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



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



Institute of Technology

Distributed Incident Management System (DIMS)





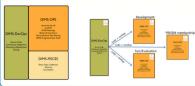
dittrich@u.washington.edu, linda.parsons@nextcentury.com

Summary

The Distributed Incident Management System (DMS) project is intended to take semi-automated sharing of structured intera information (MTHE) STS IN schemischy, building on the seconds of the Public Migraul Inflatanticus security predistorials known as Fideric and calls to the next level. DMS take solvantage of the open researge has architecture used predistorials known as Fideric and calls to the next level. DMS take solvantage of the open researge has architecture used predistorials have made to the second solvantage of the open researge has architecture used predistorials and take the second solvantage of the open researge has architecture and predistorials and another the instance, sevent history, and attactive context history) to support data sources in an architecture and predistorial and the second solvantage of the open research and a second predistorial solvantage and developed the second solvantage of the open research and a second predistorial solvantage and the second solvantage of the open research and a second predistorial solvantage and developed the second solvantage of the second solvantage of second predistorial solvantage and developed here that are solved down today to support analysis of second predistorial solvantage of the second solvantage of the second solvantage of the second solvantage of the solvantage and the second solvantage and the second solvantage of the second sol

System Architecture

The DMS project integrate over a dozen independent open source system components, some develoed by the DMS tana and many more by door open ouver projects into the functional us-by-more. DMS-De-De/Op, uses a continuous integration environment using Jenkins for othrave build and dedownent. Ansile for automated system comparation and othere installation, feffin forly eight systematic G source responsions, to obey and manage DMS-DPS and DMS-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.

(stangents)	And in case of some line in the	and the second se	in succession in the second se
		and the second sec	
		1 (1 (1 (1)))	
	11000 10		

Trust/Collaboration

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



Record Description of the Description for the International Constraints of the International Constr

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 Sleuthik forensics library. DIMS employs systematic and efficient whole disk acquisition, storage and search, enabling rapid response in malware identification.

Acknowledgments

ISBN in factor by the Department of Heresteed Society and economic HERESCO.13-C HOS DIES Crass Sectors: Devices BAD Society and An Taxonomic Ministeries • Ministeries DC • Department Host 2015



Outline



Introduction: the 2016 Election

- Who are the Stakeholders?
- What are the Threatened Targets?
- What is getting attention?



What is being done?

- ... to assure X?
- The Gap



- What is D2?
- Service Components



What is being done? Securing Operations with D2 Summary Stakeholders Targets Attention

Outline



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
- Securing Operations with D2What is D2?
 - Service Components



Stakeholders Targets Attention

Who are the Stakeholders?

Election Officials

Secretaries of State, County Elections Boards

he Electorate

The voting public (the key stakeholders) Political Campaigns 8 Candidates

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

ヘロト 人間 とくほ とくほう

102

Stakeholders Targets Attention

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

・ロト ・回 ト ・ヨト ・ ヨト

D2

Stakeholders Targets Attention

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

・ロト ・ 日 ・ ・ 日 ・ ・ 日 ・

102

Stakeholders Targets Attention

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

・ロン ・四 と ・ 回 と ・ 日 と

D2

Stakeholders Targets Attention

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

◆□▶ ◆圖▶ ◆臣▶ ◆臣▶ 三臣。

What is being done? Securing Operations with D2 Summary Stakeholders Targets Attention

Outline



- Introduction: the 2016 ElectionWho are the Stakeholders?
- What are the Threatened Targets?
- What is getting attention?
- 2) What is being done?
 - ... to assure X?
 - The Gap
- Securing Operations with D2What is D2?
 - Service Components



Stakeholders **Targets** Attention

Threatened Targets



Stakeholders **Targets** Attention

Threatened Targets

Integrity of voter		
perceptions Manipulation of the perceptions, emotions, and opinions of voters		



2

Stakeholders **Targets** Attention

Threatened Targets

Integrity of voter	Integrity of election results	
perceptions	Accurate	
Manipulation	recording and	
of the	tabulation of	
perceptions,	votes cast	
emotions, and		
opinions of		
voters		



