CMS.360 Project Proposal: The Combine

Author:
Jeremy Rubin
jr@mit.edu

Advisors:
Erhardt Graffe
erhardt@media.mit.edu
Ethan Zuckerman
ethanz@media.mit.edu

May 13, 2015

Contents

1 Introduction

There's a problem brewing in America: the American way of life is facing an attack which could shred the fundamental liberties and rights enjoyed by its citizens to pieces. This attack is multifaceted, and comes not in the form of boots on the ground, but a misalignment on the fundamental tenets of what is required for free and open society.

Civic participation is down. Mistrust in the institutions which *define* our society is up, and for good reason; the government is failing to serve and protect it's people. In the last decade or so, America has seen itself embroiled in seemingly pointless wars, responding poorly to national disasters like Hurricane Katrina, and mass surveillance programs have been revealed that put theories the "tinfoil hat" theories to shame.

Can civic participation and trust be restored? While this is debated, at least one small fact seems true: civic restoration cannot begin without first responding to the attack.

How does one respond to an attack?

With weapons.

2 The Missing Militia

2.1 Brief History of The Militia

Merriam Webster defines a militia as, "a group of people who are not part of the armed forces of a country but are trained like soldiers"[8]. Such militias served a central role in the fight for independence and foundation of the United States of America. In the founding documents of America, independently organized state militias were supposed to form the bulk of the United States military force; in fact a standing U.S. army was expressly forbidden – military appropriations for periods of more than two years were not allowed[9].

However, for the past century the role of the militia has faded away and a strong federally regulated militia has taken its place. Institutions such as the National Guard serve the role of a more locally organized military, but they are still heavily federally regulated[10][11]. The unorganized militia has somewhat fallen to distemper, as they are largely viewed as terroristic institutions after a resurgence in the 1980's (especially by the government). The groups are typically anti-government, and plan violent attacks which have negatively tainted the word militia, and perhaps rightly so there are several instances of militias attempting or carrying out deadly attacks[12][13][14].

However, just because a term has a negative connotation does not mean the true meaning of the term should be taken negatively. At its core, a militia is just a group that derives its right to act in protecting public safety [15]. In fact, the U.S. government defines, "the militia of the United States consists of all able-bodied males at least 17 years of age"[16]. This set of citizens could perform basic training together so that they would be prepared in the event they would be called upon for duty.

2.2 Lackluster Recent Use

Indeed, there are recent initiatives which have labeled themselves as militias that promote non violent methods, but taking to their core protecting certain rights such as the right to use a vaporizer or defend occupy protesters [17][18]. However, some such movements have received heavy criticism – the one to defend Occupy protestors, started by a Googler, received criticism for only trying to create "cannon fodder"[1][19].

2.3 Bringing it Back

The to-the-roots decentralized notion of militia seems to be missing, where all individuals perform basic training and then mobilize their skills on issues (or battles) which are personally relevant. What can be done to restore this preparedness? What types of threats should all citizens be prepared to respond to?

3 Militia Based Citizenship

Civic structures hinge upon some definition of a citizen. It is impossible to design and build a Civic Media system without making some set of assumptions or expectations about what the role of the citizen will be. These definitions and expectations can be a moving target. This section is organized as follows; first, the existing models of citizenship will be covered in 3.1, then a new model of citizenship will be proposed in 3.3

3.1 Existent Models of Citizenship

This subsection is a literature review of 5 concepts of citizenship.

3.1.1 Changing Concepts of Democracy[1]

In this piece, Schudson frames the evolution of the ideal citizen throughout history, and ends with his ideal citizen (Monitorial). Each citizen type is summarized below.

Solid Citizen In the solid citizenship model, an elite set of the citizenry were considered fit for leadership roles, and part of the governments role was to ensure that this elites were properly educated for leadership. The rest of the citizenry were tasked with recognizing the elites which are well intentioned and those with selfish ambitions; however this was more to the degree of local social reputations rather than policy preferences.

Party Citizen In the party citizenship model, citizens join a political party (such as the Democrats or Republicans) and their votes are cast along party lines. Parties perform an organizing function but also discourage deviation from the party's platform.

[1] another term for human shields

Informed Citizen The informed citizenship model sprang up from the Progressive Era, in response to the mass spread of party politics. The Informed Citizen is made separate from the parties and is knowledgeable about the issues. The Secret Ballot is used; which means that parties cannot directly dictate votes. This system, “asked voters to make a choice among alternatives rather than to perform an act of affiliation with a group”.

Rights-Conscious Citizen The rights-conscious citizenship model, citizens and politicians became focused on individual liberties and freedoms. The courts became the center for this rights battle, and prominent cases moved the needle for reforms and new law.

Monitorial Citizen Schudson’s novel model of citizenship is defined as follows:

> ...the obligation of citizens to know enough to participate intelligently in governmental affairs should be understood as a “monitorial” obligation. Citizens can be “monitorial” rather than informed. A monitorial citizen scans (rather than reads) the informational environment in a way so that he or she may be alerted on a very wide variety of issues for a very wide variety of ends and may be mobilized around those issues in a large variety of ways

In this model, a citizen focuses on the topics where they have expertise; not the entire spectrum of issues. It is perhaps more effective because the civic duty can be spread around and higher quality on specific issues.

