting the election data on our app. We got 25,000 new downloads of our own [news] app during the election." This early social impact and election programming really set the stage for a civically informed technology community.

Organizational Structure

By Summer 2016, Phandeeyar had 27 employees. The company could be divided into four core competencies, at least judging by the most active group "channels" on Slack, the instant messaging app in the office that is popular in technology startups. There are many overlaps and cooperation between teams, particularly given that teams are not stacked in even informal hierarchies. In this sense, Phandeeyar remains pretty heterarchical, or horizontal, in organizational structure. The teams include:

1) Social Impact Team
2) Technology and Open Data Team
3) Operations and Finance Team
4) The Accelerator

Some of the longest employed associates at Phandeeyar currently work with the Social Impact team (or "#social-impact" on the Slack channel). Projects include training religious pluralist groups how to do effective Facebook campaigns, teaching journalists how to use online

[10] Catherine Trautwein, "Hackers in programming meet to prepare for the vote," *Myanmar Times*, 15 September 2015. http://www.mmtimes.com/index.php/business/technology/16485-hackers-in-programming-meet-to-prepare-for-the-vote.html

[11] Kim N.B. Ninh, Mi Ki Kyaw Myint, Susan Lee, "Myanmar Elections Hack Challenge: Let's Vote! *The Asia Foundation,* 23 September 2015. http://asiafoundation.org/2015/09/23/myanmar-elections-hack-challenge-lets-vote/

databases, doing social media advocacy trainings with LGBT groups, collaborating with disability rights groups, or hosting meet-ups with feminist groups to combat online harassment and trolling. These civic projects were some of the first and most enduring activities at Phandeeyar.

The Technology and Open Data ("#data" on Slack) group cultivates, networks, trains, and organizes the technology community. A good example of this was the August 2016 launch of a Myanmar open data platform, a sub-site of the regional Open Development Mekong data portal funded by USAID. Phandeeyar worked with 23 organizations to facilitate and code the web-based open data portal. The Technology team also works intimately with the Social Impact team to run trainings and meet-ups.

The Operations and Finance ("#ops" on Slack) team keeps the Phandeeyar office going—a challenging task in the rough environs. This involves everything from repairing the Wi-Fi, fixing ceiling leaks during rainy season, ensuring HR trainings are completed, doing accounting on QuickBooks, and freeing captives in the elevator stopped by power outages. Given that Phandeeyar is not located in a government or multi-national compound, the operations and finance team plays a uniquely special role in ensuring the functioning of the community center. While these roles might be at the bottom of a hierarchy in some development organizations, at Phandeeyar they are celebrated as crucial and equal positions.

Probably the most independent of these groups is the new Accelerator (#accelerator on Slack), which launched in August 2016 thanks to a $2 million grant from the Omidyar Network. They recently gave $25,000 each to six startups, which won placements into the accelerator.[12] The accelerator is the newest team and physically occupies a different space in the building, compared to the other three teams, which sit together.

As far as leadership goes, there are leads to each team, comprising both Burmese and foreign individuals who have competencies from prior work in each of those areas. For instance, the lead of the accelerator is a foreigner who had come from a development tech background. The lead of the tech team is a local who worked in product development abroad. The culture of leadership at Phandeeyar does not lend itself to hierarchical decision-making but instead relies on consensus. For example, the operations officer held an open vote for which floor tiles and tables should be purchased for the remodeling of the new accelerator space. Everyone got to vote including the strategy manager, the intern, the kitchen staffer, and the author of this report. Additionally, new programs in tech or social impact are rarely initiated without a lead from the outside community, further underscoring the value placed on grassroots, community driven projects.

Madden's influence on the vision, strategic direction and fundraising success is undeniable. That said, the organizational structure and culture at Phandeeyar is not so much led by individual personality, but by grassroots organizing and horizontal leadership. It is a platform for growth and grassroots inclusion, not a pyramid of hierarchy and planning. Yet, what is the impact of building such an organization?

III. Why Build a Civic Tech Hub? Reasons and Metrics

Why invest in a civic tech hub? For one, a civic tech hub brings together diverse communities in order to innovate and create sustainable solutions to challenges, both civic and

[12] Steve Gilmore, "Local start-ups get ready for six-month accelerator," *Myanmar* Times, 12 September 2016, http://www.mmtimes.com/index.php/business/technology/22447-local-start-ups-get-ready-for-six-month-accelerator.html

commercial. Secondly, it also creates an infrastructure of resources, skills, and network capital for the growth of tech, civic, and entrepreneurial sectors – all of which are particularly important for infrastructure-poor nations. Yet why do these reasons matter? What is their impact?

First, innovation increasingly matters as an organizing principle for new economic growth. The international development community has jumped on the bandwagon of "entrepreneurship" and "innovation" initiatives thanks to the global proliferation of Silicon Valley products and principles. Yet many organizations mistake "innovation" to mean a new technology product. Innovation is more than a new product—it is a culture of change, which can be painful to bureaucracies. As economist Joseph Schumpeter identifies it, innovation is the creative recombination of assets that may deeply disrupt cultural taken-for-granteds and organizational routines.[13] This "recombining" of resources becomes greater when there is a larger and diverse community to draw on. Because entrepreneurs are inherently starting something "new," they often face less (what Schumpeter calls) "taken-for-granteds" in the quest to produce newness. Yet entrepreneurship also requires a certain culture and resources. If innovation is about the "recombining" of resources, it cannot emerge in a vacuum. Innovation requires an encouraging, networked community of skilled technologists, business friendly policies, and access to flexible funding.