2

Stakeholders **Targets** Attention

Threatened Targets

Integrity of voter	Integrity of election results	Availability of your ballot	
perceptions	Accurate	Ease of	
Manipulation	recording and	registering to	
of the	tabulation of	vote, staying on	
perceptions,	votes cast	voter roles,	
emotions, and		ability to sign	
opinions of		in and vote on	
voters		election day	



Э

Stakeholders **Targets** Attention

Threatened Targets

Integrity of voter perceptions	Integrity of election results Accurate	Availability of your ballot	Confidentiality of party com- munications
Manipulation of the perceptions,	recording and tabulation of votes cast	Ease of registering to vote, staying on voter roles,	Privacy of com- munications, internal
emotions, and opinions of voters		ability to sign in and vote on election day	documents, confidential data



æ

What is being done? Securing Operations with D2 Summary Stakeholders Targets Attention

Outline



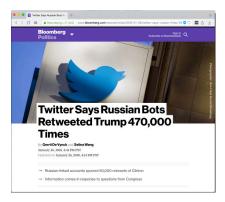
Introduction: the 2016 Election

- Who are the Stakeholders?
- What are the Threatened Targets?
- What is getting attention?
- 2) What is being done?
 - ... to assure X?
 - The Gap
- Securing Operations with D2
 What is D2?
 - Service Components



What is being done? Securing Operations with D2 Summary Stakeholders Targets Attention

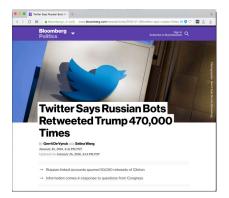
Attention!





What is being done? Securing Operations with D2 Summary Stakeholders Targets Attention

Attention!





・ロン ・回 と ・ 回 と ・



Э

Introduction: the 2016 Election What is being done?

Stakeholder Targets Attention

Attention!

Integrity of voter	Integrity of election results		Confidentiality of party com-
perceptions	Lots of	Less attention	munications
Lots of	attention		Less attention
attention			



2

・ロット 小型マネ 山マ

... **to assure X**? The Gap

Outline



- 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
- Securing Operations with D2
 What is D2?
 - Service Components



