Securing the 2020 Election Process

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

David Dittrich <dave.dittrich@gmail.com>

April 27, 2018
ISOI XX
v1.5.0

TLP:WHITE (`+= megaphone`)

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

CENTER FOR DATA SCIENCE
UNIVERSITY of WASHINGTON | TACOMA
Institute of Technology

Distributed Incident Management System (DIMS)

David Dittrich, Linda Parsons

dittrich@u.washington.edu, linda.parsons@nextcentury.com

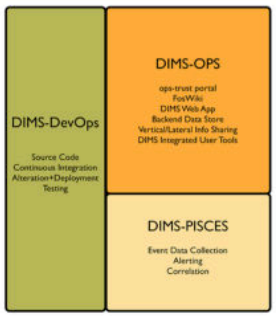
Homeland Security
Science and Technology

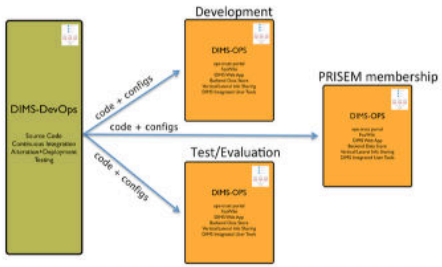
Summary

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

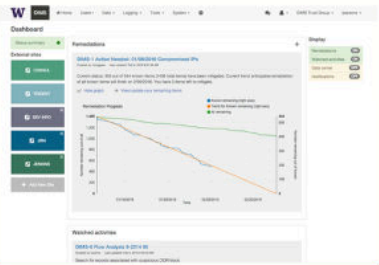
The DIMS project integrates over a dozen independent open source system components, some developed by the DIMS team and many more by other open source projects into three functional sub-systems. **DIMS-DevOps** uses a continuous integration environment using Jenkins for software build and deployment, 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.





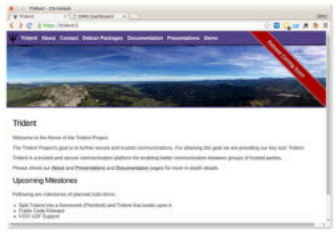
Dashboard

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

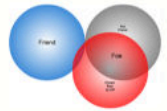


Trust/Collaboration

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



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.

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 HSHQDC-13-C-B0013

DHS Cyber Security Division R&D Showcase and Technical Workshop • Washington, DC • February 17-19, 2016

D2

Outline

Outline

Who are the Stakeholders?

D. Dittrich. The Ethics of Social Honeypots. Research Ethics, Vol 11, Issue 4, May 2015.

Election Officials	The Electorate	Political Campaigns & Candidates	Self-Interested Parties
Secretaries of State, County Elections Boards	The voting public (the *primary and key stakeholders*)	Candidates, National and state political parties, staff, volunteers, *dirty tricksters*	PACs, voting rights advocates, wealthy donors, *intel agencies, organized criminals, terrorists*

Who are the Stakeholders?

D. Dittrich. The Ethics of Social Honeypots. Research Ethics, Vol 11, Issue 4, May 2015.

Election Officials

Secretaries of State, County Elections Boards

The Electorate

The voting public (the *primary and 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?

D. Dittrich. The Ethics of Social Honeypots. Research Ethics, Vol 11, Issue 4, May 2015.

Election Officials

Secretaries of State, County Elections Boards

The Electorate

The voting public (the *primary and 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?

D. Dittrich. The Ethics of Social Honeypots. Research Ethics, Vol 11, Issue 4, May 2015.

Election Officials	The Electorate	Political Campaigns & Candidates	Self-Interested Parties
Secretaries of State, County Elections Boards	The voting public (the *primary and key stakeholders*)	Candidates, National and state political parties, staff, volunteers, *dirty tricksters*	PACs, voting rights advocates, wealthy donors, *intel agencies, organized criminals, terrorists*

Who are the Stakeholders?

D. Dittrich. The Ethics of Social Honeypots. Research Ethics, Vol 11, Issue 4, May 2015.

Election Officials	The Electorate	Political Campaigns & Candidates	Self-Interested Parties
Secretaries of State, County Elections Boards	The voting public (the *primary and key stakeholders*)	Candidates, National and state political parties, staff, volunteers, *dirty tricksters*	PACs, voting rights advocates, wealthy donors, *intel agencies*, *organized criminals*, *terrorists*

Outline

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 communications

Privacy of communications, 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 communications

Privacy of communications, 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 communications

Privacy of communications, 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 communications

Privacy of communications, 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

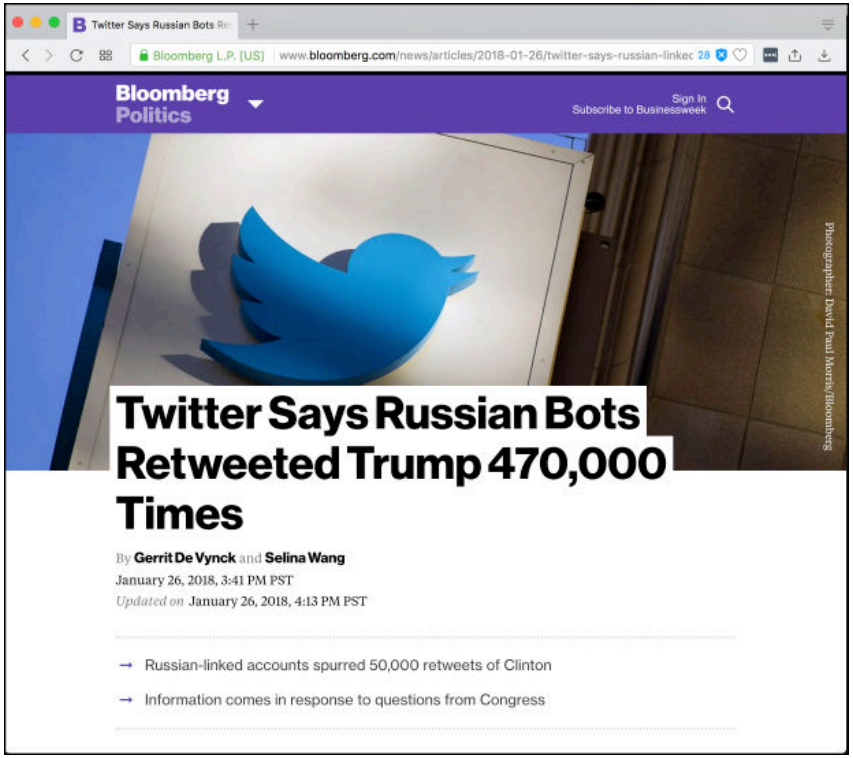
Ease of registering to vote, staying on voter roles, *ability to sign in and vote on election day*

Confidentiality of party communications

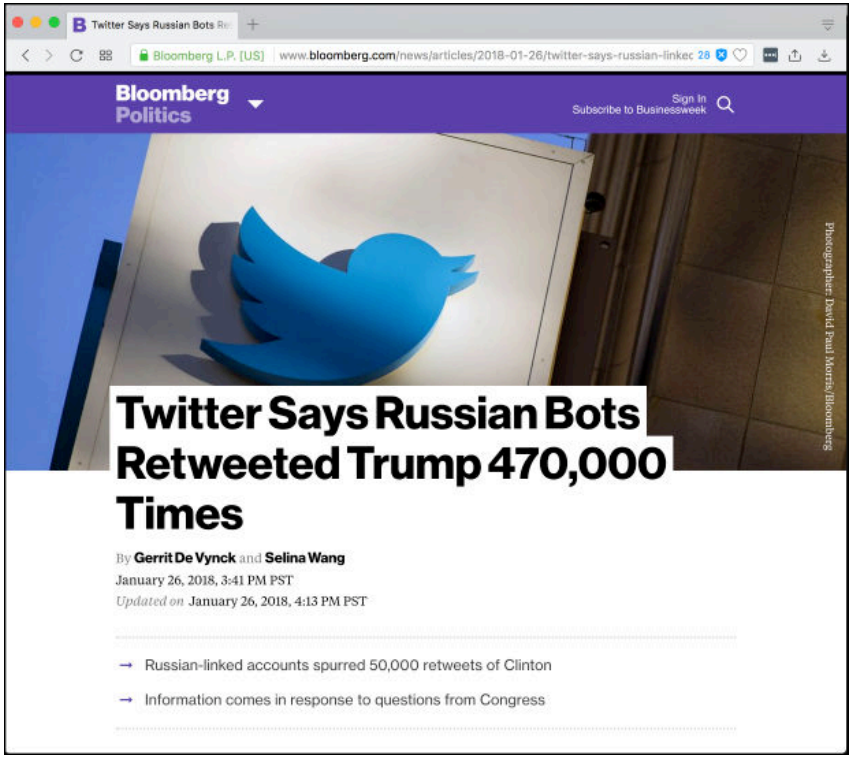
Privacy of communications, internal documents, confidential data