Omidyar Network understands the need to create a strong, diverse community that enables people to collaborate and create, probably because its founder, Pierre Omidyar, made his fortune off of a community platform, eBay. In conversations with representatives from Omidyar Network, they describe how the idea of a community driven platform influences their philanthropy and investments. By giving people a place to meet and exchange ideas, goods, or skills, they can lay the foundation for whole sectors to connect, share, and "recombine" for greater innovation. Omidyar Network calls this "priming the pump," where instead of using investment and philanthropy to fund individual projects piecemeal, they focus funding on whole sectors and communities. By doing this, they can grow supportive communities of kindred culture, support, and progress. [14]

This "priming the pump" concept is also informed by the idea of the "platform." The word "platform" can be painfully overused in the tech scene, but when built correctly and bringing in communities in the development process, platforms are tools, applications, frameworks, or foundations that "enable a whole ecosystem of participation."[15] Media entrepreneur and open source advocate Tim O'Reilly coined the term "Government as Platform" in 2010, trying to describe a new way of approaching government innovation in a more open and participatory manner.[16] He likens government to a vending machine: plug in tax money and get a service. There is very little engagement or participation. He contrasts this to the more open model of a bazaar where there is open collaboration and exchange of information, drawing on Eric Raymond's open source computing manifesto, *The Cathedral & the Bazaar*. To draw from these two foundational concepts in civic tech, a civic technology center is an embodiment of a platform (or a bazaar!) where different communities can build off of one another.

---

[13] From David Stark, *The Sense of Dissonance: Accounts of Worth in Economic Life*, Princeton: Princeton UP, 2009. p. 4.
[14] Matt Bannick and Paulsa Goldman, "Priming the Pump: The Case for a Sector Based Approach to Impact Investing," *Omidyar Network*, September 2012.
https://www.omidyar.com/sites/default/files/file_archive/insights/Priming%20the%20Pump_Omidyar%20Network_Sept_2012.pdf
[15] Tim O'Reilly, "Government as Platform" in *Open Government: Collaboration, Transparency, and Participation in Practice*, eds. Daniel Lathrop & Laurel Ruma. Cambridge: O'Reilly, 2010. p. 11-40. p. 13
[16] *ibid*. p. 13

Given that developing countries might not have a strongly connected civil society, corruption oversight, or good business policies to support growth, a civic technology center must do more than be a platform for growing the technology community. It must also "prime the pump" of the civil sector. The civic focus ensures that the ecosystem does not just have a financial bottom line, but a more holistic approach to growth. A strong local private sector in emerging markets requires small business-positive policies, media oversight, and educated citizen-consumers. One Myanmar health entrepreneur who works with Phandeeyar pointed out, "There are real problems here that Silicon Valley Tech bros who want to make laundry apps aren't persistent enough to solve." He sees civic tech as an anti-dote to what he called, "Short-termism," or the desire to just use tech to make quick apps that don't solve systemic problems. Civic tech embraces large-scale problems for meaningful growth both economically and culturally.

Omidyar Network sees investment in civic technology as a platform for growth, but also as part of a global movement. In a report they recently did with Purpose (the consultancy Madden founded), Omidyar Network outlines how well "civic tech" as a movement meets the criteria for 21st century movements: scale, grassroots activity, sustained engagement, shared vision, collective action, and shared identity.[17] It meets many of the criteria except for shared vision and identity: the vision is almost so inclusive it is too general to be defined. That does not stop the growth of investment in civic tech, up 117%, growing from $225M in venture capital in 2013 to $493M in 2015.[18] This growth is primarily in govtech (considered part of civic tech) but speaks volumes to the power of others to value the offerings of the movement.

Measuring this impact is difficult and the consensus is still out for long-term effects of building these civic tech centers. While studies might have been done on the effects of co-working centers, very little formal academic research has been done on civic tech hubs—probably because they are so new. In an effort to try to measure the impact of this movement, Omidyar looks at identity, reach, engagement, and influence of organizations in its portfolio. However, there is a known and strong consensus across the civic tech community that finding meaningful metrics is a big challenge.

What do some metrics look like? To measure engagement, Omidyar Network requests metrics on events from its grantees and investees (luckily there is an event RSVP company, Meetup.com, in its portfolio). From 2013 to 2015, civic tech events jumped from 629 to 1,737 in 2015 in the U.S. alone. Engagement might also be measured by GitHub commits. Influence and reach can be measured by the frequency of civic tech terms in social media and mainstream media. Though there is a temptation to measure "technology's reach" online with easily acquired social media states, more meaningful metrics about connection and community have to be measured offline.