... to assure X? The Gap

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 <□ → 4億 → 4億 → 4億 → 4章 → 章



... to assure X? The Gap

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 X? The Gap

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 X? The Gap

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 X? The Gap

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 X? The Gap

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

イロト イヨト イヨト イヨト



.. to assure X? The Gap

Letter from Senator Ron Wyden To: The White House

FONWOOP			
	C.		
			CONFILM ON BARRY
NAMES OF GROOM COST	ETTE OK	United States Senate	CONFIL OFFICIAL SOLAR REPORT
		second and a second second	AND COMPTLY PROPERTY.
D CRASH KINES OF STR	BILLEYC .	VANIENGTON, DC 20510-5705	
STATES OF A DESCRIPTION		December 12, 2017	
		December 12, 2011	
Assistant of The White 1600 Percent		r National Security Affairs	
Dear Geta	and McMaster.		
		immediate action to socure federal elections	from hacking by foreign
Sourcements.	nb.		
eybersecu seriously, governme election of	rity weaknesses in others are serious at cyberatheks. A dorsecurity to the	ent. Moving Reveal, firetign governments a considering industructure. While some str by lagging behind and remain workfully wile a such, the fideral government must take a e states is irresponsible and a total abdicatic is matters of rational security.	stos have taken the threats senable to foreign ction: leaving federal
electronic unbooded.	voting machines Fourtoen states a to the machines" the subsequently yote tails. Moreo	complained for decades obeat the risks oso and the need for paper andit trails. Their we fill use Direct Recentling Electronic voting lightal memory. These voting machines de- andited if voting officials have any reason ver, according to the Jves Tork Theore, Geo ting machines manion Windows 2000; per	mings have largely gone machines that record votes not produce a paper trail, to doubt the validity of the rgis conducted
and canno electronic November on machin	es running Winds	two XP. These two openating systems are d ates, which leaves them especially volveral	ecades old and no longer
and canno electronic November or machin receive cri At a Senat governme foreign all in direction complex f	es rucning Wind fical security upd e bearing in Octo at is not doing en versaties. When a s, Athomey Gene had for most of un	res XP. These two openting systems are drawn, which leaves them repecially vulneral ber, Attenney General Jeff Sessions conset ough to prevent future detection inserferment ough to prevent future detection inserferment all Sessions stated that "we're rest," and the we're net able to fully graup the sechnical.	ecades old and no longer fit to cybernitacks. ed that the U.S. by Russia and other action to provent modelling 17the matter is so langers that are out there."
and canno electronic November on cauchin receive cri- At a Senat governme foreign ad in election complete Attorney G	es running Windi fical security upd e bearing in Octo nt is not doing my versaties. When a s, Adomey Gene hat for most of un letterni Sensions?	we XP. These two operating systems are di- ators, which leaves them especially volcentl ber, Attorney General Jeff Sessions concert sugh to personn future election interference shell if the government is taking adequate a all Sension stated that "we're next" and the attorney stated that "we're next".	ecades old and no longer fit to cybenstacks. ed that the U.S. by Rounia and other action to provent meddling t "the matter is so langers that are out there." is not taking this issue
and caining electronic November or cashin receive cri At a Senai governme foreign al in election camplac d Attemps o particulty o	es reaning Winds feat security upd e bearing in Octo it is not doing en vorsaties. When a s, Advency Gene lat for most of au beend Servismi mough or dollcat	work 20: Date two opening systems and on any Addre Rover Manne opecially vulneral large, Addresserv Manne opecially vulneral ough to prevent flates clacks in instrument and its of the openiments in solaring adquares and for the outward on the solaring adquares the foreing systems flate the Addressification for net address to adjugand the address instrument systems and the Addressification for and address and the Addressification for and address and the Addressification for address and the Addressification for addressification and the Addressification and	ecades oil and no longer is to cyberntacks. I that the U.S. ty Xunit and other cuber to process modeling of the matter is so langers that are out here." is not taking this issue at change.
and calance electronic November or canchia receive cri Ar a Senar governme fereign al in electron complete d Attempte d actionally o	es receitag Wield fical security upd e bearing in Octo nt is net doing en a, Adomey Gene hat for most of us levent Servium' mough or dedicat	work 20: Done two openning systems and other starts, which known then neperchildy values bee, Ataeney General Jeff Sensions concell ogds to prevent flates classics interference on devices and the divertise that the divertise the Sension well and the divertise that the divertise interface starts and the divertise starts and the starts and the starts and the starts and the starts and the starts and the starts and the starts and the starts and the starts and the starts and the starts and the starts and the starts and the starts and the starts and the starts and the starts and the st	ecades oil and no lenger in to systematics, oil that the U.S. by Tousia and other by Tousia and other of the matter is so langers that are out here." is not taking this issue art change.
and cointo electronic November or machin receive cel Al a Senat generation foreign al in electron complex of Atlement complex	es recentage Wiedd foart secentry upd e bearing in Oceto et visynaaties. When a n, Adormey Gener has for most of us beerend Secritors' mough or dedicant	work 20: Date two opening systems and on any Addre Rover Manne opecially vulneral large, Addresserv Manne opecially vulneral ough to prevent flates clacks in instrument and its of the openiments in solaring adquares and for the outward on the solaring adquares the foreing systems flate the Addressification for net address to adjugand the address instrument systems and the Addressification for and address and the Addressification for and address and the Addressification for address and the Addressification for addressification and the Addressification and	ecades of and no longer is to cyclematical of that the U.S. by Ramin and other while matter is so "The matter is so that any source in adding the matter is source in the is not taking bits issue at change.

- 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
- Direct US Secret Service to expand Presidential candidate security to include cybersecurity assistance



.. to assure X? The Gap

Letter from Senator Ron Wyden To: The White House



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

イロト イロト イヨト イヨト

 Direct US Secret Service to expand Presidential candidate security to include cybersecurity assistance



