

# Securing the 2020 Election Process

(... or at least *one or two parts* of it!)

David Dittrich <dave.dittrich@gmail.com>

TA3M Seattle  
March 19, 2018  
v1.3.0

Introduction: the 2016 Election  
What is being done?  
Securing Operations with D2  
Summary

<https://staff.washington.edu/dittrich/home/dims.html>



## Distributed Incident Management System (DIMS)

David Dittrich, Linda Parsons

[dittrich@u.washington.edu](mailto:dittrich@u.washington.edu), [linda.parsons@nextcentury.com](mailto:linda.parsons@nextcentury.com)

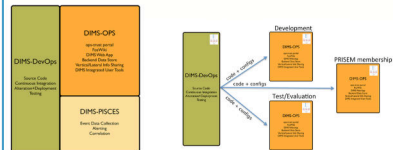


### Summary

The Distributed Incident Management System (DIMS) project is intended to take semi-automated sharing of structured threat information (MITRE's STIX technology), building on the success of the Public Regional Infrastructure Security Event Management (PRISEM) project and leveraging the portal used by an existing community of operational security professionals known as *Trident*, and scale it to the next level. DIMS takes advantage of the open message bus architecture used by PRISEM, features that support identification of friend or foe, and the ability to integrate three data sources maintained by PRISEM (network flow history, event history, and attacker context history) to support the triage process, cross-organizational correlation of events, and anonymization to promote privacy-sensitive sharing of security event data. Working with use cases defined by MITRE and PRISEM users, building features necessary to simplify structured information sharing, and operationalizing these within these existing communities, will allow DIMS to fill existing gaps in capabilities and support existing missions that are slowed down today by many complicated, manual processes.

### System Architecture

The DIMS project integrates over a dozen independent open source system components, some developed by the DIMS team and many more by other open source projects into three functional sub-systems. **DIMS-DevOps** uses a continuous integration environment using Jenkins for software build and deployment, Ansible for automated system configuration and software installation, fed from forty eight separate Git source repositories, to deploy and manage **DIMS-OPS** and **DIMS-PISCES** comprised of a range of foundational services on "bare-metal" servers, virtual machines, and Docker containers.



### Dashboard

The DIMS Dashboard is the primary user interface for analysts. Workflows are organized to interrogate disparate data sets needed for detailed analysis.



### Reputation/CIF



DIMS uses the Collective Intelligence Framework (CIF) for feeds of likely foe targets. Investigations based on known foes proceed to identify events linking friendly host activities with foes.

### Indicators of Compromise

DIMS developed Java bindings to MITRE's STIX schemas, enabling programmatic authoring, ingest and sharing of indicators using industry standards.

### Trust/Collaboration

DIMS leverages *Trident* for trust group management, self-managed vetting, user attributes, and secure email communications. (<https://trident.11/>) DIMS adds CIDR blocks and DNS domains to support real-time triage and filtering.



### Host Forensics



DIMS links these IOCs with network flows, reputation data, and event logs to derive times and file system attributes. Leveraging the open source Sleuthkit forensics library, DIMS employs systematic and efficient whole disk acquisition, storage and search, enabling rapid response in malware identification.

### Acknowledgments

DIMS is funded by the Department of Homeland Security under contract H98420C13C0003.  
D2DB Cyber Security Division R&D Sponsorship.  
Electronic Warfare & Information, 101 & 102-103, 10-10, 2014



# Outline

- 1 Introduction: the 2016 Election
  - Who are the Stakeholders?
  - What are the Threatened Targets?
  - What is getting attention?
- 2 What is being done?
  - ... to assure X?
  - The Gap
- 3 Securing Operations with D2
  - What is D2?
  - Service Components

# Outline

- 1 Introduction: the 2016 Election
  - Who are the Stakeholders?
  - What are the Threatened Targets?
  - What is getting attention?
- 2 What is being done?
  - ... to assure X?
  - The Gap
- 3 Securing Operations with D2
  - What is D2?
  - Service Components

# Who are the Stakeholders?

## Election Officials

Secretaries of State, County Elections Boards

## The Electorate

The voting public (the *key stakeholders*)

## Political Campaigns & Candidates

Candidates, National and state political parties, staff, volunteers, *dirty tricksters*

## Self-Interested Parties

PACs, voting rights advocates, wealthy donors, *intel agencies, organized criminals, terrorists*

# Who are the Stakeholders?

## Election Officials

Secretaries of State, County Elections Boards

## The Electorate

The voting public (the *key stakeholders*)

## Political Campaigns & Candidates

Candidates, National and state political parties, staff, volunteers, *dirty tricksters*

## Self-Interested Parties

PACs, voting rights advocates, wealthy donors, *intel agencies, organized criminals, terrorists*

# Who are the Stakeholders?

## Election Officials

Secretaries of State, County Elections Boards

## The Electorate

The voting public (the *key stakeholders*)

## Political Campaigns & Candidates

Candidates, National and state political parties, staff, volunteers, *dirty tricksters*

## Self-Interested Parties

PACs, voting rights advocates, wealthy donors, *intel agencies, organized criminals, terrorists*

## Who are the Stakeholders?

### Election Officials

Secretaries of State, County Elections Boards

### The Electorate

The voting public (*the key stakeholders*)

### Political Campaigns & Candidates

Candidates, National and state political parties, staff, volunteers, *dirty tricksters*

### Self-Interested Parties

PACs, voting rights advocates, wealthy donors, *intel agencies, organized criminals, terrorists*



## Who are the Stakeholders?

### Election Officials

Secretaries of State, County Elections Boards

### The Electorate

The voting public (*the key stakeholders*)

### Political Campaigns & Candidates

Candidates, National and state political parties, staff, volunteers, *dirty tricksters*

### Self-Interested Parties

PACs, voting rights advocates, wealthy donors, *intel agencies, organized criminals, terrorists*

# Outline

- 1 Introduction: the 2016 Election
  - Who are the Stakeholders?
  - What are the Threatened Targets?
  - What is getting attention?
- 2 What is being done?
  - ... to assure X?
  - The Gap
- 3 Securing Operations with D2
  - What is D2?
  - Service Components



## Threatened Targets

### Integrity of voter perceptions

Manipulation  
of the  
*perceptions,*  
*emotions,*  
*and*  
*opinions* of  
voters

### Integrity of election results

Accurate  
*recording and*  
*tabulation* of  
votes cast

### Availability of your ballot

Ease of  
registering to  
vote, staying on  
voter roles,  
ability to sign  
in and vote on  
election day