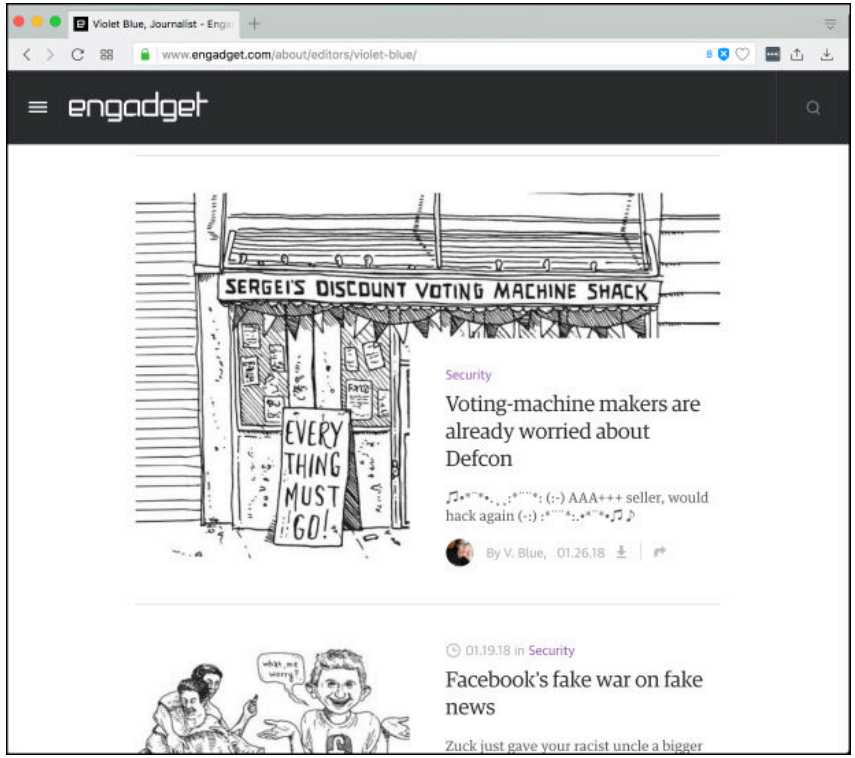
Outline

Attention!


Twitter Says Russian Bots Re
Bloomberg L.P. [US]
www.bloomberg.com/news/articles/2018-01-26/twitter-says-russian-linkec
Bloomberg
Politics
Sign In
Subscribe to Businessweek
Photographer: David Paul Morris/Bloomberg
Twitter Says Russian Bots Retweeted Trump 470,000 Times
By Gerrit De Vynck and Selina Wang
January 26, 2018, 3:41 PM PST
Updated on January 26, 2018, 4:13 PM PST
→ Russian-linked accounts spurred 50,000 retweets of Clinton
→ Information comes in response to questions from Congress

Attention!


Twitter Says Russian Bots
Bloomberg L.P. [US] www.bloomberg.com/news/articles/2018-01-26/twitter-says-russian-linkec
Bloomberg Politics
Sign In
Subscribe to Businessweek
Photographer: David Paul Morris/Bloomberg
Twitter Says Russian Bots Retweeted Trump 470,000 Times
By Gerrit De Vynck and Selina Wang
January 26, 2018, 3:41 PM PST
Updated on January 26, 2018, 4:13 PM PST
Russian-linked accounts spurred 50,000 retweets of Clinton
Information comes in response to questions from Congress


Violet Blue, Journalist - Enga
www.engadget.com/about/editors/violet-blue/
engadget
SERGEI'S DISCOUNT VOTING MACHINE SHACK
EVERY THING MUST GO!
Security
Voting-machine makers are already worried about Defcon
(:-) AAA+++ seller, would hack again (-:)
By V. Blue, 01.26.18
01.19.18 in Security
Facebook's fake war on fake news
Zuck just gave your racist uncle a bigger

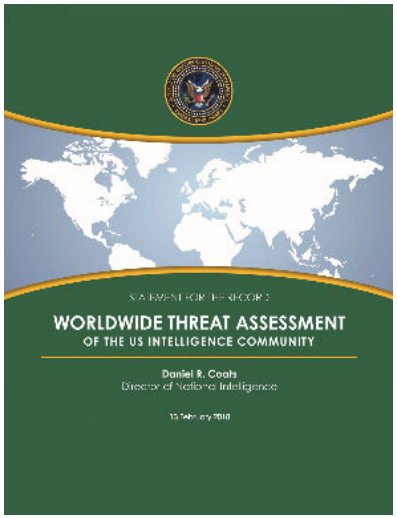
Attention!

Integrity of voter perceptions	Integrity of election results	Availability of your ballot	Confidentiality of party communications
Lots of attention	Lots of attention	~~Less~~ Getting more attention	Less attention

Outline

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

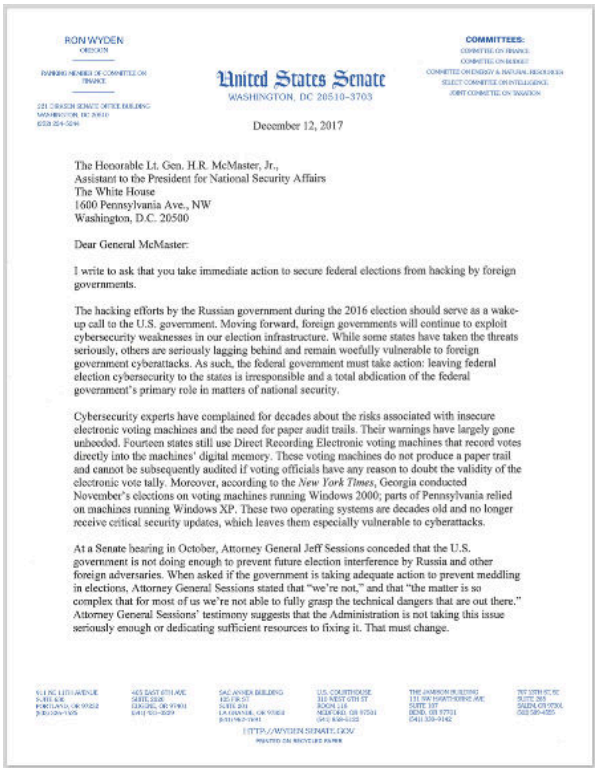
Letter from Senators Schiff and Feinstein

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



RON WYDEN
OREGON

COMMITTEES:

United States Senate
WASHINGTON, DC 20510–3703

December 12, 2017

The Honorable Lt. Gen. H.R. McMaster, Jr.,
Assistant to the President for National Security Affairs
The White House
1600 Pennsylvania Ave., NW
Washington, D.C. 20500

Dear General McMaster:

I write to ask that you take immediate action to secure federal elections from hacking by foreign governments.