As a final note, the civic tech movement in the United States has more research about it. There are different challenges and issues in the developing world's civic tech. A place like Myanmar has unique infrastructural, financial, human capital, and cultural challenges that Western organizations don't have to face. This does not mean these centers are isolated from the movement. To the contrary, they are quite plugged into trends in tools, conferences, news, and best practices in the global civic tech community. Phandeeyar invites initiatives like Founder Institute, Hack Days, Code for Change, Agile Meet-ups, Makerbot 3D printing classes, and Lean

[17] "Engines of Change," p. 9
[18] *ibid*. 13

Start-Up challenges. People feel plugged into a global movement as a result, which breeds enthusiasm and network capital.

These theoretical and empirical findings offer enough evidence for investors to put money and resources into civic tech hubs around the world. Given these trends in the movement, there are certain key best practices to building a successful civic tech hub.

IV. Practitioner Best Practices on How to Build a Civic Tech Hub

There are certain physical, financial, structural, technological and organizational elements to Phandeeyar that can be mirrored to create a civic tech hub. Of course, some elements are a matter of luck, like having a dynamic, connected founder or scoring a lease in the right location. That said, the following section offers some core principles and best practices that are ingredients to create a strong civic tech hub. Those five principles are:

- *Independence*: In funding, location, decision-making, and reputation
- *Accessibility*: In physical space and local language
- *Inclusivity*: In hiring, community-building and project facilitation
- *Platform Driven*: In organizational model and leadership
- *Distributive*: In finances, resources, and knowledge

These principles were identified through interviews and research. Additionally, though not in complete detail here, the best practices are informed by similar organizations like Civic Hall in New York or Co-Creation Lab in Lagos, but also other Myanmar initiatives in technology.[19]

Independence

Key Takeaways:

- *Flexible core-funding is absolutely necessary to independence.*
- *An independent organization is distinct from large bureaucracies in its mores, decision-making, planning, reputation, and tools.*

The single most important principle this paper offers is the principle of independence. Phandeeyar is not the "project" of another larger organization. It is an autonomous organization with flexible core funding. As such, it is not tied to legacy reporting, planning, cultural norms, mores, leadership hierarchies, technology, or accounting practices of an older bureaucratic organization. It is free to forge its own culture, leadership, budget decisions and reputation.

Most instrumental to its independence is the existence of flexible core funding from Omidyar Network. This core funding is not tied to a particular project with strict metrics or rigid budgeting tied to specific plans. Instead, the money supports projects and opportunities as they emerge—as they tend to in the tech sector. Representatives interviewed at Omidyar Network are aware that this kind of critical core-funding is often lacking in the global philanthropy scene; very often investors want a specific return, for a specific program, for a specific donor interest. This rigidity constrains creativity and limits opportunity (not to mention breeds the "vending machine" versus platform style organization discussed previously). Flexible funding offers the ability to chase needs, opportunities and markets. A Phandeeyar staff member who had spent

[19] This location was not visited by the author, but in interviews with Omidyar Network, the civic tech community, and Phandeeyar staff that knew of it, many referenced the similarities between the three places.

time in aid-rich post-conflict zones noted that, "Aid money isn't creeping into every corner of society [here] creating unhealthy dependencies to fulfill *specific* program mandates. People here take more of a market approach." The result is grassroots programming.

Compare this financing to that of a well-meaning and ambitious group at UNICEF in Yangon. A team interviewed there had recently launched UReport, a mobile tool that allows UNICEF to take polls and get feedback from SMS surveys of the youth population. The team did good work, but acknowledged they were constrained by limiting funding tied to a five-year plan—recall that five years ago Internet penetration in Myanmar was 1%. The opportunity to do mobile technology work emerged in the middle of UNICEF's Myanmar country program so trying to cobble together funding was challenging.

Phandeeyar's independence manifests itself in more than just funding. It also allows it to build its own reputation. As one Phandeeyar employee pointed out, "Many groups in Myanmar are resistant to international organizations. They got into complicated situations with locals during the military times and there was very little trust." Phandeeyar does not come with the reputation of a large multi-national organization—for better and for worse. This means they must build a unique reputation and trust with the organizations they work with. This can be a great thing, because many staff members and organizations within the Phandeeyar community see Phandeeyar as a product of Myanmar—not the international aid community.

Finally, independence manifests itself in what tools Phandeeyar uses—critical to a civic *tech* center! There are no "legacy" technology tools that Phandeeyar is forced to use that were custom built to fit the clunky requirements of a large organization. Instead, Phandeeyar can be more nimble in experimenting with out-of-the-box communication and project management tools. The offices uses many cloud-based tools like Trello (project management), Google Docs, Mailchimp, Facebook, Slack and Eventnook (a Myanmar start-up version of Eventbrite). They do this with the ease of a scrappy Silicon Valley startup trying to use the most convenient tools with the least amount of friction for the least amount of money, getting rid of those that don't work.

The independence to make these choices also affords them the freedom to be a more open and accessible organization. The difficulty of being independent does not go unacknowledged. The lack of core-funding from philanthropic organizations and eagerness of larger organizations to start but then involve themselves in projects like this makes independence difficult. Hopefully the trend Omidyar Network has started in core funding will make independence more feasible.