### Confidentiality of party com- munications

Privacy of com-  
munications,  
internal  
documents,  
confidential  
data

## Threatened Targets

### Integrity of voter perceptions

Manipulation  
of the  
*perceptions,  
emotions, and  
opinions* of  
voters

### Integrity of election results

Accurate  
*recording and  
tabulation* of  
votes cast

### Availability of your ballot

Ease of  
registering to  
vote, staying on  
voter roles,  
ability to sign  
in and vote on  
election day

### Confidentiality of party com- munications

Privacy of com-  
munications,  
internal  
documents,  
confidential  
data

## Threatened Targets

### Integrity of voter perceptions

Manipulation  
of the  
*perceptions,  
emotions, and  
opinions* of  
voters

### Integrity of election results

Accurate  
*recording and  
tabulation* of  
votes cast

### Availability of your ballot

Ease of  
registering to  
vote, staying on  
voter roles,  
ability to sign  
in and vote on  
election day

### Confidentiality of party com- munications

Privacy of com-  
munications,  
internal  
documents,  
confidential  
data

## Threatened Targets

### Integrity of voter perceptions

Manipulation  
of the  
*perceptions,*  
*emotions,*  
*and*  
*opinions* of  
voters

### Integrity of election results

Accurate  
*recording and*  
*tabulation* of  
votes cast

### Availability of your ballot

Ease of  
registering to  
vote, staying on  
voter roles,  
ability to sign  
in and vote on  
election day

### Confidentiality of party com- munications

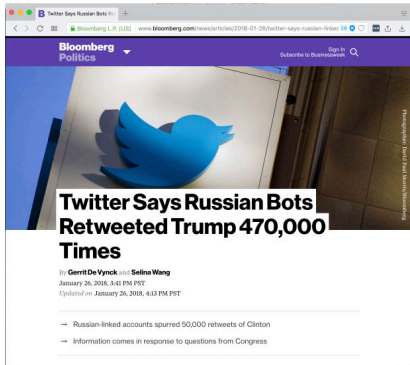
Privacy of com-  
munications,  
internal  
documents,  
confidential  
data

# Outline

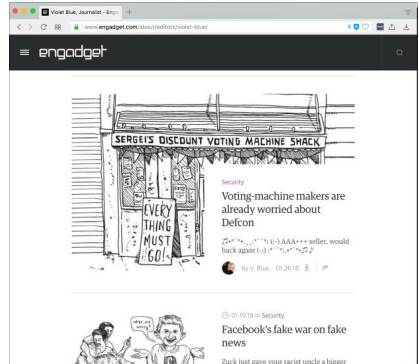
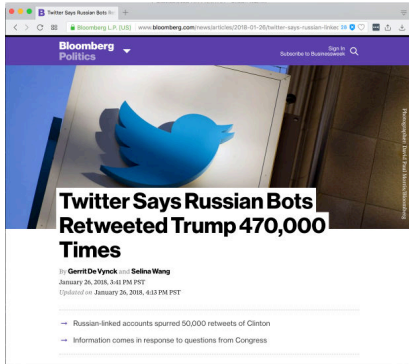
- 1 Introduction: the 2016 Election
  - Who are the Stakeholders?
  - What are the Threatened Targets?
  - What is getting attention?
- 2 What is being done?
  - ... to assure X?
  - The Gap
- 3 Securing Operations with D2
  - What is D2?
  - Service Components



# Attention!



# Attention!



# Attention!

Integrity of  
voter  
perceptions

Lots of  
attention

Integrity of  
election results

Lots of  
attention

Availability of  
your ballot

Less attention

Confidentiality  
of party com-  
munications

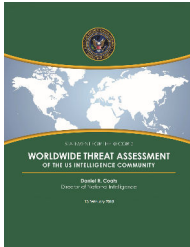
Less attention

# Outline

- 1 Introduction: the 2016 Election
  - Who are the Stakeholders?
  - What are the Threatened Targets?
  - What is getting attention?
- 2 What is being done?
  - ... to assure X?
  - The Gap
- 3 Securing Operations with D2
  - What is D2?
  - Service Components

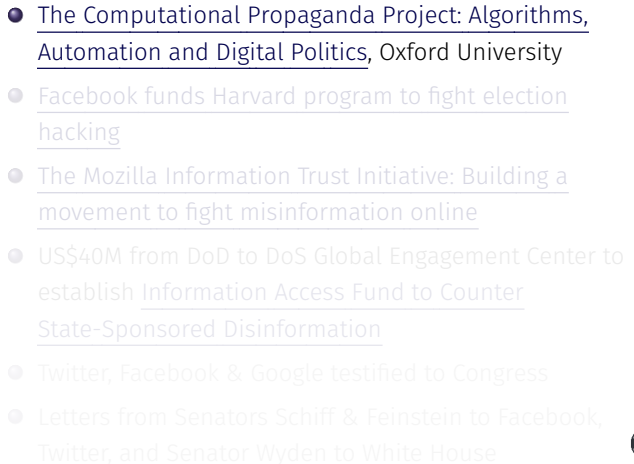
# What is being done so far?

... to assure *integrity of voter perceptions*.



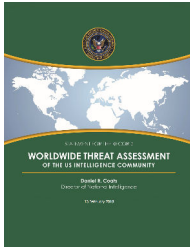
- The Computational Propaganda Project: Algorithms, Automation and Digital Politics, Oxford University
- Facebook funds Harvard program to fight election hacking
- The Mozilla Information Trust Initiative: Building a movement to fight misinformation online
- US\$40M from DoD to DoS Global Engagement Center to establish Information Access Fund to Counter State-Sponsored Disinformation
- Twitter, Facebook & Google testified to Congress
- Letters from Senators Schiff & Feinstein to Facebook, Twitter, and Senator Wyden to White House

... to assure *integrity of voter perceptions*.



# What is being done so far?

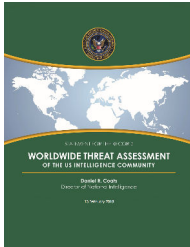
... to assure *integrity of voter perceptions*.



- The Computational Propaganda Project: Algorithms, Automation and Digital Politics, Oxford University
- Facebook funds Harvard program to fight election hacking
- The Mozilla Information Trust Initiative: Building a movement to fight misinformation online
- US\$40M from DoD to DoS Global Engagement Center to establish Information Access Fund to Counter State-Sponsored Disinformation
- Twitter, Facebook & Google testified to Congress
- Letters from Senators Schiff & Feinstein to Facebook, Twitter, and Senator Wyden to White House

# What is being done so far?

... to assure *integrity of voter perceptions*.