The hacking efforts by the Russian government during the 2016 election should serve as a wake-up call to the U.S. government. Moving forward, foreign governments will continue to exploit cybersecurity weaknesses in our election infrastructure. While some states have taken the threats seriously, others are seriously lagging behind and remain woefully vulnerable to foreign government cyberattacks. As such, the federal government must take action: leaving federal election cybersecurity to the states is irresponsible and a total abdication of the federal government's primary role in matters of national security.

Cybersecurity experts have complained for decades about the risks associated with insecure electronic voting machines and the need for paper audit trails. Their warnings have largely gone unheeded. Fourteen states still use Direct Recording Electronic voting machines that record votes directly into the machines' digital memory. These voting machines do not produce a paper trail and cannot be subsequently audited if voting officials have any reason to doubt the validity of the electronic vote tally. Moreover, according to the *New York Times*, Georgia conducted November's elections on voting machines running Windows 2000; parts of Pennsylvania relied on machines running Windows XP. These two operating systems are decades old and no longer receive critical security updates, which leaves them especially vulnerable to cyberattacks.

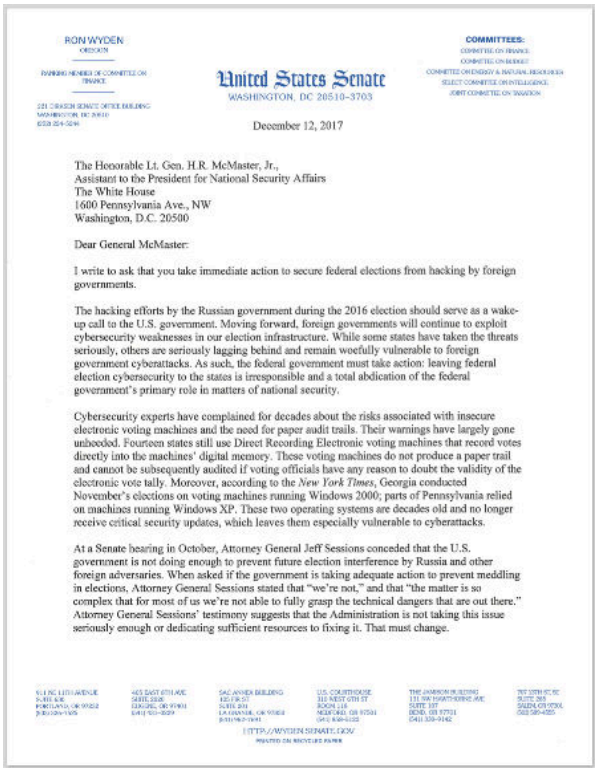
At a Senate hearing in October, Attorney General Jeff Sessions conceded that the U.S. government is not doing enough to prevent future election interference by Russia and other foreign adversaries. When asked if the government is taking adequate action to prevent meddling in elections, Attorney General Sessions stated that "we're not," and that "the matter is so complex that for most of us we're not able to fully grasp the technical dangers that are out there." Attorney General Sessions' testimony suggests that the Administration is not taking this issue seriously enough or dedicating sufficient resources to fixing it. That must change.

HTTP://WYDEN.SENATE.GOV

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



RON WYDEN
OREGON

COMMITTEES:

United States Senate
WASHINGTON, DC 20510–3703

December 12, 2017

The Honorable Lt. Gen. H.R. McMaster, Jr.,
Assistant to the President for National Security Affairs
The White House
1600 Pennsylvania Ave., NW
Washington, D.C. 20500

Dear General McMaster:

I write to ask that you take immediate action to secure federal elections from hacking by foreign governments.

The hacking efforts by the Russian government during the 2016 election should serve as a wake-up call to the U.S. government. Moving forward, foreign governments will continue to exploit cybersecurity weaknesses in our election infrastructure. While some states have taken the threats seriously, others are seriously lagging behind and remain woefully vulnerable to foreign government cyberattacks. As such, the federal government must take action: leaving federal election cybersecurity to the states is irresponsible and a total abdication of the federal government's primary role in matters of national security.

Cybersecurity experts have complained for decades about the risks associated with insecure electronic voting machines and the need for paper audit trails. Their warnings have largely gone unheeded. Fourteen states still use Direct Recording Electronic voting machines that record votes directly into the machines' digital memory. These voting machines do not produce a paper trail and cannot be subsequently audited if voting officials have any reason to doubt the validity of the electronic vote tally. Moreover, according to the *New York Times*, Georgia conducted November's elections on voting machines running Windows 2000; parts of Pennsylvania relied on machines running Windows XP. These two operating systems are decades old and no longer receive critical security updates, which leaves them especially vulnerable to cyberattacks.

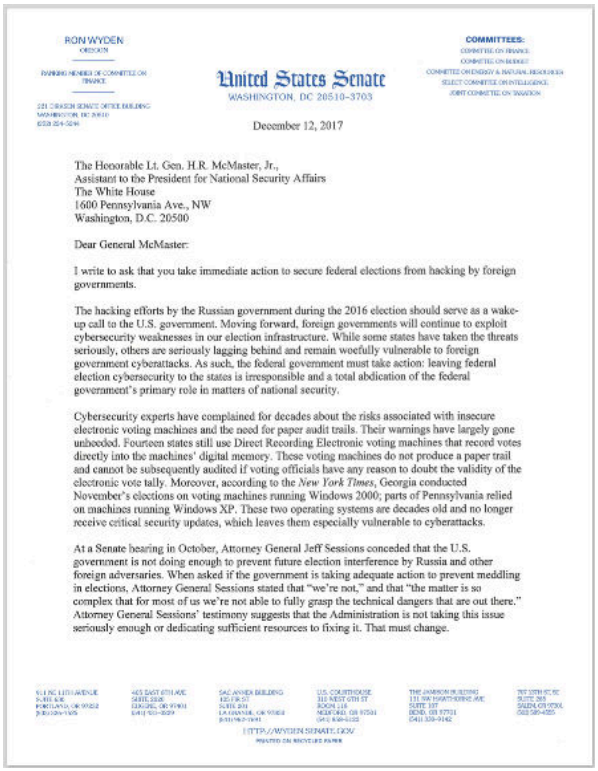
At a Senate hearing in October, Attorney General Jeff Sessions conceded that the U.S. government is not doing enough to prevent future election interference by Russia and other foreign adversaries. When asked if the government is taking adequate action to prevent meddling in elections, Attorney General Sessions stated that "we're not," and that "the matter is so complex that for most of us we're not able to fully grasp the technical dangers that are out there." Attorney General Sessions' testimony suggests that the Administration is not taking this issue seriously enough or dedicating sufficient resources to fixing it. That must change.

HTTP://WYDEN.SENATE.GOV

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



RON WYDEN
OREGON

COMMITTEES:

United States Senate
WASHINGTON, DC 20510–3703

December 12, 2017

The Honorable Lt. Gen. H.R. McMaster, Jr.,
Assistant to the President for National Security Affairs
The White House
1600 Pennsylvania Ave., NW
Washington, D.C. 20500

Dear General McMaster:

I write to ask that you take immediate action to secure federal elections from hacking by foreign governments.

The hacking efforts by the Russian government during the 2016 election should serve as a wake-up call to the U.S. government. Moving forward, foreign governments will continue to exploit cybersecurity weaknesses in our election infrastructure. While some states have taken the threats seriously, others are seriously lagging behind and remain woefully vulnerable to foreign government cyberattacks. As such, the federal government must take action: leaving federal election cybersecurity to the states is irresponsible and a total abdication of the federal government's primary role in matters of national security.

Cybersecurity experts have complained for decades about the risks associated with insecure electronic voting machines and the need for paper audit trails. Their warnings have largely gone unheeded. Fourteen states still use Direct Recording Electronic voting machines that record votes directly into the machines' digital memory. These voting machines do not produce a paper trail and cannot be subsequently audited if voting officials have any reason to doubt the validity of the electronic vote tally. Moreover, according to the *New York Times*, Georgia conducted November's elections on voting machines running Windows 2000; parts of Pennsylvania relied on machines running Windows XP. These two operating systems are decades old and no longer receive critical security updates, which leaves them especially vulnerable to cyberattacks.