3.1.2 What Kind of Citizen? The Politics of Educating for Democracy[2]

In this piece, Westheimer and Kahne discuss three types of citizen and discuss their efforts in teaching these principles to students.

Personally Responsible Citizen The personally responsible citizen is a citizen who works within ’the system’. Westheimer and Kahne identify them as working, paying taxes, obeying laws, recycling, and volunteering.

Participatory Citizen The participatory citizen is a citizen who makes ’the system’. For instance, they are identified as organizing new efforts and taking leadership roles.

Justice Oriented Citizen The justice oriented citizen is a citizen who questions ’the system’. They are identified as being critical of how existing structures serve the needs of the population and devising new structures which might address those problems.

3.1.3 Changing Citizenship in the Digital Age[3]

In this piece, Bennet discusses a dichotomy between two variants of citizen.

Actualizing Citizen The actualizing citizen does not feel the need to perform civic duty; but feels that they have an individual duty. Participation in the default democratic structures, such as elections, is shadowed by other behaviors. The actualizing citizen is cynical about the honesty of the political theater. Groups of actualized citizens are loosely organized.

Dutiful Citizen The dutiful citizen partakes in the default democratic structures; voting is critically important. They stay informed on issues through the media; and join organizations for like minded individuals.

3.1.4 Constructive Politics as Public Work: Organizing the Literature[4]

In this piece, Boyte discusses the citizen in terms of public work.

Public Worker Boyte "posits citizens as co-creators of the world, not simply deliberators and decision-makers about the world." His view is that participation in public work is a democratic primitive, and by performing it individuals will be invested in the system. This is a means of creating real power and influence in the public spheres. This work is public in the sense of its visibility, its purpose, and its creators.

3.1.5 Mistrustful Citizen[5]

Ethan Zuckerman (advisor to this project), in works yet to be published, but discussed in a Re:publica keynote, describes a type of citizenship which incentivizes monitorial behavior. This incentive is rooted in the fundamental mistrust in institutions which has emerged in the last several decades[20][2] Zuckerman's belief is that this mistrust is here to stay, but it can be utilized for good.

3.2 Summary

There are many different models and types of citizenship out there, and none of them are an *ulitmate* model citizenship. Indeed, many of these models rest on the fact that there will be some mixture of these behaviors. Moreover, a citizen can have a "grab bag" of behaviors. Perhaps they are Monitorial on one issue, but Dutiful on another. The interplay between these concepts deserves much more attention, but they are enumerated above so that the following subsection can discuss an important set of behaviors they fail to cover.

3.3 The Militial Citizen

The Militial Citizen is a new step further past Schudson's Monitorial Citizen, and augments Zuckerman's mistrustful citizen with a set of tools. If a Mistrustful citizen, who is auditing the governments activity on a specific issue discovers wrongdoings, and wishes to fulfil their Monitorial Duties, the Militial Citizen model provides the answer to the question of how they might observe a governmental body that doesn't want to be observed as well as take action

[2] as Zuckerman points out, "When you ask Americans whether they trust their government to do the right thing most of the time, 24% answer yes"

against the corruption and wrongdoing the observe. It is not enough for one citizen to find out, they must be able to spread their *intel* and strategically organize without the eyes of government surveillance. To do so necessitates a specific set of tools which can be used to protect the right to *Liberty of Information.* And the best way to protect the right to this liberty is with strong information security.

However the tools it necessitates are not tools in the sense that they have one mode of use which can solve a specific problem. These tools are a Swiss army knife; access to the Swiss army knife gives them the set of tools needed both to creatively solve the problems they face and to protect themselves and their friends from danger. The types of tools that are required to be this kind of citizen are dependent on the potential avenues of oppression a population might face.

It is important to note that being a militial citizen does not neccessitate having an agenda. The militial citizen is in a state of preparedness, ready *and able* to spring into action if need be. Zuckerman talks about the auditable promises made by Fernando Haddad to the citizens of San Paulo, Brazil[5]. Being able to audit is not enough, citizens must be able to communicate freely when their audits fail and have the capability of taking action.

Participation as a militial citizen fill the missing role of the to-the-roots decentralized militia where all individuals perform basic training and then mobilize their skills on issues (or battles) which are personally relevant.

Because the facets of this training technically include sometimes a subset of the public *building* the tools for use by the greater public, elements of the Public Work Citizen model also are prominent.

3.3.1 Appeal to Rights

Furthermore, the training with and development of these tools are fundamentally guaranteed rights of the American citizen[3]. The tools which would be needed to be used are a provable right, in that the government is not required to serve as an intermediate to the rights, these tools allow citizens to have them permissionlessly. It has been shown, especially by Edward Snowden's Revelations, that the government has been ham-fisted in it's approach to it's citizen's information[21].

These are rights that citizens *deserve* to have tools to protect, a strictly stronger protection than words on a page. This suggests a resurgence of the Rights-Conscious citizen, but with a new forum for fighting rights battles other than the courts; the computer. Because cryptography an make certain operations virtually guaranteed, such as the "right" to message content privacy in peer to peer communications, this is like appealing to the court of mathematics. But nonetheless, words have meaning and certain words are guiding principles.