Accessibility

Key Takeaways:

- *A community center with fast, available Wi-Fi must be easily and physically accessible to community members.*
- *Activities and materials should be in the local language, on- and offline.*

The importance of an easily accessible home base with high speed Internet cannot be underestimated in building a civic tech hub. While centrality and wireless connectivity might seem like a given, it cannot be taken for granted in a country with intense infrastructural challenges. One Burmese-American entrepreneur described how small improvements in access can make a huge difference: "The power goes out. There are mosquitoes. The Internet goes out. People here don't have a lot of income, making electronic fund transfer—already hard—even more difficult." This is not Silicon Alley or Valley.

Access to high-speed Internet is one of the most impressive features to many guests who come to the space. One of the most memorable aspects in Phandeeyar's early days was during the first hackathon when participants marveled at Internet speeds they never witnessed before by tweeting the mbps speed and quickly downloading content. Phandeeyar continues to offer Wi-Fi to guests for free—though the password is changed frequently to avoid freeloaders on other floors. Contrast this to many international development offices that don't offer Wi-Fi to guests (one office visited by the author was launching a digital product yet had no Wi-Fi in the office for neither guests nor employees because of security concerns).

Many visitors and team members at Phandeeyar praise the centrality of its location in the heart of Yangon's downtown area, right next to key government offices. While the traffic in Yangon is dreadful in any direction, having a place where most busses go makes it easy for people to access. Compare this to the Myanmar ICT Park (MICT Park), which is much farther away from the center. This is also where the Myanmar Computer Federation (MCF) is housed. One MCF official and media mogul shared a story: "One of my graphic designers went to Phandeeyar one day and she gave a talk about Adobe Photoshop design. 200 kids show up. I'm a [leader] of one of the largest professional associations in Myanmar and we host events every month and never get that kind of turnout." MCF tried to create something like a Phandeeyar called Kanaung Hub in MICT Park. Kanaung Hub hosts some meet-ups mostly in technical skill development (the website offers "Laravel Meetup Yangon" and "Internet of things with Raspberry Pi, Arduino, and Esp8266"). However, the space mostly functions as a co-working facility where one can rent a dedicated desk for about $40/month (Phandeeyar offers open seating for $30/month). This is reasonable given the inflated real estate prices caused by foreigners, but not cheap to many locals.

As a final note on accessibility, live and digital access in the local language is absolutely necessary. While Phandeeyar's primary website is in English, its Facebook page is sometimes exclusively in Burmese if it is not bilingual. Most people in Myanmar do not access webpages, but instead use Facebook as the primary source of information exchange. Many committed techies in the office also make sure that all of the information online is in machine readable Burmese Unicode font online that adheres to international Unicode standards, instead of Zawgyi, which is an older Burmese computer font that makes storing and rendering text more difficult. It goes without saying that many events are exclusively in Burmese and do not offer any English translation. When there are English speakers, translators into Burmese are readily available. The online and offline accessibility makes it easier to build an inclusive community.

<u>Inclusivity</u>
Key Takeaway:

- *Actively seek minority, youth, and female voices to hire and give them significant roles within the organization.*

Phandeeyar actively seeks women, religious minorities, ethnic minorities and youth to participate in the organization's activities, programming, and hiring. In a country with deep ethnic and social division, the inclusion of religious or ethnic minorities can be challenging and face a lot of critique. One night during the course of interviews, Phandeeyar hosted an openly transwoman and a panel of feminist leaders to speak. Given online harassment and violence against women and LGBT activist, an event like this is a bold statement, if not a risk. Currently, Phandeeyar is also offering financial and technology training assistance to an LGBT group called

Rainbow Organization. There are special events for women including a special Geek Girls meet-up. This kind of open and public inclusion around more Western-style identity politics is incredibly new in Myanmar, but also a source of pride for many young people involved.

Many team members were hired after working on a project with Phandeeyar in hacking, election monitoring, religious pluralism or media freedom. Many of those hired are women under 25 years old. They are not in "intern" level positions either; they take on leadership roles in coordinating projects and organizing various communities to which they belong. This includes the media, religious pluralism advocates, feminist groups, ethnic minorities who have returned from exile abroad, college computer science classes, or hacker collectives. These younger people do not come with as many rigid ideas about technology and open communication as compared to their parents' generation, which grew into adulthood during a military coup that censored most all controversial information.

Given the newness of tech, describing Phandeeyar to older generation civil society organizations can sometimes be challenging for the younger staff members. One Phandeeyar social impact team member described her pitch: "I just say I'm promoting peace at a technology hub." She then goes on to describe how they can help groups use Facebook or Slack to better coordinate their communities. The utility of tech helps sell Phandeeyar.

Inclusivity means making a special effort at building trust with parts of society that might even be suspicious of Phandeeyar's work. Sometimes this means making a case for why technology is useful to that group. One open data team member described how she convinced her MP back in the village she is from why she should use and promote open data: "I had to convince an MP that we are launching the open data dashboard for good [reasons] and it is useful for her. They should know what their constituency is." By selling utility, Phandeeyar gains trust and builds a network.

Platform Driven

Key Takeaways:

- *Horizontal structure and leadership is critical to building the foundation for a networked and solution-driven community.*
- *Innovation is a culture, not a department.*
- *The hub is the platform and facilitator of community driven projects.*

The idea of the platform, as described in the "why" section of this study, makes the case for the value of a flat organization that invites others and facilitates the development of their ideas. A platform driven organization facilitates a whole ecosystem of participation, inclusion, innovation, and growth. Yet the concept of "platform" is not necessarily intuitive, especially in emerging markets.