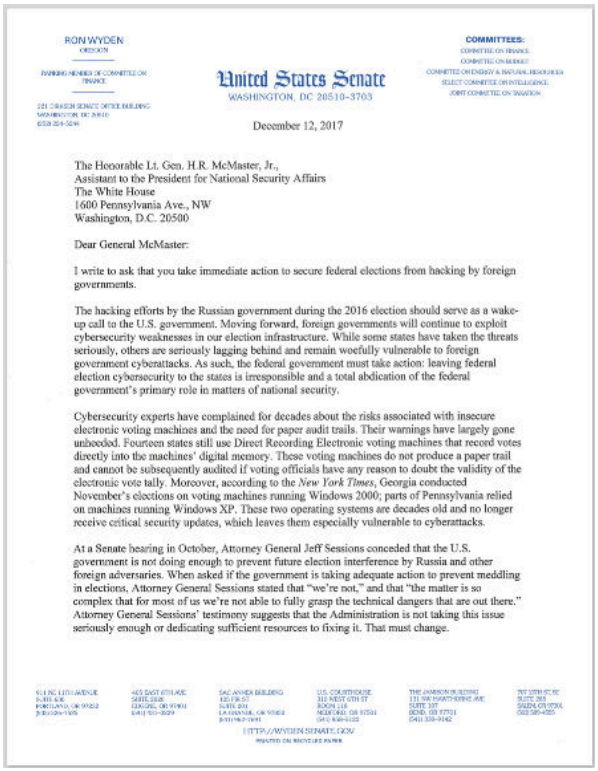
At a Senate hearing in October, Attorney General Jeff Sessions conceded that the U.S. government is not doing enough to prevent future election interference by Russia and other foreign adversaries. When asked if the government is taking adequate action to prevent meddling in elections, Attorney General Sessions stated that "we're not," and that "the matter is so complex that for most of us we're not able to fully grasp the technical dangers that are out there." Attorney General Sessions' testimony suggests that the Administration is not taking this issue seriously enough or dedicating sufficient resources to fixing it. That must change.

HTTP://WYDEN.SENATE.GOV

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



RON WYDEN
OREGON

COMMITTEES:

United States Senate
WASHINGTON, DC 20510–3703

December 12, 2017

The Honorable Lt. Gen. H.R. McMaster, Jr.,
Assistant to the President for National Security Affairs
The White House
1600 Pennsylvania Ave., NW
Washington, D.C. 20500

Dear General McMaster:

I write to ask that you take immediate action to secure federal elections from hacking by foreign governments.

The hacking efforts by the Russian government during the 2016 election should serve as a wake-up call to the U.S. government. Moving forward, foreign governments will continue to exploit cybersecurity weaknesses in our election infrastructure. While some states have taken the threats seriously, others are seriously lagging behind and remain woefully vulnerable to foreign government cyberattacks. As such, the federal government must take action: leaving federal election cybersecurity to the states is irresponsible and a total abdication of the federal government's primary role in matters of national security.

Cybersecurity experts have complained for decades about the risks associated with insecure electronic voting machines and the need for paper audit trails. Their warnings have largely gone unheeded. Fourteen states still use Direct Recording Electronic voting machines that record votes directly into the machines' digital memory. These voting machines do not produce a paper trail and cannot be subsequently audited if voting officials have any reason to doubt the validity of the electronic vote tally. Moreover, according to the *New York Times*, Georgia conducted November's elections on voting machines running Windows 2000; parts of Pennsylvania relied on machines running Windows XP. These two operating systems are decades old and no longer receive critical security updates, which leaves them especially vulnerable to cyberattacks.

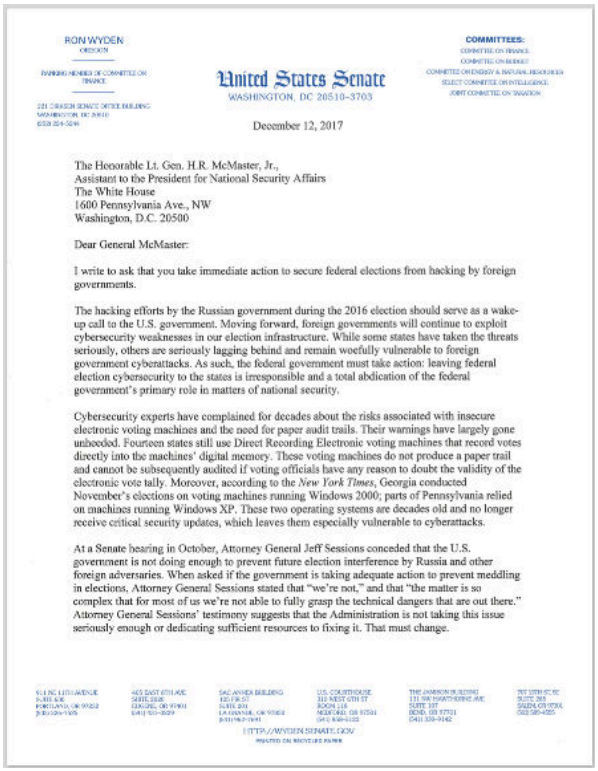
At a Senate hearing in October, Attorney General Jeff Sessions conceded that the U.S. government is not doing enough to prevent future election interference by Russia and other foreign adversaries. When asked if the government is taking adequate action to prevent meddling in elections, Attorney General Sessions stated that "we're not," and that "the matter is so complex that for most of us we're not able to fully grasp the technical dangers that are out there." Attorney General Sessions' testimony suggests that the Administration is not taking this issue seriously enough or dedicating sufficient resources to fixing it. That must change.

HTTP://WYDEN.SENATE.GOV

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



RON WYDEN
OREGON

COMMITTEES:

United States Senate
WASHINGTON, DC 20510–3703

December 12, 2017

The Honorable Lt. Gen. H.R. McMaster, Jr.,
Assistant to the President for National Security Affairs
The White House
1600 Pennsylvania Ave., NW
Washington, D.C. 20500

Dear General McMaster:

I write to ask that you take immediate action to secure federal elections from hacking by foreign governments.

The hacking efforts by the Russian government during the 2016 election should serve as a wake-up call to the U.S. government. Moving forward, foreign governments will continue to exploit cybersecurity weaknesses in our election infrastructure. While some states have taken the threats seriously, others are seriously lagging behind and remain woefully vulnerable to foreign government cyberattacks. As such, the federal government must take action: leaving federal election cybersecurity to the states is irresponsible and a total abdication of the federal government's primary role in matters of national security.

Cybersecurity experts have complained for decades about the risks associated with insecure electronic voting machines and the need for paper audit trails. Their warnings have largely gone unheeded. Fourteen states still use Direct Recording Electronic voting machines that record votes directly into the machines' digital memory. These voting machines do not produce a paper trail and cannot be subsequently audited if voting officials have any reason to doubt the validity of the electronic vote tally. Moreover, according to the *New York Times*, Georgia conducted November's elections on voting machines running Windows 2000; parts of Pennsylvania relied on machines running Windows XP. These two operating systems are decades old and no longer receive critical security updates, which leaves them especially vulnerable to cyberattacks.

At a Senate hearing in October, Attorney General Jeff Sessions conceded that the U.S. government is not doing enough to prevent future election interference by Russia and other foreign adversaries. When asked if the government is taking adequate action to prevent meddling in elections, Attorney General Sessions stated that "we're not," and that "the matter is so complex that for most of us we're not able to fully grasp the technical dangers that are out there." Attorney General Sessions' testimony suggests that the Administration is not taking this issue seriously enough or dedicating sufficient resources to fixing it. That must change.