The courts will continue to be important, and they may even circumvent some holy assumptions made in cryptography[4]. And so:

The First Amendment

[3] And with our American ivory tower hats on, fundamental rights for all citizens of the world

[4] Such as the government being able to compel your secret keys[22]

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Speech Code is speech[23]. The tools to allow people to perform these functions are mostly code, therefore their distribution is protected. Furthermore, the functionality of these tools can in turn protect the freedom of speech, partially eliminating the burden of government to protect it – citizens can fight for it.

The Press These tools work to protect the freedoms of the press. The press can safely interact with sensitive sources, acquire and process vast text corpora, and publish them in an uncensorable way. Furthermore, they can protect themselves from intimidation or assassination attempts by employing scorched-earth defensive strategies like dead-man switches.

Assembly The tools could provide ways to assemble in virtual space which can be unregulated and proceed without interference as well as provide utilities to organize in person Assembly without informing 3rd parties.

Petition the Government Certain tools could be used to allow the government to receive signed petitions which can be anonymously, but verifiably signed so that the burden is lightened on petition organizers to identify their constituents.

The Second Amendment

> A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

These tools are very much weapons. Yes, they can focus on defensive means primarily but a strong information defense allows one to dabble safely in offense.

Securing the State A strong argument could be made that training with such tools there are more individuals able to build secure infrastructure. The cyber-insecurity of much of the United States is a grave threat; for example there are consistently media reports that hackers may be able to take out the grid. Being able to get intelligence data on all United States citizens would also be a major breach; therefore spreading knowledge of such tools is directly in the interest of securing the state.

Bearing Arms The people have a fundamental right to keep and bear arms. This is one of the most hotly contested bits of the constitution, but most of the conversation is with regards to firearms. However, arms are both offensive and defensive, and bullets aren't the only form of armament. Using a broader definition, there is no right to restrict the bearing of information security tools such as cryptography and network security because they are quintessential arms in the information war.

3.3.2 Prior Art

There have been other prior efforts which look similar to this model of citizenship and provide good guidance on the direction for this project.

Critical Engineering Julian Oliver [24] is an engineer and an artist, and has created projects such as the Transparency Grenade, a device that can be thrown like a traditional explosive grenade but logs all snoop-able network traffic and local audio onto a remote server [25]. More importantly, Julian and a few other artist hackers wrote the Critical Engineering Manifesto, a document that outlines principles an activist technologist should adhere to (see Appendix B). In addition, they hold an annual set of workshops in Berlin every October since 2011[26].

CryptoParty CryptoParty[6] describes itself as

> a decentralized, global initiative to introduce basic cryptography tools - such as the Tor anonymity network, public key encryption (PGP/GPG), and OTR (Off The Record messaging) - to the general public.

It was started in reaction to a piece of bad Australian legislation on cybercrimes. It's fundamental idea is that getting people together to get guidance on crypto technology and learn how to protect themselves is the way forward. The parties are encouraged to be maximally inclusive, with content aimed at novice computer users, heavy encouragement to be zero-cost to participants, open to the public, and a strictly enforced non-harassment policy [27][28].

Circuit Riders The "Circuit Rider" movement, which started in 1996, aimed to place information technology savvy activists at various grassroots organizations and non profits. However the movement faced challenge from corporate interests which wanted to profit from providing IT services to these organizations, which they were able to respond to with Free and Open Source Software (FOSS)[29]. The FOSS mentality, as a movement, is still outside the mindset of most users.

Tactical Technology Collective The Tactical Technology Collective, which formed in 2003, supports several thousand activists with technology training every year[30]. In addition to training, they also produce projects such as security in-a-box which have comprehensive guides for activists to learn about privacy and security[31].

Where Militial Citizen Differs The difference with the Militial Citizen is that everyone is a member of the militia. It's not a right reserved to activists or non-profits, but rather something that should be enjoyed by all. Furthermore, it is important to make the importance clear to those who do not yet recognize the importance of the knowledge, whereas Tactical Tech and Circuit Riders seem to have targeted those who want the technology actively. In the Militial model there would be no need for either of these, all citizens would equip themselves with these tools as a default form of participation and *apply* them when needed. This is a win for CryptoParty and Critical Engineering, they are designed to be more open participation, but this participation needs to be active, a yearly set of beginner workshops held outside the U.S. is not quite efficient to constitute militia training, and it seems no one has organized a CryptoParty in the last few years.

Of course, this is not to discount the Prior art, it provides guidance and instruction for the bootstrapping of a transformation to this new model of citizenship.

4 The Proposal

In order to move the Militial Citizenship Model from idea to implementation, I propose creating the first of a new kind of militia, which is focused on fighting ignorance in the population on matters of cybersecurity and privacy.

I think that the formation of such an advocacy group is an effective means to combating civic disinterest, while learning real defense tools. This has the potential to be a part of a new 'joiner' movement, the death of which Putnam lamented[32]. By being a part of something, people may care about the issue more.

In order to build this new militia, an initial corpus of motivating factors and organization must be formed.

4.1 Non-Violence and Defensive Techniques

A key part of this is to focus on non-violence and defensive techniques. Even the Black Panther Party, a notoriously violent organization, placed heavy emphasis on non violent techniques for citizen wellbeing, such as providing breakfast for school children[33]. By focusing on positive use case technology, the negative connotations of militia can be neatly side stepped while gaining the sense of civic duty being fulfilled.