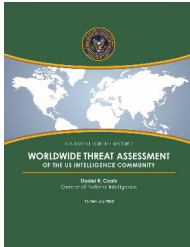


- The Computational Propaganda Project: Algorithms, Automation and Digital Politics, Oxford University
- Facebook funds Harvard program to fight election hacking
- The Mozilla Information Trust Initiative: Building a movement to fight misinformation online
- US\$40M from DoD to DoS Global Engagement Center to establish Information Access Fund to Counter State-Sponsored Disinformation
- Twitter, Facebook & Google testified to Congress
- Letters from Senators Schiff & Feinstein to Facebook, Twitter, and Senator Wyden to White House



# What is being done so far?

... to assure *integrity of voter perceptions*.



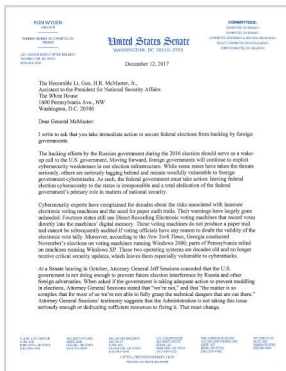
- The Computational Propaganda Project: Algorithms, Automation and Digital Politics, Oxford University
- Facebook funds Harvard program to fight election hacking
- The Mozilla Information Trust Initiative: Building a movement to fight misinformation online
- US\$40M from DoD to DoS Global Engagement Center to establish Information Access Fund to Counter State-Sponsored Disinformation
- Twitter, Facebook & Google testified to Congress
- Letters from Senators Schiff & Feinstein to Facebook, Twitter, and Senator Wyden to White House

# Letter from Senators Schiff and Feinstein

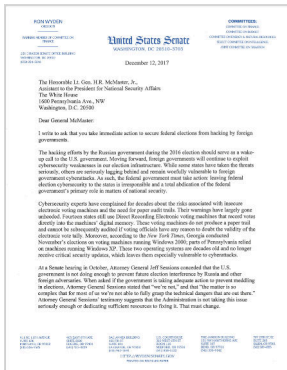
To: Facebook, Twitter

If these reports are accurate, we are witnessing an ongoing attack by the Russian government through Kremlin-linked social media actors directly acting to intervene and influence our democratic process. This should be disconcerting to all Americans, but especially your companies as, once again, it appears the vast majority of their efforts are concentrated on your platforms. This latest example of Russian interference is in keeping with Moscow's concerted, covert, and continuing campaign to manipulate American public opinion and erode trust in our law enforcement and intelligence institutions.

— Senator Adam Schiff, Senator Diane Feinstein



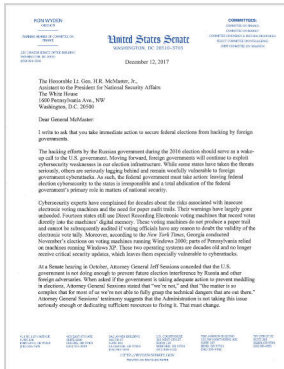
# Letter from Senator Ron Wyden To: The White House



1. Designate a senior White House official to “own” campaign security
2. Direct NIST & DHS to create a framework, “scorecards” for measuring improvement
3. Direct DHS to designate *campaigns* as critical national infrastructure
4. Direct US Secret Service to expand Presidential candidate security to include cybersecurity assistance

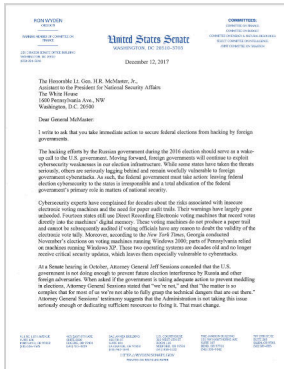
# Letter from Senator Ron Wyden

## To: The White House



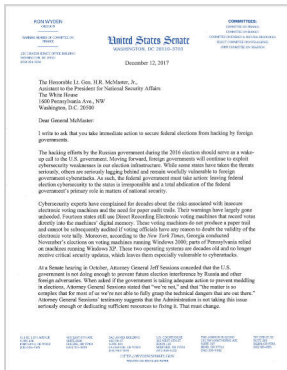
1. Designate a senior White House official to “own” campaign security
2. Direct NIST & DHS to create a framework, “scorecards” for measuring improvement
3. Direct DHS to designate *campaigns* as critical national infrastructure
4. Direct US Secret Service to expand Presidential candidate security to include cybersecurity assistance

1. Designate a senior White House official to “own” campaign security
2. Direct NIST & DHS to create a framework, “scorecards” for measuring improvement
3. Direct DHS to designate *campaigns* as critical national infrastructure
4. Direct US Secret Service to expand Presidential candidate security to include cybersecurity assistance



# Letter from Senator Ron Wyden

## To: The White House



1. Designate a senior White House official to “own” campaign security
2. Direct NIST & DHS to create a framework, “scorecards” for measuring improvement
3. Direct DHS to designate *campaigns* as critical national infrastructure
4. Direct US Secret Service to expand Presidential candidate security to include cybersecurity assistance

# What is being done so far?

... to assure *integrity of election results*.





# What is being done so far?

... to assure *integrity of election results*.

- “The Secret Ballot at Risk: Recommendations for Securing Democracy” report (Caitriona Fitzgerald, Electronic Privacy Information Center; Pamela Smith, Verified Voting Foundation; Susannah Goodman, Common Cause Education Fund)
- National Conference of State Legislatures “ALL-MAIL ELECTIONS (AKA VOTE-BY-MAIL)”
- Alex Halderman (UMICH), Matt Blaze (U Penn), Matt Bishop (UC Davis)
- Brennan Center for Justice report “Securing Elections From Foreign Interference” (Lawrence Norden and Ian Vandewalker; forward by Amb. R. James Woolsey)
- U.S. Senate and House (H.R.4884) have both introduced the “Defending Elections from Threats by Establishing Redlines Act of 2018”

## What is being done so far?

... to assure *integrity of election results*.

- “The Secret Ballot at Risk: Recommendations for Securing Democracy”  
report (Caitriona Fitzgerald, Electronic Privacy Information Center; Pamela Smith, Verified Voting Foundation; Susannah Goodman, Common Cause Education Fund)
- National Conference of State Legislatures “ALL-MAIL ELECTIONS (AKA VOTE-BY-MAIL)”
- Alex Halderman (UMICH), Matt Blaze (U Penn), Matt Bishop (UC Davis)
- Brennan Center for Justice report “Securing Elections From Foreign Interference” (Lawrence Norden and Ian Vandewalker; forward by Amb. R. James Woolsey)
- U.S. Senate and House (H.R.4884) have both introduced the “Defending Elections from Threats by Establishing Redlines Act of 2018”

## What is being done so far?

... to assure *integrity of election results*.