HTTP://WYDEN.SENATE.GOV

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.*

- "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)
- 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)

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 Goverernment 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 *integrity of election results.*

- Senate Select Committee on Intelligence releases election security recommendations
- U.S. Senate and House (H.R.4884) have both introduced the "Defending Elections from Threats by Establishing Redlines Act of 2018"
- Omnibus budget has $380 Million for election security grants to states
- Current chair of the Election Assistance Commission being let go (selected by Speaker of the House)

Despite Cash From Congress, Key Election Security Issue May Not Get Fixed

But that money is going to be allocated based on the same population-based formula laid out in the 2002 Help America Vote Act, as the $380 million represents money that was approved as part of that legislation but was never spent. The U.S. Election Assistance Commission will determine the exact amount each state receives, but the [Brennan Center estimates] only two of the 13 states that use machines that lack an auditable paper trail — Arkansas and Delaware — could receive enough money to fully replace them. Most of the states are expected to receive less than 60 percent of what it would cost to fully replace the paperless systems currently in use.

— Miles Parks, NPR

What is being done so far?

Multiple: Google *Protect Your Electon* 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 Electon* 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?

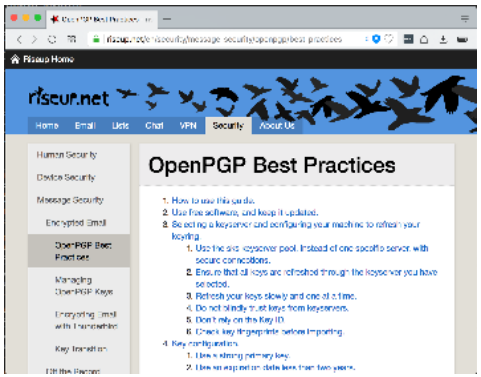
Multiple: Cloudflare *Project Athenian*

- 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.*

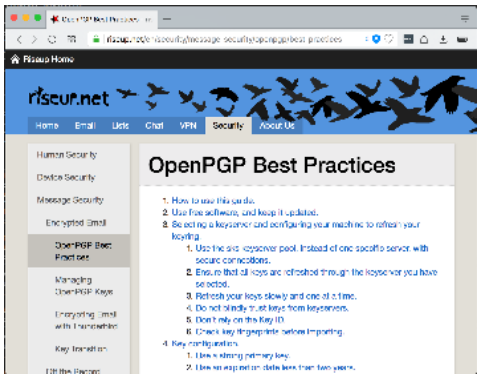


Riseup Message Security OpenPGP Best Practices

- Electronic Frontier Foundation's Surveillance Self Defense guides
- The Field Guide to Security Training in the Newsroom, OpenNews and BuzzFeed Open Lab.
- 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.*

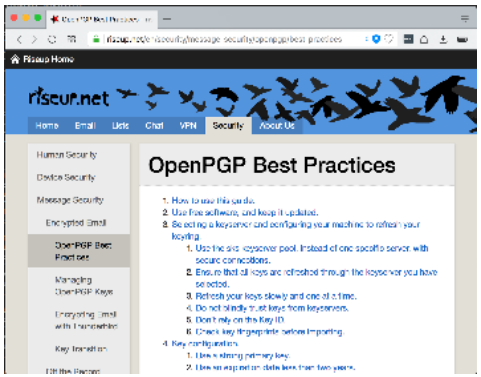


Riseup Message Security OpenPGP Best Practices

- Electronic Frontier Foundation's Surveillance Self Defense guides
- The Field Guide to Security Training in the Newsroom, OpenNews and BuzzFeed Open Lab.
- 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 Field Guide to Security Training in the Newsroom, OpenNews and BuzzFeed Open Lab.
- 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

- 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

- 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

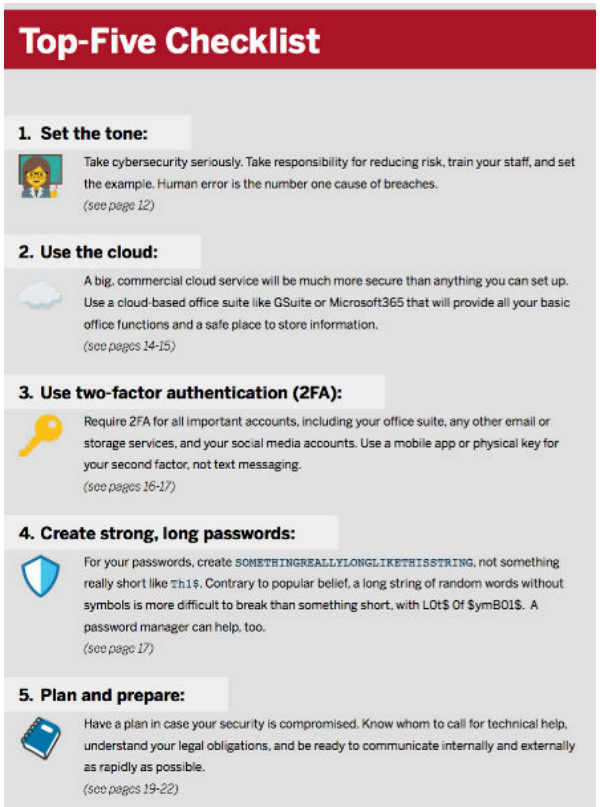
- 1. Objective is not "don't get hacked," but "don't let the adversary get useable information"
- 2. Authenticity is the only thing that people believe
- 3. The "e" in *email* stands for *evidence*
- 4. Use deception to lure the adversary out
- 5. Use deception to consume the adversary's analytic resources (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

- 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 page 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 `SOMETHINGREALLYLONGLIKETHISSTRING`, not something really short like `Th1$`. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with LOt$ Of $ymB01$. A password manager can help, too.
(see page 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