One of the most striking elements at Phandeeyar is the horizontal leadership and culture of openness. In the work culture of many Myanmar businesses, there is a strong hierarchy with very little incentive to speak to superiors for fear of making a mistake. The team at Phandeeyar rejects this culture and tries to teach new staff members how their office culture is different. One junior team member said, "In Myanmar, if you don't know, you can't ask. Here [at Phandeeyar], if I don't know, I don't know and I can ask." This openness and fluidity between team members, no matter how long they've been there, allows problems to be surfaced and solved faster.

Earlier, this paper mentioned Joseph Schumpeter's and also sociologist David Stark's notion of innovation as a "creative recombination of assets."[20] The combination of a diverse community and the flatness in the organization itself invites the rapid recombination of assets. Many people in the organization offer multiple skill sets, communities, and histories. As an "Innovation Lab" in Myanmar, Phandeeyar does not segregate "innovation," to a department or to a certain individual dubbed as the innovation lead as they might be at UNICEF or Impact Hub Yangon.[21] Innovation is a culture endemic to every activity, tool and behavior of Phandeeyar's diverse organization. Seeing as how they cannot solve systemic societal problems amongst just their staff, Phandeeyar looks outside of their organization to help facilitate and connect groups already tackling these problems.

As one of the leads in the social impact team describes, Phandeeyar "facilitates" existing organizations instead of building products or programming solo. He mentioned there are three criteria in looking for partners: "Who has capacity, who has a small budget, who really needs technology to make impact with their work." Instead of trying to build new competencies from scratch, Phandeeyar partners with other organizations, enhancing their work with technology resources and connections. One Phandeeyar staff member sees the work they do as truly being grassroots: "We are not implementing programs so much as we are supporting." While Phandeeyar plans events with visiting technology experts or supports the Open Data portal, all of these initiatives have one or more external partners.

In valuing the principle of "platform" Phandeeyar facilitates the work and networks of others and thus creates a buzzing ecosystem that is much more effective than if they built new competencies from scratch. As one Phandeeyar team member describes, "We might not achieve our slated goals [with an event or program] but we do build network capital."

Distributive

Key Takeaways:

- *More can be accomplished when the platform distributes money and resources to self-initiated groups, instead of trying to scale up those capacities inorganically.*
- *Expectations on "returns" are not tied to strict metrics so experimentation is encouraged.*

In a country still struggling with poverty, conflict, literacy, digital literacy, and reliable mobile signals, material needs cannot be taken for granted. This is why a distributive attitude towards sharing resources within the community is critical. This is not to say a civic tech hub should be freely giving away computers at every turn. On the contrary, the distributive nature should be thought of as *investing* in key projects in disadvantaged groups.

Phandeeyar recently started offering microgrants to various organizations in its Social Impact network in order to do work in more remote areas of the country. Money went to Rainbow Organization, an LGBT group that organizes ten grassroots groups to use social media advocacy tools in tech conferences. Another grantee was Myanmar Fifth Estate, a civic tech startup that launched Open Hluttaw, a mobile web platform that promotes political accountability among citizens by offering an open database of information about the country's 440 parliamentarians. Myanmar Fifth Estate also uses digital marketing strategies to drive engagement between citizens and elected officials on Facebook. Finally, one of the recent

[20] From Stark, p. 4.

[21] Both UNICEF and Impact Hub in Myanmar each have a special "Innovation Lead."

grantees includes iSchool Myanmar, which is a campaign promoting inclusive technology to improve the civic participation of persons with disabilities in Myanmar.

Then there is the Accelerator. After a three-month recruiting period, six startups were recently brought on and given $25,000 in seed funding plus access to over $200,000 of donated services like servers, accounting, and legal help. Startups include an AirBnb-style app for Myanmar apartments, a cargo truck sharing app, and a tech-based microloan company. The lack of startup capital in Myanmar made the launch of Phandeeyar's accelerator all the more exciting—especially after one local telecom's accelerator failed to launch. The lack of startup capital is even worse for civic-minded businesses. As one entrepreneur of a search and insights app said, "Being a good guy in business is a problem. Our investors look at our app or civic engagement projects and say 'We don't want to fund a research lab.' People need to see the value of civic tech, especially in Asia." When there is social impact investment money available, the terms aren't great. Says one entrepreneur: "Social impact investors expect the same types of returns as other businesses, but with *additional* social impact returns. It is impossible to get those returns here." Phandeeyar does not escape similar critiques: it takes a 12% equity stake for a $25,000 investment[22] – a significant amount by Silicon Valley accelerator standards for such a relatively small amount of money. Regardless, the access to capital has energized the startup scene.

For a point of comparison it is worth noting a company doing similar work: Telenor, the Norwegian telecommunications provider that has over 17 million active users of its services. A "business sustainability" representative (not an "innovation officer") at Telenor described their Lighthouse Digital Literacy training centers that they were setting up all over Myanmar. These physical centers offer mobile and computer trainings to locals in an effort to build capacity (and customers). They are also currently trying to develop an app to give these trainings remotely. The representative noted that the program is not obliged to link their success to sales metrics—which might put undue pressure on each Lighthouse. In addition to meaningfully training more users of their products, the program builds the perception of Telenor as an innovative and collaborative player in the Myanmar technology ecosystem.