4.2 Accessibility

4.2.1 Expense

Joining the militia should be cheap, activities should mostly be runnable by anyone with a shoestring budget[5].

4.2.2 Engagement

The militia should be fun, heavily promoting play and collaboration. Training exercises are all about the secure exchange of information — the exchange of information[6] requires partners.

4.2.3 Prior Skills

The militia would assume some level of comfort with a computer, and would be much easier to participate with some coding ability. In otehr words, it would b hard to join the militia

[5] All that should be needed is access to a computer, which can be had for ¡ $30

[6] For sticklers: yes you can and should secure your own information as well

when you can't march a mile.

However, the militia can attempt to offer baseline training programs to get people to this point. Additionally, exercises can be tuned to address groups with less programming experience, and additional "learn-to-program" workshops can be included[7].

4.3 Goals

The goal is comfort with the core tech and a desire to learn more. The goal certainly not the production of fully functioning industrial grade software, but to imbue people with a functional sense of empowerment.

These exercises can be considered *symbolic gestures*. The effect is not necessarily the direct results of the action, but rather the mental conditioning of having performed the routine. The related research on this topic is rich. The facial feedback hypothesis – the theory that expressions can change emotions – has been experimentally shown in many experiments, including one in which participants who were forced to smile found cartoons funnier than counterparts who were made to frown[34].

Terry Crews, a very muscular actor and former NFL player, had a particularly salient description of the importance of symbolic gestures with respect to going to the gym in a reddit Ask Me Anything[35]:

> TREAT THE GYM LIKE A SPA.
>
> Yes. It has to feel good. I tell people this a lot - go to the gym, and just sit there, and read a magazine, and then go home. And do this every day.

What Crews makes clear is that the focus *must* be on enjoyment. People do what they like to do. Even if they are aware of the longterm potential consequences of inaction, including life-or-death matters such as health, an individual has only a certain threshold of tolerance for unenjoyable activities which combat longterm consequence.

This places and additional emphasis on the importance of engagement for the overall accessibility of this medium. For maximum impact, the exercises should include a socially enjoyable part as well. This cannot be generally prescribed; different groups have different concepts of fun. For instance: drinking beer and eating pizza during and or after might be an effective way to attract college aged participants[8]. An event catered to elementary-school girls could be based around a sleepover[9].

This points to a more general principle; not everyone joins the same militia, but we would like for militia membership to be ubiquitous. It is unlikely, for example, that elementary-

[7] The author is extremely biased and happens to believe he can teach almost anyone who wants to the basics of programming in an hour or so

[8] Although it would run counter to Habermas' notion of sobriety being required to create a working public sphere.

[9] The author recognizes this is slightly gendered, but who didn't love a sleepover when they were younger? It would be more trivial, and require less of a footnote to have selected *children* rather than *girls*. But there are difficulties facing women who want to be involved in tech (here's a random citation about the matter, there are dozens which could be referenced[36]). And so the point of selecting gendered language is not to reinforce stereotypes, but to exclaim that even in the face of stereotypes, this model is inclusive, therefore there is no valid excuse to not include excluded groups in the design of this.

school girls would hang out with college student, let alone engage in joint training exercises with them! It is everyone's right to be a part of the militia.

This movement shouldn't aim to create a single group, with a single set of priorities, but rather encourage ownership over the groups direction and activities. This ties back to the social principle, groups of friends will continue to hang out. The difficulty lies in sustaining the groups prioritization of the militia's training functionality.

4.4 Initial Workshops

To kickstart the militia training, I have developed an initial set of workshops that teach people how to make nonviolent freedom-promoting technology and demonstrate it to advocate for privacy. Key to this is be demonstrating simple to build yet subversive technology which allows people to openly communicate.

In initial set of workshops, I focused on two categories of security: Theory and Practice[10]. There are a total of two labs, one on theory and one on practice.

I propose the following labs, with ample room to include more:

4.4.1 Roll your own crypto:

Common wisdom says to never roll your own crypto[37] – this workshop will anyways.

We'll try to exploit our implementations for subtle bugs.

The workshop will end with a key-signing party on both our protocol and a *"real"* standardized protocol. This will help make sure all participants know how to communicate to each other securely.

Lamport Signatures In order to make the workshop more accessible, the protocol implemented was selected for ease of understanding. However, ease of understanding is not at odd with security; in general the easier to understand a system the more secure it is[11]

Lamport signatures as actually a *very cool* signature scheme. They are believed to be resistant to quantum computer cracking attempts. The chief drawback is that a Lamport key should only be used once, however there are tricks to getting around this that make ample fodder for the workshop.

Lamport signatures work as follows[38]:

- Generate a list of 256 pairs of random 256-bit numbers. This list is the *secret key.*
- Take the secret key and , using a cryptographic *hash function* – or a function where you can solve equations of the form $hash(x) = y$ for y given x very easily, but never for x given y – which returns a 256-bit digest[12], hash each number into a list. This list is the *public key.*
- Make the public key know to whomever you would like to later sign a message.

[10] In classic MIT fashion, *Mens et Manus*

[11] Compared to a harder to understand system with similar guarantees otherwise, a simpler system will be easier to verify and implement.