Outline

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

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

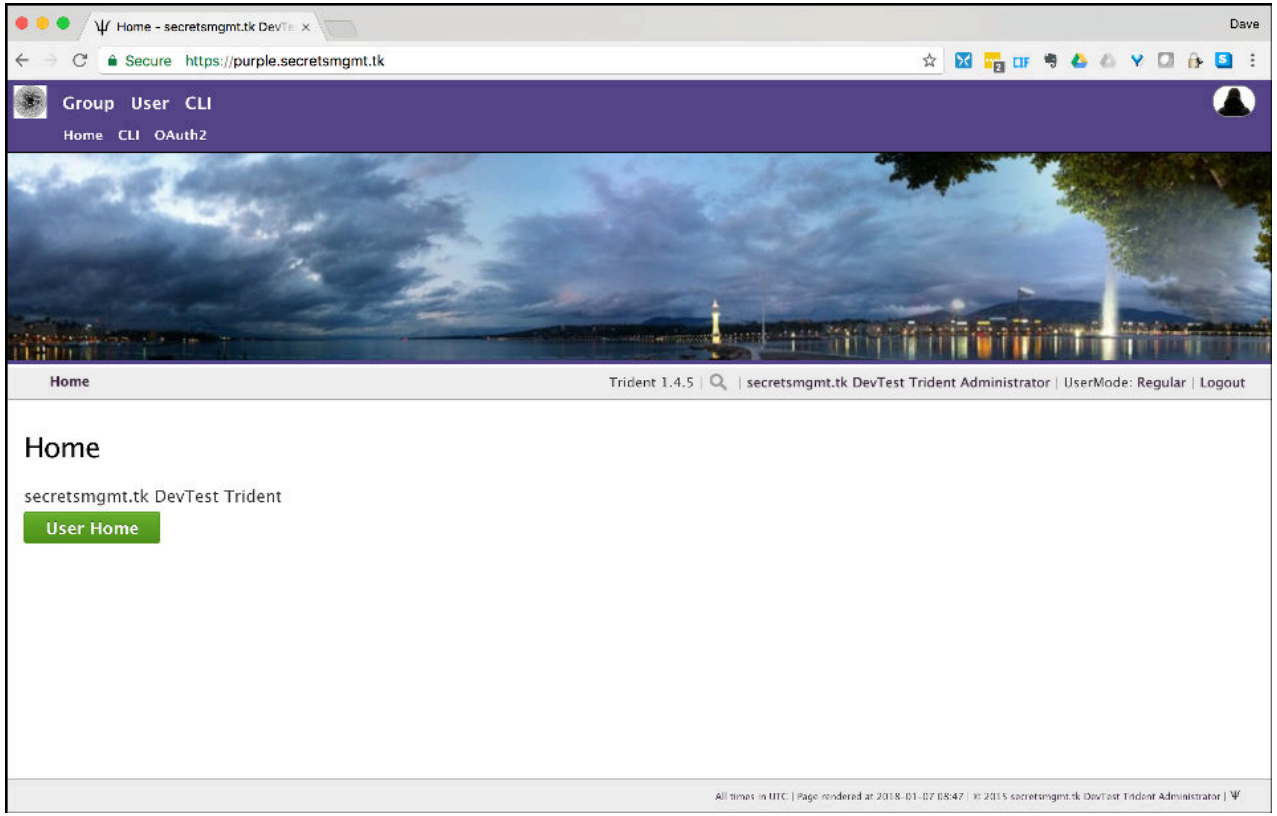
What is D2?
Technical Features

- 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

D2 Service Components

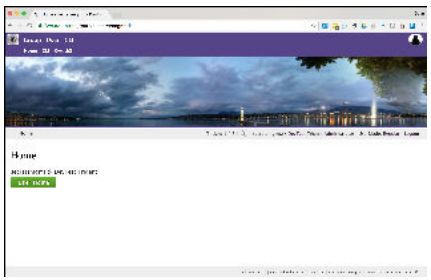
Trident Portal



Trident Portal

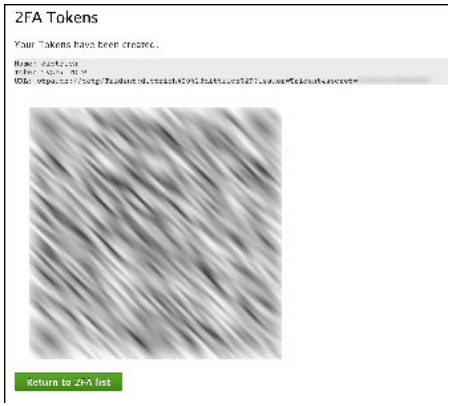
D2 Service Components

Trident Portal



https://trident.li/

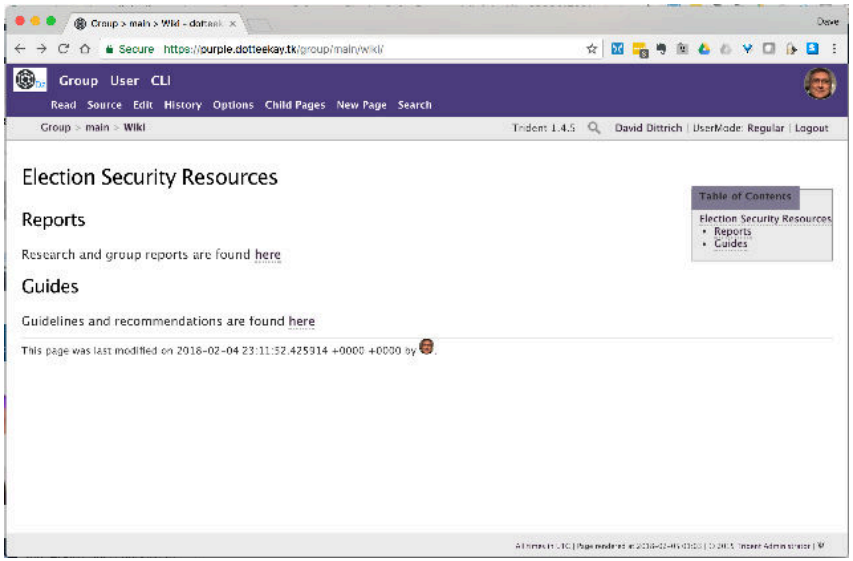
- Trust group management (nomination & vouching automation)
- PGP encrypted email lists, group keyring
- Secure wiki and file upload
- Second-factor authentication support