- “The Secret Ballot at Risk: Recommendations for Securing Democracy”  
report (Caitriona Fitzgerald, Electronic Privacy Information Center; Pamela Smith, Verified Voting Foundation; Susannah Goodman, Common Cause Education Fund)
- National Conference of State Legislatures “ALL-MAIL ELECTIONS (AKA VOTE-BY-MAIL)”
- Alex Halderman (UMICH), Matt Blaze (U Penn), Matt Bishop (UC Davis)
- Brennan Center for Justice report “Securing Elections From Foreign Interference” (Lawrence Norden and Ian Vandewalker; forward by Amb. R. James Woolsey)
- U.S. Senate and House (H.R.4884) have both introduced the “Defending Elections from Threats by Establishing Redlines Act of 2018”

# What is being done so far?

... to assure *integrity of election results*.

- “The Secret Ballot at Risk: Recommendations for Securing Democracy” report (Caitriona Fitzgerald, Electronic Privacy Information Center; Pamela Smith, Verified Voting Foundation; Susannah Goodman, Common Cause Education Fund)
- National Conference of State Legislatures “ALL-MAIL ELECTIONS (AKA VOTE-BY-MAIL)”
- Alex Halderman (UMICH), Matt Blaze (U Penn), Matt Bishop (UC Davis)
- Brennan Center for Justice report “Securing Elections From Foreign Interference” (Lawrence Norden and Ian Vandewalker; forward by Amb. R. James Woolsey)
- U.S. Senate and House (H.R.4884) have both introduced the “Defending Elections from Threats by Establishing Redlines Act of 2018”

# What is being done so far?

... to assure *integrity of election results*.

- “The Secret Ballot at Risk: Recommendations for Securing Democracy” report (Caitriona Fitzgerald, Electronic Privacy Information Center; Pamela Smith, Verified Voting Foundation; Susannah Goodman, Common Cause Education Fund)
- National Conference of State Legislatures “ALL-MAIL ELECTIONS (AKA VOTE-BY-MAIL)”
- Alex Halderman (UMICH), Matt Blaze (U Penn), Matt Bishop (UC Davis)
- Brennan Center for Justice report “Securing Elections From Foreign Interference” (Lawrence Norden and Ian Vandewalker; forward by Amb. R. James Woolsey)
- U.S. Senate and House (H.R.4884) have both introduced the “Defending Elections from Threats by Establishing Redlines Act of 2018”

# What is being done so far?

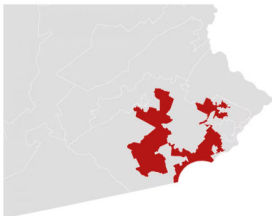
... to assure *integrity of election results*.

Belfer Center for Science and International Affairs, Harvard Kennedy School

- For Campaigns
  - [“Hacking Chads: The Motivations, Threats, and Effects of Electoral Insecurity”](#)
- For State and Local Government Officials
  - [“The State and Local Election Cybersecurity Playbook”](#)
  - [“Election Cyber Incident Communications Coordination Guide”](#)
  - [“Election Cyber Incident Communications Plan Template”](#)

## What is being done so far?

... to assure *availability of your ballot.*

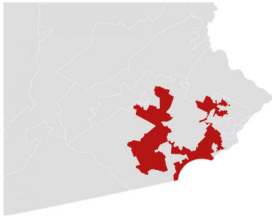


Pennsylvania's 7th  
District ("Goofy  
Kicking Donald  
Duck")

- Gerrymandering cases in multiple states, SCOTUS to review two cases in 2018
- ["The New Pennsylvania Congressional Map, District by District,"](#) by Nate Cohn, Matthew Bloch and Kevin Quealy, New York Times, February 19, 2018
- Eric Holder and the National Democratic Redistricting Committee
- Brennan Center ["Securing Elections From Foreign Interference"](#) also covers Voter Registration Databases
- Reality Winner going on trial in March for leaking NSA report

# What is being done so far?

... to assure *availability of your ballot.*



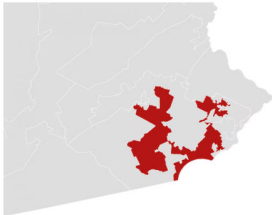
Pennsylvania's 7th  
District ("Goofy  
Kicking Donald  
Duck")

- Gerrymandering cases in multiple states, SCOTUS to review two cases in 2018
- ["The New Pennsylvania Congressional Map, District by District,"](#) by Nate Cohn, Matthew Bloch and Kevin Quealy, New York Times, February 19, 2018
- Eric Holder and the National Democratic Redistricting Committee
- Brennan Center ["Securing Elections From Foreign Interference"](#) also covers Voter Registration Databases
- Reality Winner going on trial in March for leaking NSA report



## What is being done so far?

... to assure *availability of your ballot.*

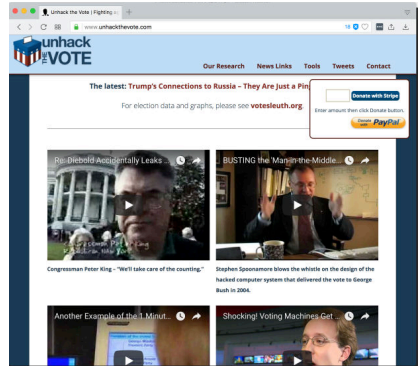


Pennsylvania's 7th  
District ("Goofy  
Kicking Donald  
Duck")

- Gerrymandering cases in multiple states, SCOTUS to review two cases in 2018
- ["The New Pennsylvania Congressional Map, District by District,"](#) by Nate Cohn, Matthew Bloch and Kevin Quealy, New York Times, February 19, 2018
- Eric Holder and the National Democratic Redistricting Committee
- Brennan Center ["Securing Elections From Foreign Interference"](#) also covers Voter Registration Databases
- Reality Winner going on trial in March for leaking NSA report

# What is being done so far?

## "Open Source" Groups



# What is being done so far?

Multiple: Google *Protect Your Electron Suite*

- Project Shield (DDoS attack mitigation)
- Password Alert (Chrome extension)
- Two-Step Verification
- Advanced Protection Program

Availability: Publishers, journalists, NGOs, and election monitoring sites operating a website containing election information.