[12] Such as SHA256

- To sign a message M, hash M and then, for each bit in the 256-bit message hash if it is 0 then publicize the first random number of the corresponding pair in the secret key, otherwise (if the bit is 1) publicize the second. All of the publicized random numbers from the secret key are the *signature*.

- To verify a message M against a public key K and a signature S, hash M and then, for each bit in the 256-bit message hash if it is 0 then the hash of the corresponding random number in S should be the first hash in the corresponding pair in K, otherwise (if the bit is 1) it should match the second. If this is true for all 256 bits, then the signature matches the message.

This scheme, while providing utmost security, is simple enough to be understood by someone with almost no cryptographic, mathematic, or programming background in an afternoon.

This lab is in development and will be available at `https://github.com/JeremyRubin/Lamport-Signatures`

4.4.2 Tortise

Platforms like Twitter have been enormously important tools for civic change. However, these platforms are centralized and serve as a single point of failure for an unpopular movement, and Twitter encourages non anonymity of users.

Can we do better than Twitter? Technologies like Tor allow for users to anonymously connect to the internet, and host hidden applications over it.

In this lab, participants will learn how to build a toy decentralized anonymous distributed application, explore some attacks against it, and how to mitigate them. Discussion will continue into incentivization schemes and how we might harden this into a real application.

What is Tortise Tortise is a (very) simple, distributed, decentralized Twitter which runs over Tor. It is designed to be a good basis for learning more about how to build systems on top of privacy protecting technology like Tor.

Instructions

1. Make sure you have the latest python installed, using a tool like brew

2. Clone this repository to your home directory

3. Install Tor Browser: https://www.torproject.org/

4. Add the following lines to your torrc file.

   HiddenServiceDir /Users/<YOUR USERNAME>/tortise/priv
   HiddenServicePort 80 127.0.0.1:8083

Hints:

- You'll need to customize the directory paths to wherever you cloned this repo!
- The priv/ subfolder will automatically be created
- My torrc is located at: /Applications/TorBrowser.app/TorBrowser/Data/Tor/torrc
- Still Need help? https://www.torproject.org/docs/tor-hidden-service.html.en has more detailed instructions

Fun Fact: the -rc suffix doesn't really stand for anything useful, but you can think of it as resource configuration.

5. (Re)Start TorBrowser.
6. in src/, run **python run.py**, and leave it running. This is your server.
   You may need some dependencies:
   pip install PySocks
   pip install tornado
7. check priv/hostname to see your onion address (keep key in priv private)
8. Paste the address into the Tor Browser to connect.
9. visit /peer on your website to put your friends domains (ie, http://<hostname>/ in and send/recieve messages
10. CHALLENGE EXERCISES:
    (a) Make your peers persistent: that is, make it so that you don't need to reconnect every time
    (b) Allow People to post messages with a username...
        i. Make that username a keypair!
    (c) Make a nicer user interface
    (d) Clear out old messages
    (e) Make it so that only you can post to your server

This lab is in development and will be made available at `https://github.com/JeremyRubin/tortise`.

4.5 Contextualizing

As discussed previously, these workshops must be *contextualized* so that disparate groups can fully engage. To that end, we will consider the workshops in the context two group *personas*, our sleepover-loving elementary school girls, and our college-aged beer-drinking pizza-lovers. For each persona, interaction with one workshop will be narrated.

These hypothetical situations are not intended to be completely accurate but rather paint a believable narrative for how this might realistically integrate into diverse communities.

4.5.1 Elementary School Girls and Tortise

Our elementary school girls are in the 6th grade. They are all active Girl Scouts. It's the weekend, and their parents have agreed to let them have a sleepover at one of the girl's parent's houses as part of their Girl Scout program. Girl Scout events frequently have an educational component; tonight's topic, selected by the hosting parent, is computer security. All of them can use a computer, but none of them have programming experience.

The evening starts off as any typical Girl Scout sleepover event does[13]: dinner and a physical activity. After those, the event turns to the topic; tonight the girls will be learning how to build Tortise.

First the host parent teaches the girls how to code for an hour. The parent has fully configured Raspberry Pi computers which makes it easier to control for things like environment errors. Follow the introduction to coding, the host parent talks about anonymity and privacy and Tor's role in protecting those. The parent, knowing the audience, talks about note passing in class. The girls wouldn't like it if the teacher could see the notes they were passing, right? Tor is described as a way that they can bundle notes together such that the sender and receiver of the notes cannot be discerned.

Then, they are split into groups of three to begin working on Tortise. The parent has gone through the code from the repo and stubbed out some of the methods for the girls to implement so that they have to do a small, easy set of tasks to get it running (depending on how well the girls pick up coding, perhaps even just running the fully implemented example or connecting the peers).

The girls are allowed to keep the Raspberry Pi and are told that if they enjoyed the exercise, there are a lot of other really fun exercises to do and work on; they are given information about how to learn more. The parent also engages the girls in a discussion about the note passing from earlier; is it really the teacher's right to stop note passing? To read the notes? The parent emphasizes that learning about this technology is really central to them being able to express their fundamental freedoms.

4.5.2 College Aged Beer-Drinkers/Pizza-Lovers and Roll Your Own Crypto

Our college aged beer-drinkers and pizza-lovers are on campus for a long weekend holiday. They are of a mixed set of majors, some technical, some not. They are all friends through a program they did together their freshman year. They hear about an interesting workshop called, "Free as in Pizza, Free as in Beer, and Free as in Freedom" and agree to check it out. The workshop is organized by some of the hackers on campus.