- Low cost to deploy and administer

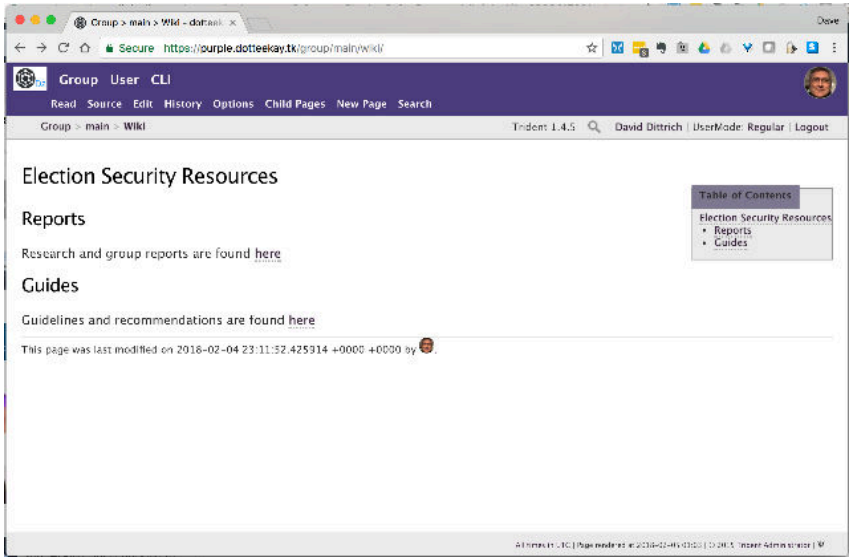
D2 Service Components

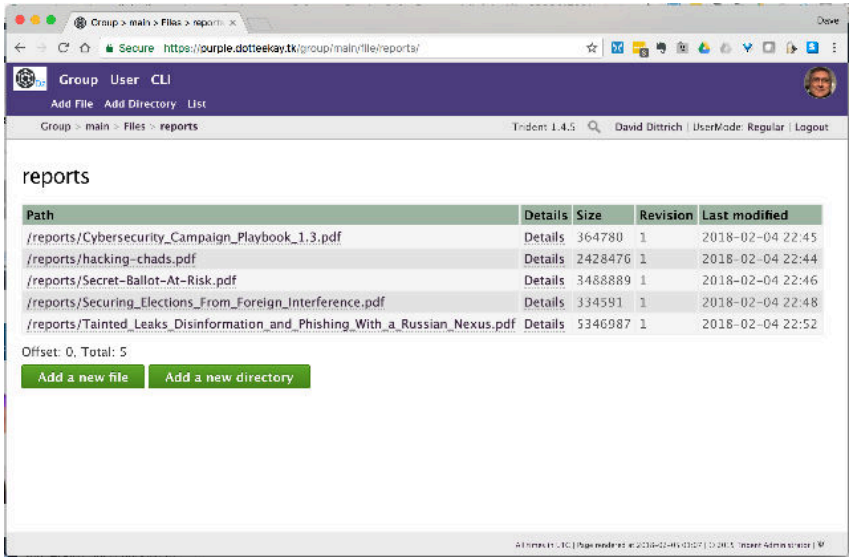
Trident Portal: Wiki and Files



D2 Service Components

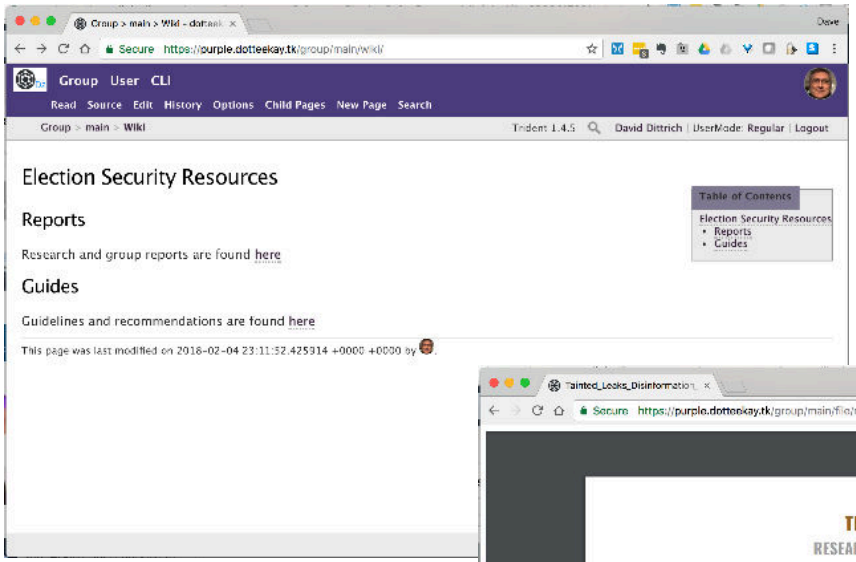
Trident Portal: Wiki and Files

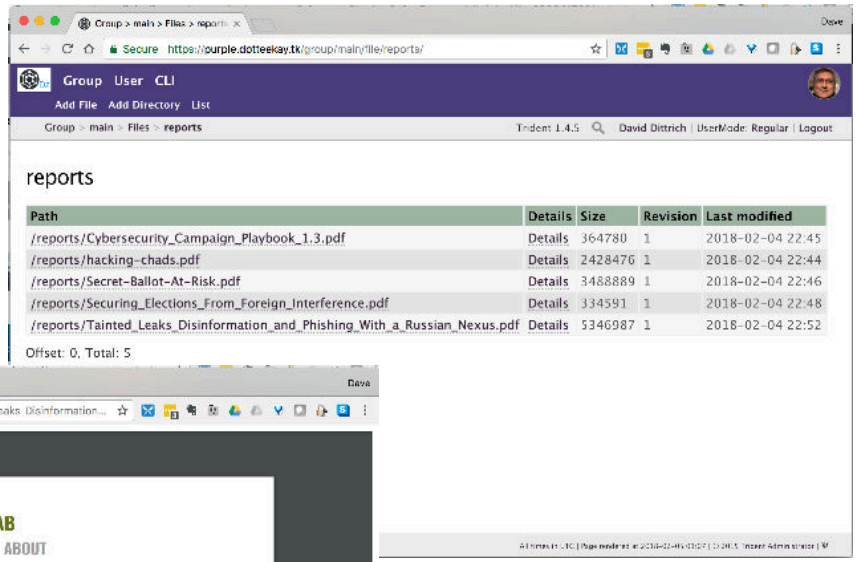


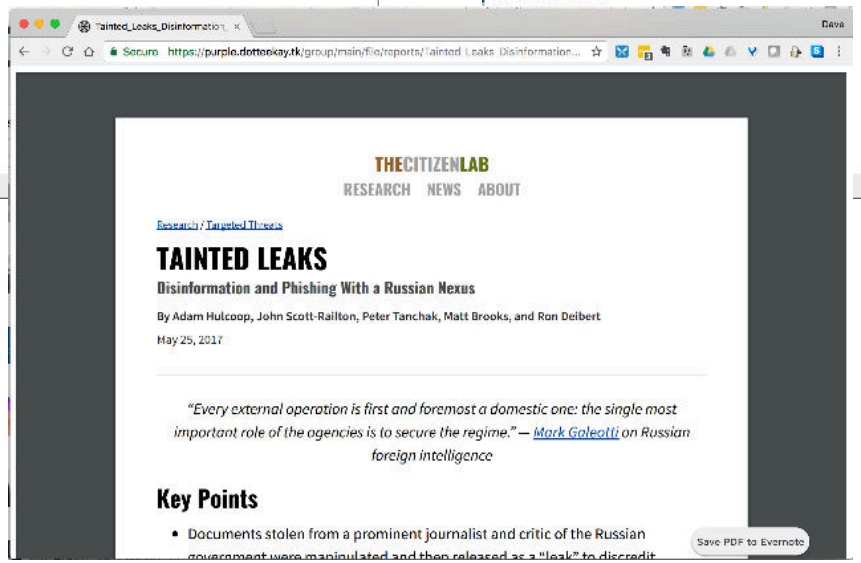


D2 Service Components

Trident Portal: Wiki and Files

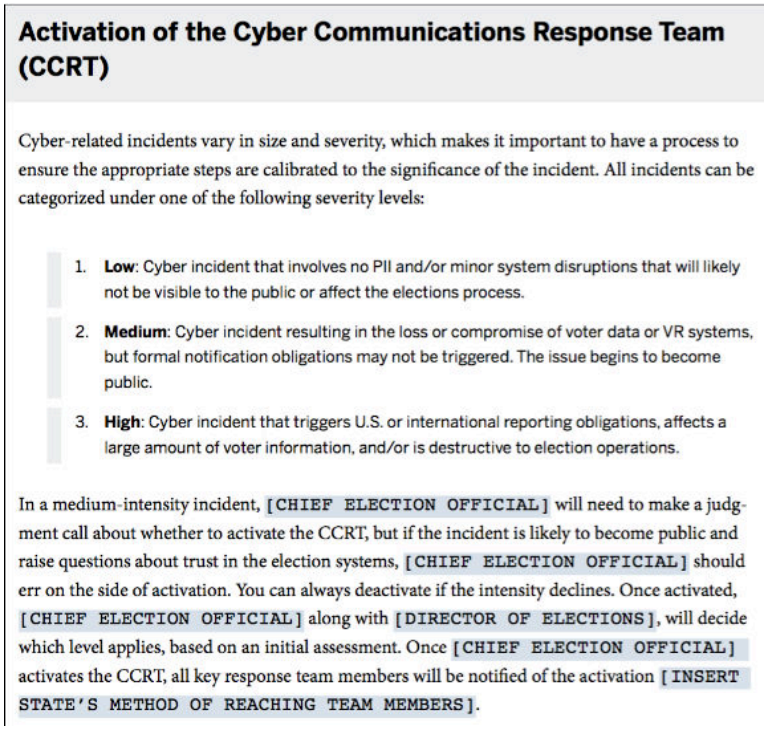






D2 Service Components

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.

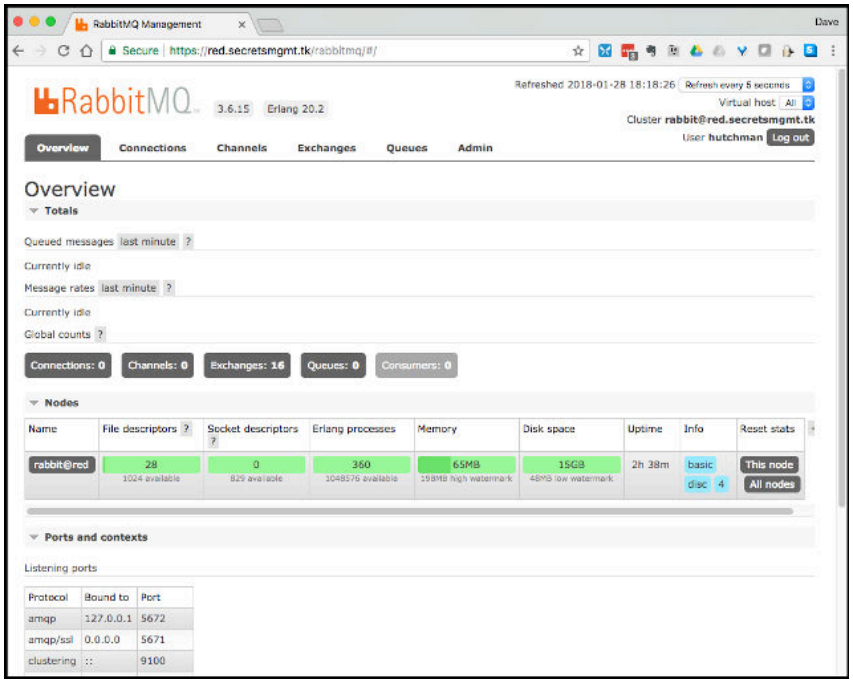
In a medium-intensity incident, `[CHIEF ELECTION OFFICIAL]` will need to make a judgment call about whether to activate the CCRT, but if the incident is likely to become public and raise questions about trust in the election systems, `[CHIEF ELECTION OFFICIAL]` should err on the side of activation. You 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