One Phandeeyar staff member who had seen a lot of the poverty and conflict of Myanmar first hand feels strongly about making sure that Phandeeyar disperses its knowledge of digital literacy and technology to remote or poor places: "I don't want to see young people compete for a device or resort to prostitution to get [a smartphone], but then not know what to do with it." As with the Telenor Lighthouses, Phandeeyar considers the distribution of skills, knowledge, and tools as fundamental to developing a fair and valuable tech market just as much as selling a phone.

V. Conclusion: Thoughts on Improvement and the Future

The Phandeeyar journey has been one of great community building, skill development, networked diversity, and facilitation. But it has also been one of navigating disparate communities, difficult terrains, and cultural challenges. In its first iteration, Phandeeyar has managed to bring together groups of people, train them, expose them to opportunities to work together, and offered resources to do so.

---

[22] Juliet Shwe Gaung, "Myanmar: Phandeeyar sets up accelerator, to invest $200k in 8 startups in 2016," *Deal Street Asia*, 12 June 2016 http://www.dealstreetasia.com/stories/phandeeyar-to-seed-fund-up-to-200000-through-their-first-tech-startup-accelerator-43871/

Yet what challenges will Phandeeyar face looking ahead? Staff and community members chimed in with a few critiques and challenges. One start-up executive said Phandeeyar's generalist attitude could be a challenge, "They put their hands into everything because no one else does, but that is tricky. Because I don't know who they are about and what they are about. The people in Phandeeyar are generalists. Specialists bring a certain credibility." This generalist culture might also affect how much Phandeeyar can actually impact certain areas, like government tech for instance. As one tech executive with government ties described, "We need someone who understands both tech and government bureaucracy. So many explain e-Government without understanding what it means here." Phandeeyar will probably not satisfy that niche given it focuses on community more than pure technology solutions. Organizations with government ties like MCF better serve technicality heavy trades like enterprise technology. Regardless, as Phandeeyar grows its staff and community, more work will have to be done beyond just connecting and facilitating projects. Phandeeyar might have to support or hire more specialists to address complicated problems. One entrepreneur thought this would be useful in framing meaningful problems, challenges, or questions, and then actively nudging community members to solve them.

Several people noted Phandeeyar is so strong because of its exceptional people. (One start-up executive compared one Phandeeyar staff member to "that elf lady in the Hobbit who can do everything.") A few questioned if Phandeeyar could survive without the leadership of David Madden. Given Madden's track record of leaving behind sustainable businesses after stepping down as a CEO, this did not seem to be a worry at Phandeeyar.

These two points were the most frequent critiques, but for the most part there was a lot of enthusiasm and optimism about Phandeeyar. Most just wanted Phandeeyar to become more well-known and present in the mainstream. The uniqueness and specialness of Phandeeyar is palpable as soon as you walk-in; most Phandeeyar enthusiasts just want to share that with people who never knew such open and vocal organizing because of their experience under a military regime.

Right now, the youth of Myanmar are excited, engaged, and enthusiastic about the future of the country and the new connectivity revolution. Yet, will this newness lose its luster as time goes on and disappointments or scandals emerge—as they tend to in any political system? Will loss of optimism affect Phandeeyar's growth? Many of these questions are speculation and hard to address. Yet, if Phandeeyar can remain true to its role as an independent, accessible and diverse platform for change, collaboration training, and resource acquisition, it is in a good place to prime the pump for the next chapter of development in the tech and civic sectors.

Global Digital Futures Policy Forum 2016: Issues Brief

Panel 5: Civic entrepreneurs: Global perspectives on open data, engagement and urban governance

By Hollie Russon Gilman

It is common nowadays to bemoan the state of our democracy: from growing citizen disaffection, to the growing influence of money in politics. The 2015 Edelman Trust Barometer shows a global decline of trust in government with numbers reaching historic lows.[1] In surveys, government dysfunction continues to surpass the economy as the problem Americans' are most likely to list as the country's most serious. A recent Pew survey found that trust in government remains at historic lows. [2] Only 19% of Americans say they can trust the government always or most of the time. The majority of Americans (60%) think their government needs "major reform," in contrast to the late 1990s when less than 40 percent of those surveyed thought so. Only 20% would describe government programs as being well run and 55% of the public says that "ordinary Americans" would do a better job of solving national problems then elected officials.[3]

However, partly in response to citizens' growing disaffection, a wave of participatory policy reform has emerged in America's largest cities, capitalizing on new technology, open data and democratic experiments that aim to improve democracy.[4] Around the globe technologists, government innovators, and civil society are leveraging digital tools and open data to make governance more responsive to citizens, strengthen the relationship between citizens and their government, provide new ways for citizens to participate in decision-making in their communities, and make governments more accountable.

Civic Tech

There are many conversations concerning "civic technology," or "civic tech" and the opportunities for leveraging digital tools to benefit the public. The $6 billion civic technology is just a piece of the $25.5 billion that government spends on external information technology (IT). Government investments in civic technology can spur powerful partnerships that foster public sector innovation.[5]

---

[1] Edelman Trust Barometer 2015

[2] Pew Research Center, November, 2015, "Beyond Distrust: How Americans View Their Government.