# What is being done so far?

Multiple: Google *Protect Your Electron Suite*

- Project Shield (DDoS attack mitigation)
- Password Alert (Chrome extension)
- Two-Step Verification
- Advanced Protection Program

Availability: Publishers, journalists, NGOs, and election monitoring sites operating a website containing election information.

# What is being done so far?

Multiple: Cloudflare *Project Athenian*

- DDoS attack mitigation
- Data Protection
- Website Integrity
- Website Availability
- Support & Services

Availability: State and Local government running elections, handling voter registration and identification data, reporting election results.

# What is being done so far?

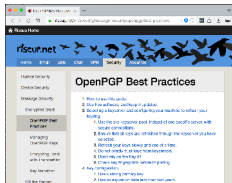
## Multiple: Cloudflare *Project Athenian*

- DDoS attack mitigation
- Data Protection
- Website Integrity
- Website Availability
- Support & Services

Availability: State and Local government running elections, handling voter registration and identification data, reporting election results.

# What is being done so far?

... to ensure *confidentiality of party communications*.



Riseup Message  
Security  
OpenPGP Best  
Practices

## ● Electronic Frontier Foundation's Surveillance Self Defense guides

### ● The grugq

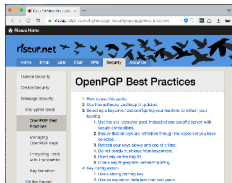
- "Campaign Information Security In Theory and Practice"
- "The Zen of PGP"
- "Operational PGP"
- "Security, Cyber, and Elections (part1, part2, part3, part4)"

## ● Harvard Kennedy School Belfer Center "Cybersecurity Campaign Playbook"

## ● Tech Solidarity "Security Guidelines for Congressional Campaigns"

# What is being done so far?

... to ensure *confidentiality of party communications*.



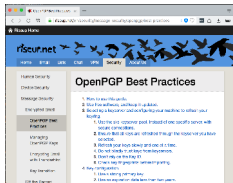
Riseup Message  
Security  
OpenPGP Best  
Practices

- Electronic Frontier Foundation's Surveillance Self Defense guides
- The grugq
  - "Campaign Information Security In Theory and Practice"
  - "The Zen of PGP"
  - "Operational PGP"
  - "Security, Cyber, and Elections (part1, part2, part3, part4)"
- Harvard Kennedy School Belfer Center "Cybersecurity Campaign Playbook"
- Tech Solidarity "Security Guidelines for Congressional Campaigns"



# What is being done so far?

... to ensure *confidentiality of party communications*.



Riseup Message  
Security  
OpenPGP Best  
Practices

- Electronic Frontier Foundation's Surveillance Self Defense guides
- The grugq
  - "Campaign Information Security In Theory and Practice"
  - "The Zen of PGP"
  - "Operational PGP"
  - "Security, Cyber, and Elections (part1, part2, part3, part4)"
- Harvard Kennedy School Belfer Center "Cybersecurity Campaign Playbook"
- Tech Solidarity "Security Guidelines for Congressional Campaigns"

# Campaign Information Security in Theory and Practice

[https://medium.com/@thegrugq/  
campaign-information-security-ff6ac49966e1](https://medium.com/@thegrugq/campaign-information-security-ff6ac49966e1)

- 1. Objective is not “don’t get hacked,” but “don’t let the adversary get useable information”
- 2. Authenticity is the only thing that people believe
- 3. The “e” in *email* stands for *evidence*
- 4. Use deception to lure the adversary out
- 5. Use deception to consume the adversary’s analytic resources (hide your lake in an ocean)
- 6. Use deception to mitigate the damage of a penetration
- 7. The way to fight trolls is with elves

# Campaign Information Security in Theory and Practice

[https://medium.com/@thegrugq/  
campaign-information-security-ff6ac49966e1](https://medium.com/@thegrugq/campaign-information-security-ff6ac49966e1)

- 1. Objective is not “don’t get hacked,” but “don’t let the adversary get useable information”
- 2. Authenticity is the only thing that people believe
- 3. The “e” in *email* stands for *evidence*
- 4. Use deception to lure the adversary out
- 5. Use deception to consume the adversary’s analytic resources (hide your lake in an ocean)
- 6. Use deception to mitigate the damage of a penetration
- 7. The way to fight trolls is with elves

# Campaign Information Security in Theory and Practice

[https://medium.com/@thegrugq/  
campaign-information-security-ff6ac49966e1](https://medium.com/@thegrugq/campaign-information-security-ff6ac49966e1)

- 1. Objective is not “don’t get hacked,” but “don’t let the adversary get useable information”
- 2. Authenticity is the only thing that people believe
- 3. The “e” in *email* stands for *evidence*
- 4. Use deception to lure the adversary out
- 5. Use deception to consume the adversary’s analytic resources (hide your lake in an ocean)
- 6. Use deception to mitigate the damage of a penetration
- 7. The way to fight trolls is with elves

# Campaign Information Security in Theory and Practice

[https://medium.com/@thegrugq/  
campaign-information-security-ff6ac49966e1](https://medium.com/@thegrugq/campaign-information-security-ff6ac49966e1)

- 1. Objective is not “don’t get hacked,” but “don’t let the adversary get useable information”
- 2. Authenticity is the only thing that people believe
- 3. The “e” in *email* stands for *evidence*
- 4. Use deception to lure the adversary out
- 5. Use deception to consume the adversary’s analytic resources (hide your lake in an ocean)
- 6. Use deception to mitigate the damage of a penetration
- 7. The way to fight trolls is with elves

# Harvard Kennedy School Belfer Center

## Top-Five Checklist

### 1. Set the tone:



Take cybersecurity seriously. Take responsibility for reducing risk, train your staff, and set the example. Human error is the number one cause of breaches.

(see pages 12)

### 2. Use the cloud:



A big, commercial cloud service will be much more secure than anything you can set up. Use a cloud based office suite like GSuite or Microsoft365 that will provide all your basic office functions and a safe place to store information.

(see pages 14-15)

### 3. Use two-factor authentication (2FA):



Require 2FA for all important accounts, including your office suite, any other email or storage services, and your social media accounts. Use a mobile app or physical key for your second factor, not text messaging.

(see pages 16-17)

### 4. Create strong, long passwords:



For your passwords, create `S0METHINGR0LL0NGLIKETH1S8TR1NG`, not something really short like `12345`. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with `LO$ OF $ymb0L$`. A password manager can help, too.

(see pages 17)

### 5. Plan and prepare:



Have a plan in case your security is compromised. Know whom to call for technical help, understand your legal obligations, and be ready to communicate internally and externally as rapidly as possible.