One of the hacker organizers open up by talking about making bets, and says that he/she will take any proposed bet for $10 so long as it is written on paper and passed to the front. A confident participant passes forward an easy bet, "I bet that this is written on a piece of paper". However, along the way one of the other hackers conspicuously modifies the message to an impossible claim. The students laugh at the impossible claim[14], and the hackers begin to talk about why it would be important to be able to digitally sign a message.

[13] I have no intel on what these might be like, but I'm hypothesizing based on my Boy Scouts experience. Apologies for any and all inaccuracies — please do read the earlier footnote on this subject

[14] something about the participant's mother most likely

Another hacker organizer starts to talk about digital signatures, and goes into the ideas behind a Lamport signature. The presenter ends by asking, “Who wants to build this, show of hands?”. A good portion of hands go up. The hacker asks, “Would any brave volunteer *who didn’t* raise their hand like to share why?” Some discussion ensues, and the concern from them is that they don’t have any message they would like to authenticate[15]. The hackers give them 10 examples they might want to protect, and eventually the nay sayer is convinced that they *might* like to know a little but more.

Before they can continue, the hackers want to get a sense of the attendees skill level. Most of those in attendance, including our group of friends, have, “tried coding once” – but mostly they mean they did some HTML in Middle school. The Hackers running the event pass out slips of paper to run a quick pop-quiz to divide people into groups based on ability and friends:

> Define a function, in python syntax, which squares every element of an input list and returns a list of the numbers in reverse. If you don’t know python pick a syntax.
> Write one friend you would like to work with, or no preference.

The organizers put the responses into a spreadsheet, grading the solutions. Once everyone has answered, then they pair people up such everyone is working with a friend, and also someone who solved the coding challenge.

With the set of steps needed to produce a Lamport signature on the board, the hackers tell the attendees to, “Get Hacking!” and filter about the room helping people when they get stuck.

Following people getting their implementations to work, the organizers lead a follow-up discussion on what people thought. They emphasize the importance of having common high-quality protocols that everyone can use, and tell people about how they can use them. They then tell people about the next event topic, and people head out.

4.5.3 Limitations and Strengths of Narratives

While these narratives are *nice*, they are by no means non-fiction. However, they do point to a general potential setting within which to try these; future work could be testing the workshops in these environments to see what the challenges are in getting people to really care and continue to learn more about the topics. It would also be interesting to explore more personas, for instance it would be of particular interest to craft a story of how this might integrate with African American Citizen journalists.

The strength of the narrative lies in the fact that they are able to exploit stereotypes to let us imagine how things might play out, and plan against it. For instance, the apathetic college student who only cares about beer and pizza is engaged by the topic of making bets, and elementary school students regularly pass notes.

[15] A play on the classic, I have nothing to hide

5 Discussion

Overall, this paper identifies the militia as a missing facet of democratic life, presents a new model of citizenship – the Militial Citizen – and explores with personas a potential design for the bootstrapping of such a system through accessible workshops.

The design expressed so far focuses on the large picture goals as well as beginning to delve into the longer term planning. It is critical for mission of the group to make the sense of empowerment through technology widespread. The first step is getting more people involved, but then what? Perhaps public demonstrations, perhaps more introductory workshops; with decent membership established this side of things will flourish. But at a certain point, there will be an issue. And this won't just be a militia in name only, people will use there tools to effect social change. Perhaps they will build a "real" Tortise, or invent a new quantum hard crypto scheme based on Lamport signatures. Perhaps the government will try to crack down. What issues will be worth fighting for is unclear, and hard to preprescribe. But if the population doesn't know how to fight before they *need* to fight, then perhaps it will be too late.

As great as this all may sound, I still think the label of a militia could be an obstacle to the greater adoption – much like calling a group a 'clan' might give the wrong impression as well. While I don't think that hiding the militia-oriented design is paramount, branding it as such could be harmful. And given the importance of inclusivity in this design, it would be a violation of the core principles to call it a militia if that negatively impacts the potential reach of this movement. Instead I want to use a valid but infrequently used term for this kind of movement, a combine. To combine means to unify and bring together. Combine, a group can be greater than the sum of its parts.

Will you join The Combine?

Appendices

A CryptoParty Manifesto[6]

"Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth." - Oscar Wilde

In 1996, John Perry Barlow, co-founder of the Electronic Frontier Foundation (EFF), wrote 'A Declaration of the Independence of Cyberspace'. It includes the following passage:

> Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.
>
> We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.
>
> We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Sixteen years later, and the Internet has changed the way we live our lives. It has given us the combined knowledge of humankind at our fingertips. We can form new relationships and share our thoughts and lives with friends worldwide. We can organise, communicate and collaborate in ways never thought possible. This is the world we want to hand down to our children, a world with a free Internet.

Unfortunately, not all of John Perry Barlows vision has come to pass. Without access to online anonymity, we can not be free from privilege or prejudice. Without privacy, free expression is not possible.

The problems we face in the 21st Century require all of humanity to work together. The issues we face are are serious: climate change, energy crises, state censorship, mass surveillance and on-going wars. We must be free to communicate and associate without fear. We need to support free and open source projects which aim to increase the commons knowledge of technologies that we depend on http://opensourceecology.org/wiki Contribute!