... to assure X? The Gap

Letter from Senator Ron Wyden To: The White House

	N.		CONSTITUES.
			CONVERTING ON INCOME.
THE REAL PROPERTY OF	NUMBER OF COLUMN	United States Senat	COMPTEE OF END OF A SECTION AND AND AND AND AND AND AND AND AND AN
		WASHINGTON, DC 26510-5705	ARE COMPTE IN YOURSE
DI CRAZIA RINITI OFFI	E BULLENC		
ite dis land		December 12, 2017	
The Hern	wable Lt. Gen. H.F.	R. McMann, Jr.	
Assisted The Whit		e National Security Affairs	
	arybaria Ave., N	w.	
Washingt	ice, D.C. 20500		
Dear Ger	end McMaster:		
I write to		immediate action to socure federal elect	ions from hacking by foreign
up call to cybersect seriously, governmo election o governmo	the U.S. griverness arity weaknesses in others are serious ant cyberatacks. A phenecurity to the rat's primary role i	bassiss government during the 2016 of one dowing forward, foreign governme or or election informerance. While som by lagging behind and remain workfully a such, the followal government must the status is invesponsible and a total abdit is mattern of national security.	uts will continue to exploit a states have taken for threats vulnerable to foreign se action: leaving federal ation of the foderal
electronic	voting machines a Fourteen states at to the machines" of	complained for decades about the risks and the noted for paper and/i trulks. Their BL use Direct Recording Electronic vot fightal memory. These voting machines andhod If voting officials have any rea were according to the <i>New York Tanes</i> .	rwarnings have largely gone ing machines that record votas do not produce a paper trail, on to doubt the validity of the jeergin conducted
directly in and camp electronic Novembe on machi	vote taily. Moreo- r's elections on vo res running Winds	ver, accorecing to the view stave staves, ting machines running Windows 2000; nvo XP. These two operating systems a atca, which leaves them especially values	re decades old and no longer
directly is and come electracia Novembe on machin necesive ci At a Semi governove foreign a in electric complete Attaches	vote taily. Moreov r's elections on vo- ses receivag Winde rifeal security updi- de bearing in Octol are is not doing ene hversaties. When a m, Adomey Gener that for most of us General Semismi	ting machines naming Windows 2000 nwo XP. Those two openating systems a max, which haves them expectably with her, Attenney General Jeff Semions on raph to pervant thates election insertirs siked if the government is taking along all Semions stated that "we're rest," are we're not able to fully graup the techni- testimery wagness that the Administra testimery wagness that the Administra	in decades old and no lenger enable to cyberstlacks. ceded that the U.S. no by Xhundia and other ne action to provent meddling that "the matter is so cal dangen that are out there," ion is not taking this issue
directly is and come electracia Novembe on machin necesive ci At a Semi governove foreign a in electric complete Attaches	vote taily. Moreov r's elections on vo- ses receivag Winde rifeal security updi- de bearing in Octol are is not doing ene hversaties. When a m, Adomey Gener that for most of us General Semismi	ting machines ranning Windows 2000, res XP. These two openting systems a atta, which lowers them especially vul- ber, Attorney General Jeff Sessions on cogits to prevent future elacidon interfirm added if the government is aking adequa al Semicron stated that "we're rest." me wi're net able to fully graup the sochal	in decades old and no lenger enable to cyberstlacks. ceded that the U.S. no by Xhundia and other ne action to provent meddling that "the matter is so cal dangen that are out there," ion is not taking this issue
directly is and come electracia Novembe on machin necesive ci At a Semi governov foreign a in electric complete Attachesey	vote taily. Moreov r's elections on vo- ses receivag Winde rifeal security updi- de bearing in Octol are is not doing ene hversaties. When a m, Adomey Gener that for most of us General Semismi	ting machines naming Windows 2000 nwo XP. Those two openating systems a max, which haves them expectably with her, Attenney General Jeff Semions on raph to pervant thates election insertirs siked if the government is taking along all Semions stated that "we're rest," are we're not able to fully graup the techni- testimery wagness that the Administra testimery wagness that the Administra	in decades old and no lenger enable to cyberstlacks. ceded that the U.S. no by Xhundia and other ne action to provent meddling that "the matter is so cal dangen that are out there," ion is not taking this issue