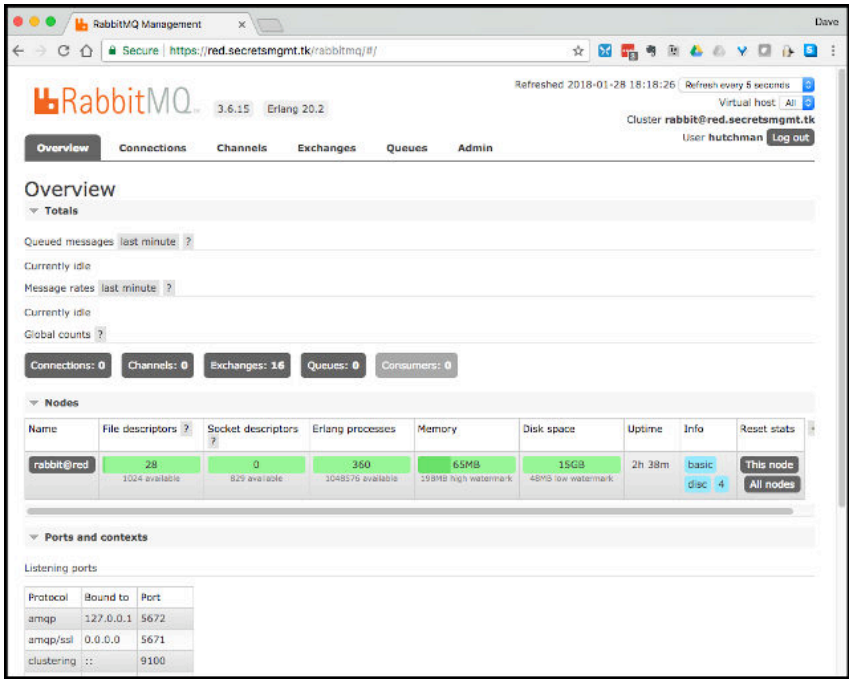
D2 Service Components

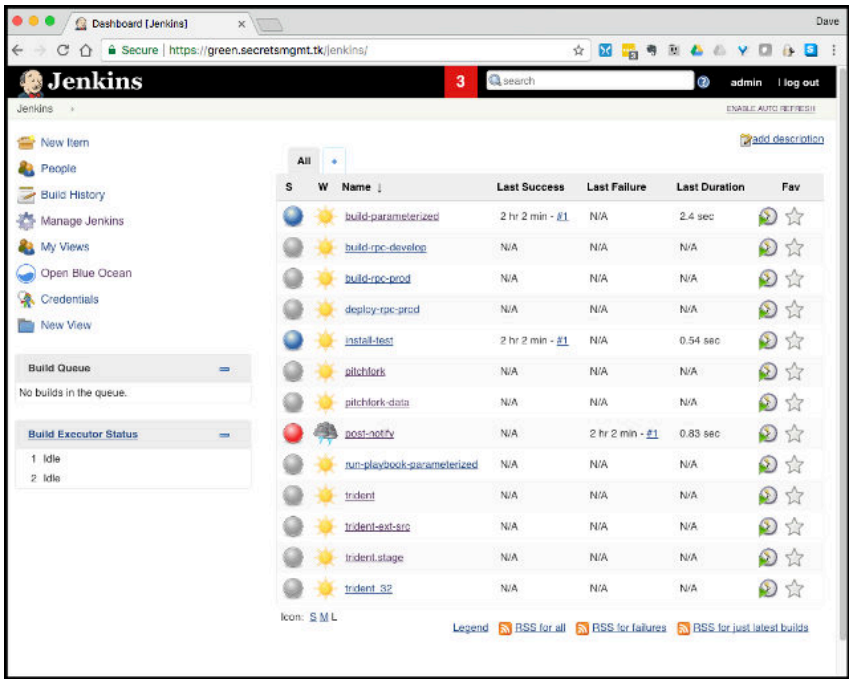
DevOps Services



D2 Service Components

DevOps Services





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 13, 2017 58.5K

Getty Images

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.

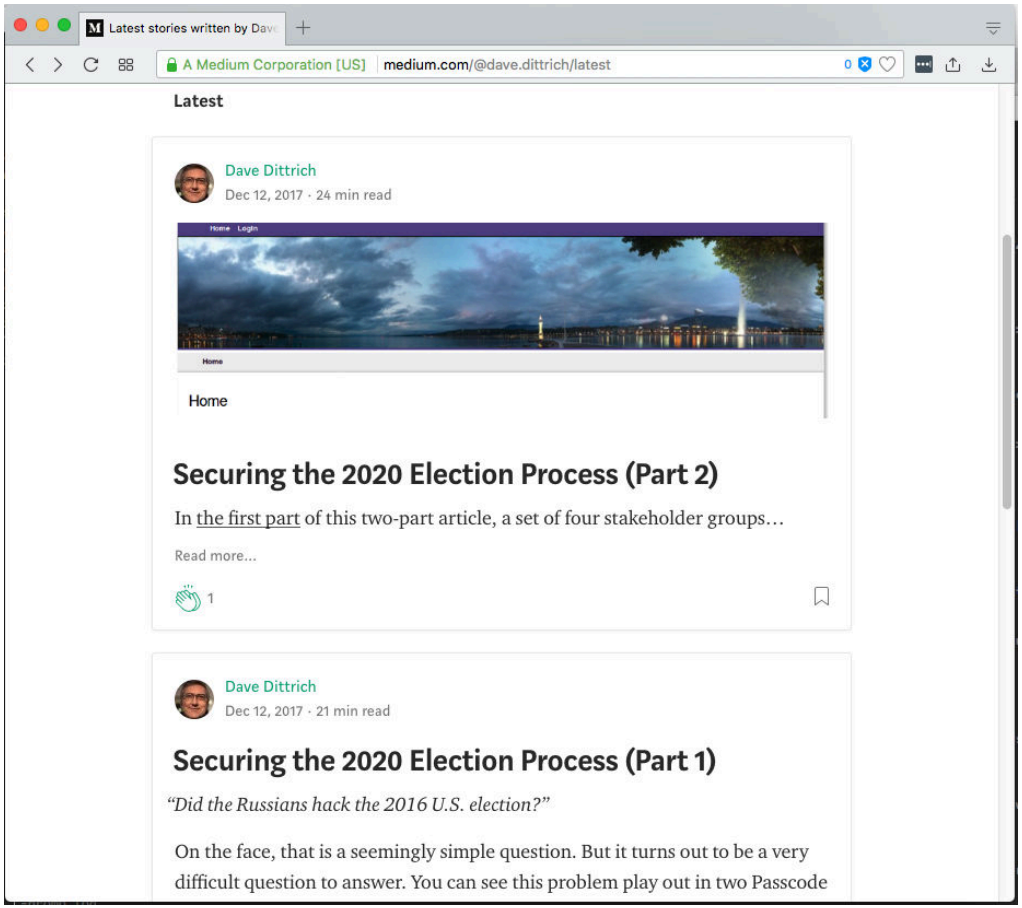
BY CHARLES P. PIERCE JUN 13, 2017 58.5K

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>

April 27, 2018
ISOI XX
v1.5.0

TLP:WHITE (+= megaphone)