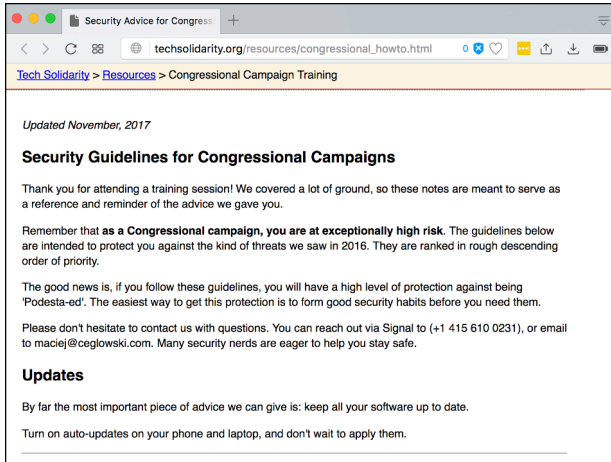
(see pages 19-22)

## “Cybersecurity Campaign Playbook”

1. Take this seriously
2. Use commercial cloud services
3. Use Two-Factor Authentication
4. Create strong passwords
5. Have a plan and be ready

# Tech Solidarity

## Congressional Campaign Training



Security Advice for Congress

techsolidarity.org/resources/congressional\_howto.html

Tech Solidarity > Resources > Congressional Campaign Training

Updated November, 2017

### Security Guidelines for Congressional Campaigns

Thank you for attending a training session! We covered a lot of ground, so these notes are meant to serve as a reference and reminder of the advice we gave you.

Remember that **as a Congressional campaign, you are at exceptionally high risk**. The guidelines below are intended to protect you against the kind of threats we saw in 2016. They are ranked in rough descending order of priority.

The good news is, if you follow these guidelines, you will have a high level of protection against being 'Podesta-ed'. The easiest way to get this protection is to form good security habits before you need them.

Please don't hesitate to contact us with questions. You can reach out via Signal to (+1 415 610 0231), or email to [maciej@ceglowski.com](mailto:maciej@ceglowski.com). Many security nerds are eager to help you stay safe.

### Updates

By far the most important piece of advice we can give is: keep all your software up to date.

Turn on auto-updates on your phone and laptop, and don't wait to apply them.

# Outline

- 1 Introduction: the 2016 Election
  - Who are the Stakeholders?
  - What are the Threatened Targets?
  - What is getting attention?
- 2 What is being done?
  - ... to assure X?
  - The Gap
- 3 Securing Operations with D2
  - What is D2?
  - Service Components



# The Gap



- Some talk of *what to do*
- Less talk about *technology enabling how to do it*
- This is where D2 fits in

# The Gap



- Some talk of *what to do*
- Less talk about *technology enabling how to do it*
- This is where D2 fits in

## The Gap



- Some talk of *what to do*
- Less talk about *technology enabling how to do it*
- This is where D2 fits in

## The Gap



- Some talk of *what to do*
- Less talk about *technology enabling how to do it*
- This is where D2 fits in

# Outline

- 1 Introduction: the 2016 Election
  - Who are the Stakeholders?
  - What are the Threatened Targets?
  - What is getting attention?
- 2 What is being done?
  - ... to assure X?
  - The Gap
- 3 Securing Operations with D2
  - What is D2?
  - Service Components

# What is D2?



- Built on open source service components
- Ansible Playbooks to configure servers & services
- Automated (terraform) or manual host creation

# What is D2?



- Built on open source service components
- Ansible Playbooks to configure servers & services
- Automated (`terraform`) or manual host creation

# What is D2?



- Built on open source service components
- Ansible Playbooks to configure servers & services
- Automated (`terraform`) or manual host creation



# What is D2?



- Built on open source service components
- Ansible Playbooks to configure servers & services
- Automated (**terraform**) or manual host creation

# What is D2?

## Technical Features

- DigitalOcean droplets, DNS, with **terraform**
- SSH host and user key management
- SSL/TLS certificate management (Letsencrypt, or self-signed)
- SSL/TLS securing RabbitMQ, Postfix, rsyslog, NGINX
- Centralized logging, distributed AMQP message bus
- Backup and restore automation for certs, portal database

# What is D2?

## Technical Features

- DigitalOcean droplets, DNS, with **terraform**
- SSH host and user key management
- SSL/TLS certificate management (Letsencrypt, or self-signed)
- SSL/TLS securing RabbitMQ, Postfix, rsyslog, NGINX
- Centralized logging, distributed AMQP message bus
- Backup and restore automation for certs, portal database

# What is D2?

## Technical Features

- DigitalOcean droplets, DNS, with **terraform**
- SSH host and user key management
- SSL/TLS certificate management (Letsencrypt, or self-signed)
- SSL/TLS securing RabbitMQ, Postfix, rsyslog, NGINX
- Centralized logging, distributed AMQP message bus
- Backup and restore automation for certs, portal database

# What is D2?

## Technical Features

- DigitalOcean droplets, DNS, with **terraform**
- SSH host and user key management
- SSL/TLS certificate management (Letsencrypt, or self-signed)
- SSL/TLS securing RabbitMQ, Postfix, rsyslog, NGINX
- Centralized logging, distributed AMQP message bus
- Backup and restore automation for certs, portal database

# What is D2?

## Technical Features

- DigitalOcean droplets, DNS, with **terraform**
- SSH host and user key management
- SSL/TLS certificate management (Letsencrypt, or self-signed)
- SSL/TLS securing RabbitMQ, Postfix, rsyslog, NGINX
- Centralized logging, distributed AMQP message bus
- Backup and restore automation for certs, portal database

# What is D2?

## Technical Features

- DigitalOcean droplets, DNS, with **terraform**
- SSH host and user key management
- SSL/TLS certificate management (Letsencrypt, or self-signed)
- SSL/TLS securing RabbitMQ, Postfix, rsyslog, NGINX
- Centralized logging, distributed AMQP message bus
- Backup and restore automation for certs, portal database