- 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

・ロト ・回ト ・ヨト ・ヨト

4. Direct US Secret Service to expand Presidential candidate security to include cybersecurity assistance



... to assure X? The Gap

Letter from Senator Ron Wyden To: The White House

	N.		CONSTITUES.
			CONVERTING ON INCOME.
THE REAL PROPERTY OF	NUMBER OF COLUMN	United States Senat	COMPTEE OF END OF A SECTION AND AND AND AND AND AND AND AND AND AN
		WASHINGTON, DC 26510-5705	ARE COMPTE IN YOURSE
DI CRAZIA RINITI OFFI	E BULLENC		
ite dis land		December 12, 2017	
The Hern	wable Lt. Gen. H.F.	R. McMaurer, Jr.	
Assisted The Whit		e National Security Affairs	
	arybaria Ave., N	w.	
Washingt	ice, D.C. 20500		
Dear Ger	end McMaster:		
I write to		immediate action to socure federal elect	ions from hacking by foreign
up call to cybersect seriously, governmo election o governmo	the U.S. griverness arity weaknesses in others are serious ant cyberatacks. A phenecurity to the rat's primary role i	bassiss government during the 2016 of one dowing forward, foreign governme or or election inducementers. While sees by lagging behind and remain workfully a such, the followal government must the status is investorishin and a total abdit is mattern of national security.	uts will continue to exploit a states have taken for threats vulnerable to foreign se action: leaving federal ation of the foderal
electronic	voting machines a Fourteen states at to the machines" of	complained for decades about the risks and the noted for paper and/i trulks. Their BL use Direct Recording Electronic vot fightal memory. These voting machines andhod If voting officials have any rea were according to the <i>New York Tanes</i> .	rwarnings have largely gone ing machines that record votas do not produce a paper trail, on to doubt the validity of the jeergin conducted
directly in and camp electronic Novembe on machi	vote taily. Moreo- r's elections on vo res running Winds	ver, accoreing to the view stave stave, ting machines running Windows 2000; nvo XP. These two operating systems a atca, which leaves them especially values	re decades old and no longer
directly is and come electracia Novembe on machin necesive ci At a Semi governov foreign a in electric complete Attachesey	vote taily. Moreov r's elections on vo- ses receivag Winde rifeal security updi- de bearing in Octol are is not doing ene hversaties. When a m, Adomey Gener that for most of us General Semismi	ting machines naming Windows 2000 nwo XP. Those two openating systems a max, which haves them expectably with her, Attenney General Jeff Semions on raph to pervant thates election insertirs siked if the government is taking along all Semions stated that "we're rest," are we're not able to fully graup the techni- testimery wagness that the Administra testimery wagness that the Administra	in decades old and no lenger enable to cyberstlacks. ceded that the U.S. no by Xhundia and other ne action to provent meddling that "the matter is so cal dangen that are out there," ion is not taking this issue
directly is and come electracia Novembe on machin necesive ci At a Semi governov foreign a in electric complete Attachesey	vote taily. Moreov r's elections on vo- ses receivag Winde rifeal security updi- de bearing in Octol are is not doing ene hversaties. When a m, Adomey Gener that for most of us General Semismi	ting machines ranning Windows 2000, www.XP. Those two openting systems a atos, which lowers them especially vul- ber, Attorney General Jeff Sessions on cogits to prevent future elacidon interfirm added if the government is subling adequa al Semicien stated that "we're rest." me wi're net able to fully graup the suchal	in decades old and no lenger enable to cyberstlacks. ceded that the U.S. no by Xhundia and other ne action to provent meddling that "the matter is so cal dangen that are out there," ion is not taking this issue
directly is and come electracia Novembe on machin necesive ci At a Semi governov foreign a in electric complete Attachesey	vote taily. Moreov r's elections on vo- ses receivag Winde rifeal security updi- de bearing in Octol are is not doing ene hversaties. When a m, Adomey Gener that for most of us General Semismi	ting machines naming Windows 2000 nwo XP. Those two openating systems a max, which haves them expectably with her, Attenney General Jeff Semions on raph to pervant thates election insertirs siked if the government is taking along all Semions stated that "we're rest," are we're not able to fully graup the techni- testimery wagness that the Administra testimery wagness that the Administra	in decades old and no lenger enable to cyberstlacks. ceded that the U.S. no by Xhundia and other ne action to provent meddling that "the matter is so cal dangen that are out there," ion is not taking this issue