To realise our right to privacy and anonymity online, we need peer-reviewed, crowd-sourced solutions. CryptoParties provide the opportunity to meet up and learn how to use these solutions to give us all the means with which to assert our right to privacy and anonymity online.

- We are all users, we fight for the user and we strive to empower the user. We assert user requests are why computers exist. We trust in the collective wisdom of human beings, not software vendors, corporations or governments. We refuse the shackles of digital gulags, lorded over by vassal interests of governments and corporations. We are the CypherPunk Revolutionaries.

- The right to personal anonymity, pseudonymity and privacy is a basic human right. These rights include life, liberty, dignity, security, right to a family, and the right to live without fear or intimidation. No government, organisation or individual should prevent people from accessing the technology which underscores these basic human rights.

- Privacy is the right of the individual. Transparency is a requirement of governments and corporations who act in the name of the people.

- The individual alone owns the right to their identity. Only the individual may choose what they share. Coercive attempts to gain access to personal information without explicit consent is a breach of human rights.

- All people are entitled to cryptography and the human rights crypto tools afford, regardless of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, political, jurisdictional or international status of the country or territory in which a person resides.

- Just as governments should exist only to serve their citizens - so too, cryptography should belong to the people.Technology should not be locked away from the people.

- Surveillance cannot be separated from censorship, and the slavery it entails. No machine shall be held in servitude to surveillance and censorship. Crypto is a key to our collective freedom.

- Code is speech: code is human created language. To ban, censor or lock cryptography away from the people is to deprive human beings from a human right, the freedom of speech.

- Those who would seek to stop the spread of cryptography are akin to the 15th century clergy seeking to ban the printing press, afraid their monopoly on knowledge will be undermined.

B THE CRITICAL ENGINEERING MANIFESTO[7]

0. The Critical Engineer considers Engineering to be the most transformative language of our time, shaping the way we move, communicate and think. It is the work of the Critical Engineer to study and exploit this language, exposing its influence.

1. The Critical Engineer considers any technology depended upon to be both a challenge and a threat. The greater the dependence on a technology the greater the need to study and expose its inner workings, regardless of ownership or legal provision.

2. The Critical Engineer raises awareness that with each technological advance our techno-political literacy is challenged.

3. The Critical Engineer deconstructs and incites suspicion of rich user experiences.

4. The Critical Engineer looks beyond the "awe of implementation" to determine methods of influence and their specific effects.

5. The Critical Engineer recognises that each work of engineering engineers its user, proportional to that user's dependency upon it.

6. The Critical Engineer expands "machine" to describe interrelationships encompassing devices, bodies, agents, forces and networks.

7. The Critical Engineer observes the space between the production and consumption of technology. Acting rapidly to changes in this space, the Critical Engineer serves to expose moments of imbalance and deception.

8. The Critical Engineer looks to the history of art, architecture, activism, philosophy and invention and finds exemplary works of Critical Engineering. Strategies, ideas and agendas from these disciplines will be adopted, re-purposed and deployed.

9. The Critical Engineer notes that written code expands into social and psychological realms, regulating behaviour between people and the machines they interact with. By understanding this, the Critical Engineer seeks to reconstruct user-constraints and social action through means of digital excavation.

10. The Critical Engineer considers the exploit to be the most desirable form of exposure.

References

[1] M. Schudson, “Changing Concepts of Democracy.” [Online]. Available: http://web.mit.edu/comm-forum/papers/schudson.html

[2] J. K. Joel Westheimer, “What Kind of Citizen? The Politics of Educating for Democracy.” [Online]. Available: http://democraticdialogue.com/DDpdfs/WhatKindOfCitizenAERJ.pdf

[3] W. L. Bennett, “Changing Citizenship in the Digital Age.” [Online]. Available: https://mitpress.mit.edu/sites/default/files/titles/content/9780262524827_sch_0001.pdf

[4] H. Boyte, “Constructive Politics as Public Work: Organizing the Literature.” [Online]. Available: http://civicmediaclass.mit.edu/wp-content/uploads/sites/11/2015/03/Boyte-Constructive_Politics_as_Public_Work.pdf

[5] E. Zuckerman, “Re:Publica Keynote: The System Is Broken – That’s the Good News.” [Online]. Available: http://www.ethanzuckerman.com/blog/2015/05/05/republica-keynote-the-system-is-broken-thats-the-good-news/

[6] “Cryptoparty Handbook,” 2013. [Online]. Available: http://mirror-de.cryptoparty.is/handbook/index.html

[7] D. V. Julian Oliver, Gordan Savicic, “The Critical Engineering Manifesto,” 2011-2014. [Online]. Available: http://criticalengineering.org/

[8] “Militia — definition of militia by merriam-webster.” [Online]. Available: http://www.merriam-webster.com/dictionary/militia

[9] M. Owens, “Army clause.” [Online]. Available: http://www.heritage.org/constitution/#!/articles/1/essays/52/army-clause

[10] C. Dougherty, “The Minutemen, the National Guard and the Private Militia Movement: Will the Real Militia Please Stand Up?” 28 John Marshall Law Review 959, 962-970 (Summer 1995) (195 footnotes).