[3] Ibid.

[4] See also Beth Simone Noveck (2015). *Smart citizens, smarter state: The technologies of expertise and the future of governing.* Cambridge, MA: Harvard University Press

[5] See also Hollie Russon Gilman, "The Future of Civic Technology" April 20, 15 *Brookings Institute* http://www.brookings.edu/blogs/techtank/posts/2015/04/20-civic-technology

There is debate about its precise definition including who is even involved in civic tech. For instance, does it include governments seeking to modernize their systems or people sharing resources better? Is it about efficacy or effectiveness? Should the emphasis be on people or politics? Perhaps a definition can be expansive enough to include a variety of actors and activities.

Further, we need more examples of data and technology being used to hold government to account, better govern urban areas or increase civic engagement. This can help spur research of the subsequent outcomes – both positive and negative - in areas such as governance, healthcare and sustainable or local development? Evidence is required to generate robust and meaningful evaluations of the outcomes and success various open data initiatives. This paper outlines four examples of data and innovation to strengthen urban governance and concludes with three key takeaways for researchers, policymakers, and practitioners.

Chicago OpenGrid

Chicago has created OpenGrid to provide an open source, situational awareness system to enable an easily accessible and centralized open source repository of public information.[6] OpenGrid reflects one of the most advanced deployments to use government data to empower citizens.[7] It reflects the latest installation in Chicago to build open source data efficiency that is scalable.[8] Their WindyCity platform integrated seven million pieces of data from city departments every day and paired it with a powerful analytics tool to create data visualization to equip managers with new insights on city operations in real time.[9] It won $1 million dollars from Bloomberg Philanthropies Mayor's Challenge.[10] OpenGrid reflects the latest version of open data being released to spur civic education, agency, and industry. In contrast to processes that simply release data without an engagement strategy, OpenGrid is designed for participation, collaboration, and replicability.

Participatory Budgeting

Participatory budgeting (PB) started in 1989 in Porto Alegre, Brazil, by the leftist Partido dos Trabalhadores (Workers' Party). PB gives citizens the opportunity to learn about government practices and to come together to deliberate, discuss, and substantively

---

[6] See also "Chicago Tech Plan," City of Chicago http://techplan.cityofchicago.org/

[7] See Sean Thornton "Chicago Launches OpenGrid to Democratize Open Data" *Harvard Data-Smart City* Solutions, January 20, 2016 http://datasmart.ash.harvard.edu/news/article/chicago-launches-opengrid-to-democratize-open-data-778?utm_content=buffere195b&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

[8] Jason Sheuh "3 Reason's Chicago's Analytics Could be Coming to Your city" *Government Technology,* April 1, 2014 http://www.govtech.com/data/3-Reasons-Chicagos-Analytics-Could-be-Coming-to-Your-City.html

[9] "Chicago Uses MongoDB To Create A Smart and Safer City" https://www.mongodb.com/customers/city-of-chicago.

[10] Amina Elahi "Bloomberg Awards Chicago $1 M for Real-Time Analytics Platform" *Built in Chicago* March 13th, 2013. http://www.builtinchicago.org/blog/bloomberg-awards-chicago-1m-real-time-analytics-platform.

affect budget allocations (Shah 2007). In its original campaign for participatory budgeting, the PT outlined four basic principles guiding PB: (1) direct citizen participation in government decisionmaking processes and oversight; (2) administrative and fiscal transparency as a deterrent for corruption; (3) improvements in urban infrastructure and services, especially aiding the indigent; and (4) a renewed political culture in which citizens would serve as democratic agents. Recent research convincingly demonstrates that in the last twenty years PB has enhanced the quality of democracy in Brazil and other positive outcomes linked to specific uses of PB in Brazil include increased municipal spending on sanitation and health, increased numbers of CSOs, and decreased rates of infant mortality.[11] Digital tools, including SMS, have been used for various aspect of the process including ideation, dissemination of ideas, and voting. In 2016, New York City conducted the first digital voting, with in person registration, providing an access code for people to use to vote online.

Boston New Urban Mechanics

In 2010, Boston launched the first Mayor's Office of New Urban Mechanics (MONUM) at the beginning of Mayor Menino's fifth term.[12] The office was designed to pilot experiments, and work directly with entrepreneurs, to leverage technology and innovation to improve the quality of City services and strengthen the relationship between citizens and the City for "peer-produced governance.[13]" Menino was long interested in the process of tinkering with tools, which gave him the nickname "The Urban Mechanic." Since 2010, the office quickly gained momentum, with the two co-heads receiving an award as the Public Officers of the Year by *Governing Magazine*.[14] MONUM has been recognized as a global example, including by the UK Innovation Unit NESTA and recently received $1.3 million as part of Bloomberg Philanthropies Innovation Team program to develop solutions to the middle-income housing challenge. The MONUM model has spread to Philadelphia and Salt Lake City and continues to serve as an international paradigm for cities to emulate. The success of MONUM illustrates the opportunity for digital technology to alter institutional culture to make it more amenable to experimentation and focused on residents.[15]