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



... to assure X? The Gap

Letter from Senator Ron Wyden To: The White House

	N.		CONSTITUES.
			CONVERTING ON INCOME.
THE REAL PROPERTY OF	NUMBER OF COLUMN	United States Senat	COMPTEE OF END OF A SECTION AND AND AND AND AND AND AND AND AND AN
		WASHINGTON, DC 26510-5705	ARE COMPTE IN YOURSE
DI CRAZIA RINITI OFFI	EBULIERO		
ite dis land		December 12, 2017	
The Hern	wable Lt. Gen. H.F.	R. McMaurer, Jr.	
Assisted The Whit		e National Security Affairs	
	arybaria Ave., N	w.	
Washingt	ice, D.C. 20500		
Dear Ger	end McMaster:		
I write to		immediate action to socure federal elect	ions from hacking by foreign
up call to cybersect seriously, governmo election o governmo	the U.S. griverness arity weaknesses in others are serious ant cyberatacks. A phenecurity to the rat's primary role i	bassiss government during the 2016 of one dowing forward, foreign governme or or election inducementers. While sees by lagging behind and remain workfully a such, the followal government must the status is investorishin and a total abdit is mattern of national security.	uts will continue to exploit a states have taken for threats vulnerable to foreign se action: leaving federal ation of the foderal
electronic	voting machines a Fourteen states at to the machines" of	complained for decades about the risks and the noted for paper and/i trulks. Their BL use Direct Recording Electronic vot fightal memory. These voting machines andhod If voting officials have any rea were according to the <i>New York Tanes</i> .	rwarnings have largely gone ing machines that record votas do not produce a paper trail, on to doubt the validity of the jeergin conducted
directly in and camp electronic Novembe on machi	vote taily. Moreo- r's elections on vo res running Winds	ver, accoreing to the view stave stave, ting machines running Windows 2000; nvo XP. These two operating systems a atca, which leaves them especially values	re decades old and no longer
directly is and come electracia Novembe on machin necesive ci At a Semi governov foreign a in electric complete Attachesey	vote taily. Moreov r's elections on vo- ses receivag Winde rifeal security updi- de bearing in Octol are is not doing ene hversaties. When a m, Adomey Gener hat for most of us General Semismi	ting machines naming Windows 2000 nwo XP. Those two openating systems a max, which haves them expectably with her, Attenney General Jeff Semions on raph to pervant thates election insertirs siked if the government is taking along all Semions stated that "we're rest," are we're not able to fully graup the techni- testimery wagness that the Administra testimery wagness that the Administra	in decades old and no lenger enable to cyberstlacks. ceded that the U.S. no by Xhundia and other ne action to provent meddling that "the matter is so cal dangen that are out there," ion is not taking this issue
directly is and come electracia Novembe on machin necesive ci At a Semi governov foreign a in electric complete Attachesey	vote taily. Moreov r's elections on vo- ses receivag Winde rifeal security updi- de bearing in Octol are is not doing ene hversaties. When a m, Adomey Gener hat for most of us General Semismi	ting machines ranning Windows 2000, res XP. These two openting systems a atta, which lowers them especially vul- ber, Attorney General Jeff Sessions on cogits to prevent future elacidon interfirm added if the government is aking adequa al Semicron stated that "we're rest." me wi're net able to fully graup the sochal	in decades old and no lenger enable to cyberstlacks. ceded that the U.S. no by Xhundia and other ne action to provent meddling that "the matter is so cal dangen that are out there," ion is not taking this issue
directly is and come electracia Novembe on machin necesive ci At a Semi governov foreign a in electric complete Attachesey	vote taily. Moreov r's elections on vo- ses receivag Winde rifeal security updi- de bearing in Octol are is not doing ene hversaties. When a m, Adomey Gener that for most of us General Semismi	ting machines naming Windows 2000 nwo XP. Those two openating systems a max, which haves them expectably with her, Attenney General Jeff Semions on raph to pervant thates election insertirs siked if the government is taking along all Semions stated that "we're rest," are we're not able to fully graup the techni- testimery wagness that the Administra testimery wagness that the Administra	in decades old and no lenger enable to cyberstlacks. ceded that the U.S. no by Xhundia and other ne action to provent meddling that "the matter is so cal dangen that are out there," ion is not taking this issue

- 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

イロト イヨト イヨト イヨト

4. Direct US Secret Service to expand Presidential candidate security to include cybersecurity assistance



... to assure X? The Gap

What is being done so far? ... to assure integrity of election results.