[11] V. R. Randall, “The History of the Militia in the United States,” law 801: Health Care Law Seminar. [Online]. Available: http://academic.udayton.edu/health/syllabi/bioterrorism/8military/milita01.htm

[12] United States Federal Bureau of Investigation, “Domestic Terrorism: Focus on Militia Extremism.” [Online]. Available: http://www.fbi.gov/news/stories/2011/september/militia_092211

[13] Wikipedia, “Militia organizations in the United States — Wikipedia, the free encyclopedia,” 2015, [accessed 10-May-2015]. [Online]. Available: http://en.wikipedia.org/wiki/Militia_organizations_in_the_United_States

[14] Anti Defamation League, “The Militia Movement.” [Online]. Available: http://archive.adl.org/learn/ext_us/militia_m.html?LEARN_Cat=Extremism&LEARN_SubCat=Extremism_in_America&xpicked=4&item=mm

[15] J. Roland, 1996-2015. [Online]. Available: http://www.constitution.org/mil/cs_milit.htm

[16] “10 U.S. Code 311 - Militia: composition and classes.” [Online]. Available: https://www.law.cornell.edu/uscode/text/10/311

[17] “The Vaping Militia.” [Online]. Available: http://thevapingmilitia.org/

[18] J. Donovan, “What Might Occupy’s Nonviolent Militia Look Like?” 2013. [Online]. Available: http://interoccupy.net/blog/what-might-occupys-nonviolent-militia-look-like/

[19] G. Brecher, “War Nerd: The long, sleazy history behind a Googler’s ”Nonviolent Militia”,” 2014. [Online]. Available: http://pando.com/2014/02/12/war-nerd-the-long-sleazy-history-behind-a-googlers-nonviolent-militia/

[20] Pew Research Center, “Public Trust in Government: 1958-2014.” [Online]. Available: http://www.people-press.org/2014/11/13/public-trust-in-government/

[21] Wikipedia, “Edward Snowden — Wikipedia, the free encyclopedia,” 2015, [accessed 10-May-2015]. [Online]. Available: http://en.wikipedia.org/wiki/Edward_Snowden

[22] M. H. Hanni Fakhoury, “Prosecutors Demand Laptop Password in Violation of Fifth Amendment ,” 2011. [Online]. Available: https://www.eff.org/press/archives/2011/07/08

[23] G. Coleman, “Code is speech: Legal tinkering, expertise, and protest among free and open source software developers.” [Online]. Available: https://steinhardt.nyu.edu/scmsAdmin/uploads/005/984/Coleman-Code-is-Speech.pdf

[24] J. Oliver. [Online]. Available: http://julianoliver.com/output/category/about

[25] ——, “The Transparency Grenade,” 2012. [Online]. Available: http://transparencygrenade.com/

[26] D. V. Julian Oliver, Gordan Savicic, “Critical Engineering Intensive Workshop Series,” 2011-2014. [Online]. Available: http://criticalengineering.org/courses/

[27] “How To CryptoParty,” 2015. [Online]. Available: https://www.cryptoparty.in/organize/howto

[28] “Guiding Principles,” 2015. [Online]. Available: https://www.cryptoparty.in/guiding_principles

[29] P.-B. McInerney, “Technology Movements and the Politics of Free/Open Source Software,” 2007. [Online]. Available: http://tigger.uic.edu/~pbm/Publications/McInerney-Open%20Source%20paper.pdf

[30] "About us: Tactical Technology Collective," 2015. [Online]. Available: https://www.tacticaltech.org/about

[31] F. Tactical Technology Collective, "security in-a-box — tools and tactics for digital security." [Online]. Available: https://securityinabox.org/en

[32] R. D. Putnam, *Bowling Alone*. Simon & Schuster, 2000, ch. The Collapse and Revival of American Community. [Online]. Available: https://www.nytimes.com/books/first/p/putnam-alone.html

[33] M. Potorti, "Feeding Revolution: The Black Panther Party and the Politics of Food," 2014. [Online]. Available: http://radicalteacher.library.pitt.edu/ojs/index.php/radicalteacher/article/view/80

[34] S. S. Fritz Strack, Leonard L. Martin, "Inhibiting and facilitating conditions of the human smile: A nonobtrusive test of the facial feedback hypothesis." vol. 54, 1988, pp. 768–777.

[35] T. Crews, "Terry Crews (back again on reddit). AMA!" 2015. [Online]. Available: https://www.reddit.com/r/IAmA/comments/2u4h7f/terry_crews_back_again_on_reddit_ama/co52d5s

[36] D. J. Armstrong and C. K. Riemenschneider, "The barriers facing women in the information technology profession: An exploratory investigation of ahuja's model," in *Proceedings of the 52Nd ACM Conference on Computers and People Research*, ser. SIGSIM-CPR '14. New York, NY, USA: ACM, 2014, pp. 85–96. [Online]. Available: http://doi.acm.org/10.1145/2599990.2600006

[37] Stack Exchange User Polynomial, "Why shouldn't we roll our own?" [Online]. Available: http://security.stackexchange.com/questions/18197/why-shouldnt-we-roll-our-own

[38] Wikipedia, "Lamport signature — Wikipedia, the free encyclopedia," 2015, [accessed 10-May-2015]. [Online]. Available: http://en.wikipedia.org/wiki/Lamport_signature