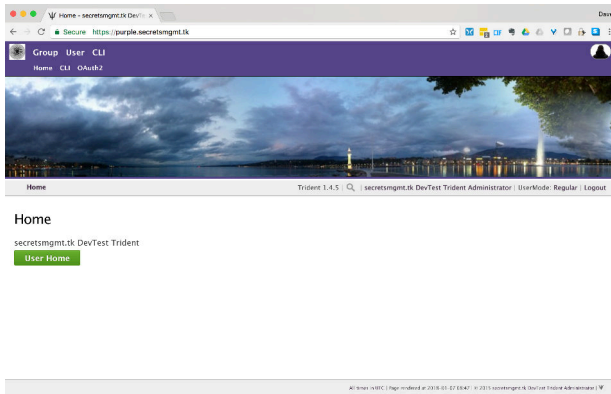
# Outline

- 1 Introduction: the 2016 Election
  - Who are the Stakeholders?
  - What are the Threatened Targets?
  - What is getting attention?
- 2 What is being done?
  - ... to assure X?
  - The Gap
- 3 Securing Operations with D2
  - What is D2?
  - Service Components



# D2 Service Components

## Trident Portal



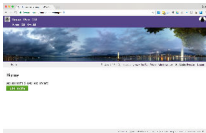
Trident Portal



# D2 Service Components

## Trident Portal

- Trust group management (nomination & vouching automation)
- PGP encrypted email lists, group keyring
- Secure wiki and file upload
- Second-factor authentication support



<https://trident.li/>

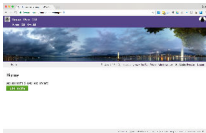
- Low cost to deploy and administer



# D2 Service Components

## Trident Portal

- Trust group management (nomination & vouching automation)
- PGP encrypted email lists, group keyring
- Secure wiki and file upload
- Second-factor authentication support



<https://trident.li/>

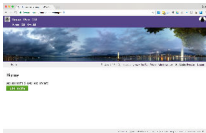
- Low cost to deploy and administer



# D2 Service Components

## Trident Portal

- Trust group management (nomination & vouching automation)
- PGP encrypted email lists, group keyring
- Secure wiki and file upload
- Second-factor authentication support



<https://trident.li/>

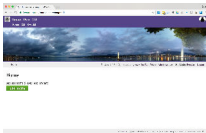
- Low cost to deploy and administer



# D2 Service Components

## Trident Portal

- Trust group management (nomination & vouching automation)
- PGP encrypted email lists, group keyring
- Secure wiki and file upload
- Second-factor authentication support



<https://trident.li/>

### 2FA Tokens

You: "Tokens Run from" (tokens)

Key: "tokens" (tokens)

Key: "tokens" (tokens)



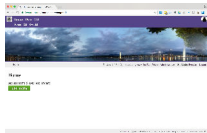
(tokens li 2FA tool)

- Low cost to deploy and administer

# D2 Service Components

## Trident Portal

- Trust group management (nomination & vouching automation)
- PGP encrypted email lists, group keyring
- Secure wiki and file upload
- Second-factor authentication support



<https://trident.li/>

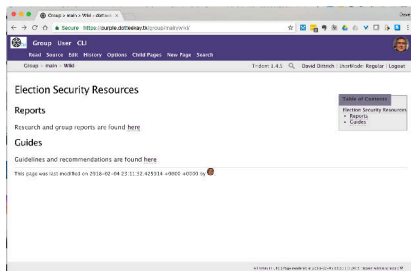
### 2FA Tokens



- Low cost to deploy and administer

## D2 Service Components

### Trident Portal: Wiki and Files



# D2 Service Components

## Trident Portal: Wiki and Files

The screenshot shows a web browser displaying the Trident Portal Wiki. The page title is "Election Security Resources". Under the "Reports" section, it says "Research and group reports are found here". Under the "Guides" section, it says "Guidelines and recommendations are found here". A sidebar on the right shows a "Table of Contents" with links to "Election Security Resources", "Reports", and "Guides". At the bottom, it says "This page was last modified on 2018-02-04 23:11:32 425314 +0000 40599 by".

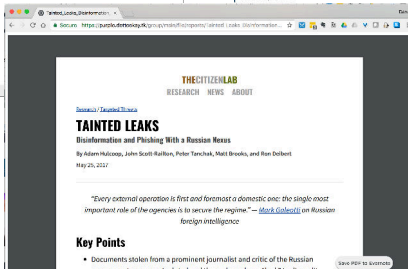
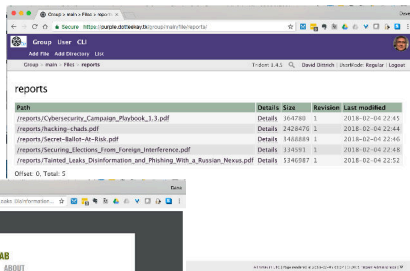
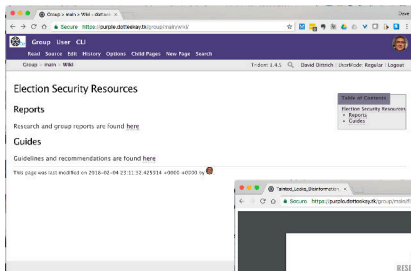
The screenshot shows a web browser displaying the Trident Portal Files page. The page title is "reports". It contains a table with columns: "Path", "Details", "Size", "Revision", and "Last modified". The table lists several files, including "Cybersecurity\_Campaign\_Playbook\_1.3.pdf", "hacking-chads.pdf", "Secret-Ballot-At-Risk.pdf", "Securing\_Elections\_From\_Foreign\_Interference.pdf", and "Tainted\_Leaks\_Disinformation\_and\_Phishing\_With\_a\_Russian\_Nexus.pdf". Below the table, it says "Offset: 0, Total: 5". At the bottom, there are two buttons: "Add a new file" and "Add a new directory".

Path	Details	Size	Revision	Last modified
/reports/Cybersecurity_Campaign_Playbook_1.3.pdf	Details	164780	1	2018-02-04 22:45
/reports/hacking-chads.pdf	Details	2428470	1	2018-02-04 22:44
/reports/Secret-Ballot-At-Risk.pdf	Details	1488889	1	2018-02-04 22:46
/reports/Securing_Elections_From_Foreign_Interference.pdf	Details	334591	1	2018-02-04 22:48
/reports/Tainted_Leaks_Disinformation_and_Phishing_With_a_Russian_Nexus.pdf	Details	1346987	1	2018-02-04 22:52



# D2 Service Components

## Trident Portal: Wiki and Files



## D2 Service Components

### Distributed Content

#### Activation of the Cyber Communications Response Team (CCRT)

Cyber-related incidents vary in size and severity, which makes it important to have a process to ensure the appropriate steps are calibrated to the significance of the incident. All incidents can be categorized under one of the following severity levels:

1. **Low:** Cyber incident that involves no PII and/or minor system disruptions that will likely not be visible to the public or affect the elections process.
2. **Medium:** Cyber incident resulting in the loss or compromise of voter data or VR systems, but formal notification obligations may not be triggered. The issue begins to become public.
3. **High:** Cyber incident that triggers U.S. or international reporting obligations, affects a large amount of voter information, and/or is destructive to election operations.