Rhode Island Civic Crowd Funding

Central Falls, Rhode Island is a densely populated community in a small geographic area, with Rhode's Island only majority Hispanic community. In 2011, Central Falls declared chapter 9 bankruptcy – the first time a city in Rhode Island has declared bankruptcy. In this socio-political climate, the city government decided to try

---

[11] Michael Touchton and Brian Wampler, B. (2014). "Improving Social Well-Being through New Democratic Institutions." *Comparative Political Studies* 47, no. 10, pp. 1442–69.
[12] See http://newurbanmechanics.org/boston/
[13] See Ben Schreckinger "Boston: There's an Apps for That" *Politico Magazine* June 10, 2014.
[14] See Steve Goldsmith "An Old-School Mayor on the Forefront of Innovation" *Governing September 6, 2012.*
[15] See Susan Crawford and Walter (2013), "Citizen-Centered Governance: The Mayor's Office of New Urban Mechanics and the Evolution of CRM in Boston" *Harvard Berkman Center Case Study.*

something new to engage the community around a shared project.[16] They partnered with Citizinvestor,[17] a crowdfunding and civic engagement that works similarly to Kickstarter for governments, to launch a civic crowdfunding campaign – one of the first in the United States. Municipalities post a project with a funding goal. Citizens donate online. If the goal is met, the municipality receives the funds minus fees. It's an all or nothing model -- in order for the entity to receive the funds, the fundraising goal must be met. Central Falls launched a Citizinvestor campaign that hit their goal of $10,044. Local residents were active participants in every part of the process; identifying the topic for fundraising, pledging their own dollars, and collaboratively designing artistic trash cans working directly with a local arts nonprofit The Steel Yard.

3 Policy Lessons: Civic Tech for More Inclusive Governance

(1) Leveraging Multi-Sector Partners

Each of the examples took advantage of talent and expertise and have partnered with external experts, such as the Citizinvestor platform itself and leveraging resources from external entities such as the Amazon Web Services in Chicago. OpenGrid has partnered with the Smart Chicago Collaborative, which is funded by the MacArthur Foundation and the Chicago Community Trust. The civic tech examples here also take advantage of University expertise. This can take the form of fellowships (e.g. MONUM), computing power (e.g. OpenGrid) or research support (PBNYC).

Policy makers can think more expansively about the resources at their disposable and structure civic tech experiments with deliberate intent to engage multi-sector stakeholders. The methods employed enable public private partnerships and create entry points for the public sector to leverage external resources.

(2) Embedding pilot programs to become institutionalized

Many of these examples moved from pilot processes to become more embedded and institutionalized structures. The Boston New Urban Mechanics were able to prototype several types of programs in a lean and agile way. Through gaining momentum and winning support from citizens, they now are being asked to solve critical problems for the city in a systematic way. PB in the United States began as a pilot with $1 Million in 2009 and now upwards of $50 Million is being allocated through the process. By starting out as small and nimble programs, many of these projects were able to take risks they otherwise would not have been able to. Importantly, this enables less pressure from the onset and the ability to think more creativity about implementation.

Policy makers can learn valuable lessons from pilot projects. The stakes are lower and they can try outreach to traditionally marginalized communities. Experiments offer an opportunity to reach citizenry in non-traditional way and expand the traditional public service delivery model of citizen as only a customer. Pilots that are well structured can empower people for more inclusive decisionmaking.

---

[16] See more at http://www.citizinvestor.com/project/clean-up-cf-new-bins-in-jenks-park.
[17] See http://www.citizinvestor.com/ for more information.

(3) Learned Lessons Across Contexts

Because civic tech is not bound to one geographic region, many of these examples take a more network approach. This enables an opportunity to take lessons learned from various contexts and apply these principles. Participatory budgeting first began in the Global South and is quickly spreading across the North. Philadelphia was the first city to experiment with a Citizinvestor public funding campaign and though they did not reach their goal, valuable insights from their process directly improved the process in subsequent cities. The Chicago DoIT ensures that all the code for the city is open source and available on GitHub. Other cities, in turn, can use this code for their own public interfaces to spawn more open and democratic open data.

Policy makers can take lessons from many types of actors across diverse contexts. Best practices from global experiments can be translated to fit specific contexts and ensure local, community needs are front and center. These experiments do not need to be viewed in isolation from one another, but rather can serve as a useful petri dish to shed light on further implementations. The result can be a more expansive approach to innovation, which is inclusive of diverse cultures and backgrounds. The critical factor is applying these lessons to a context specific locality that is sensitive to the local socio-political context and environment.

Practitioner Points

- Public sector officials can leverage multi-sector partnerships to capitalize and harness the expertise of academia, civil society, industry and philanthropy to spur civic tech and data for governance.
- Creating centralized repositories of interested funders, open source digital tools, collaborations, and best practices for civic engagement can streamline multi-stakeholder partnerships in order to circumvent some of the current institutional barriers facing government officials eager to implement change.
- In order to incorporate civic tech for more inclusive governance, practitioners can start small by piloting civic tech experiments and then move to embed and institutionalize new practices into governance.
- Public officials in the United States can learn best practices from a variety of global examples. Lessons learned can be shared internationally.