In a medium-intensity incident, [CHIEF ELECTION OFFICIAL] will need to make a judgment call about whether to activate the CCRT, but if the incident is likely to become public and raise questions about trust in the election systems, [CHIEF ELECTION OFFICIAL] should err on the side of activation. You can always deactivate if the intensity declines. Once activated, [CHIEF ELECTION OFFICIAL] along with [DIRECTOR OF ELECTIONS], will decide which level applies, based on an initial assessment. Once [CHIEF ELECTION OFFICIAL] activates the CCRT, all key response team members will be notified of the activation [INSERT STATE'S METHOD OF REACHING TEAM MEMBERS].

Belfer Communications Template

- Policies and Procedures
- Sign-in Forms, Provisional Ballot Forms
- Reports (government, industry, academia, etc.)
- OPSEC Guides, Handbooks
- Contingency Plans, Emergency Checklists
- Incident Reporting Forms

# Securing the 2020 Election Process

## Improve criminal and counter-intelligence investigations

### The Hard Truth Keeps Trickling Out, Little by Little

It increasingly looks like Russian hackers may have affected actual vote totals.



BY CHARLES P. PIERCE JUN 19, 2017

58.5K



<https://www.esquire.com/news-politics/politics/news/a55603/russia-hack-voting-totals/>



# Securing the 2020 Election Process

## Improve criminal and counter-intelligence investigations

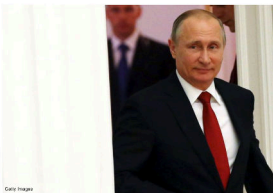
### The Hard Truth Keeps Trickling Out, Little by Little

It increasingly looks like Russian hackers may have affected actual vote totals.



BY CHARLES P. PIERCE JUN 19, 2017

58.5K



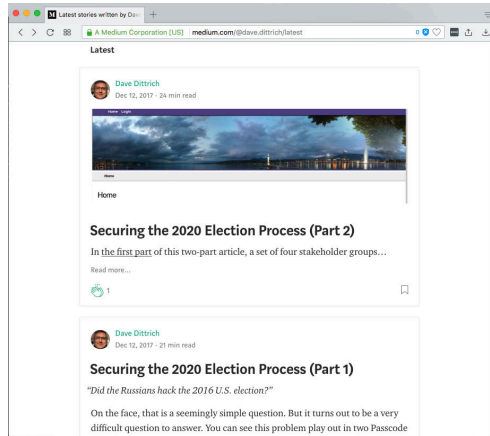
Getty Images

Illinois became Patient Zero in the government's probe, eventually leading investigators to a hacking pandemic that touched four out of every five U.S. states. Using evidence from the Illinois computer banks, federal agents were able to develop digital "signatures" -- among them, Internet Protocol addresses used by the attackers -- to spot the hackers at work. The signatures were then sent through Homeland Security alerts and other means to every state. Thirty-seven states reported finding traces of the hackers in various systems, according to one of the people familiar with the probe. In two others -- Florida and California -- those traces were found in systems run by a private contractor managing critical election systems.

<https://www.esquire.com/news-politics/politics/news/a55603/russia-hack-voting-totals/>



# Securing the 2020 Election Process



<https://medium.com/@dave.dittrich/latest>



## Where can someone get D2?

- GitHub repo:  
<https://github.com/davedittrich/ansible-dims-playbooks/>  
License: Apache 2.0 & Berkeley Three Clause
- Documentation:  
<https://davedittrich.readthedocs.io/projects/ansible-dims-playbooks/en/latest/>

- Talk to me about supporting a deployment!



## Where can someone get D2?

- GitHub repo:  
<https://github.com/davedittrich/ansible-dims-playbooks/>  
License: Apache 2.0 & Berkeley Three Clause
- Documentation:  
<https://davedittrich.readthedocs.io/projects/ansible-dims-playbooks/en/latest/>



- Talk to me about supporting a deployment!



## Where can someone get D2?

- GitHub repo:  
<https://github.com/davedittrich/ansible-dims-playbooks/>  
License: Apache 2.0 & Berkeley Three Clause
- Documentation:  
<https://davedittrich.readthedocs.io/projects/ansible-dims-playbooks/en/latest/>



- Talk to me about supporting a deployment!





# Summary

- **Mind the Gap!** (campaign and election OPSEC)
- Technology (D2) exists, but **adoption will be slow**
- Changing processes **will take effort**
- Motivation
  - 2018 mid-term elections **begin in months!**
  - 2020 campaigning **begins next year!**
  - Elections happen *around the world!* (this is not just a U.S. problem)

**Get involved in securing democracy!**



# Summary

- **Mind the Gap!** (campaign and election OPSEC)
- Technology (D2) exists, but **adoption will be slow**
- Changing processes **will take effort**
- Motivation
  - 2018 mid-term elections **begin in months!**
  - 2020 campaigning **begins next year!**
  - Elections happen *around the world!* (this is not just a U.S. problem)

Get involved in securing democracy!

# Summary

- **Mind the Gap!** (campaign and election OPSEC)
- Technology (D2) exists, but **adoption will be slow**
- Changing processes **will take effort**
- Motivation
  - 2018 mid-term elections **begin in months!**
  - 2020 campaigning **begins next year!**
  - Elections happen *around the world!* (this is not just a U.S. problem)

Get involved in securing democracy!

# Summary

- **Mind the Gap!** (campaign and election OPSEC)
- Technology (D2) exists, but **adoption will be slow**
- Changing processes **will take effort**
- Motivation
  - 2018 mid-term elections **begin in months!**
  - 2020 campaigning **begins next year!**
  - Elections happen *around the world!* (this is not just a U.S. problem)

Get involved in securing democracy!

# Summary

- **Mind the Gap!** (campaign and election OPSEC)
- Technology (D2) exists, but **adoption will be slow**
- Changing processes **will take effort**
- Motivation
  - 2018 mid-term elections **begin in months!**
  - 2020 campaigning **begins next year!**
  - Elections happen *around the world!* (this is not just a U.S. problem)

**Get involved in securing democracy!**



# Securing the 2020 Election Process

(... or at least *one or two parts* of it!)

David Dittrich <dave.dittrich@gmail.com>

TA3M Seattle  
March 19, 2018  
v1.3.0