6	matt blaze Virialization I get asked for advice on the best way to be involved in improving election security. Best I've got is: GET TO KNOW YOUR LOCAL ELECTION OFFICIALS (becoming a pollworker is a great way to do that). Relationships between clueful tech/security people & local officials are critical.
	18 Retweets 32 Likes 🙀 💿 🎯 🚱 🚱 🚱 🖗
6	Q 3 1.18 ♥ 32 ♥ matt blaze ♥ mattblaze 30 ↓ Local officials are critical to EVERYTHING about election security. They run (at least some) leverage with vendors. Make friends with them. Learn their concerns. Be a helpful resource.



1

イロト イヨト イヨト イヨト

... to assure X? The Gap

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 "<u>ALL-MAIL ELECTIONS (AKA</u> 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"



... to assure X? The Gap

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 "<u>ALL-MAIL ELECTIONS (AKA</u> 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"



... to assure X? The Gap

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 "<u>ALL-MAIL ELECTIONS (AKA</u> 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"



... to assure X? The Gap

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 "<u>ALL-MAIL ELECTIONS (AKA</u> 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"



... to assure X? The Gap

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 "<u>ALL-MAIL ELECTIONS (AKA</u> 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"



・ロト ・回ト ・ヨト ・ヨト

... to assure X? The Gap

What is being done so far? ... to assure integrity of election results.

Belfer Center for Science and International Affairs, Harvard Kennedy School

- For Campaigns
 - <u>"Hacking Chads: The Motivations, Threats, and Effects of Electoral</u> Insecurity"
- For State and Local Goververnment Officials
 - "The State and Local Election Cybersecurity Playbook"
 - "Election Cyber Incident Communications Coordination Guide"
 - "Election Cyber Incident Communications Plan Template"



・ロト ・回ト ・ヨト ・ヨト

... to assure X? The Gap

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
- <u>"The New Pennsylvania Congressional Map, District</u> <u>by District</u>," 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



... to assure X? The Gap

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
- <u>"The New Pennsylvania Congressional Map, District</u> <u>by District</u>," by Nate Cohn, Matthew Bloch and Kevin Quealy, New York Times, February 19, 2018
- Eric Holder and the National Democratic Redistricting Committee
- Brennan Center "<u>Securing Elections From Foreign</u> <u>Interference</u>" also covers Voter Registration Databases
- Reality Winner going on trial in March for leaking NSA report



... to assure X? The Gap

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
- <u>"The New Pennsylvania Congressional Map, District</u> <u>by District</u>," by Nate Cohn, Matthew Bloch and Kevin Quealy, New York Times, February 19, 2018
- Eric Holder and the National Democratic Redistricting Committee
- Brennan Center "<u>Securing Elections From Foreign</u> <u>Interference</u>" also covers Voter Registration Databases
- Reality Winner going on trial in March for leaking NSA report



... <mark>to assure X</mark>? The Gap

What is being done so far? "Open Source" Groups





... to assure X? The Gap

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.



... to assure X? The Gap

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.



... to assure X? The Gap

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.



... to assure X? The Gap

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.



... to assure X? The Gap

What is being done so far?

... to ensure confidentiality of party communications.





Electronic Frontier Foundation's <u>Surveillance Self</u> 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 <u>Belfer Center</u> "<u>Cybersecurity</u> Campaign Playbook"
- Tech Solidarity <u>"Security Guidelines for Congressional</u> Campaigns"



... to assure X? The Gap

What is being done so far?

... to ensure confidentiality of party communications.





- Electronic Frontier Foundation's <u>Surveillance Self</u> 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 <u>Belfer Center</u> "<u>Cybersecurity</u> <u>Campaign Playbook</u>"
- Tech Solidarity <u>"Security Guidelines for Congressional</u> Campaigns"



... to assure X? The Gap

What is being done so far?

... to ensure confidentiality of party communications.





 Electronic Frontier Foundation's <u>Surveillance Self</u> 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 <u>Belfer Center</u> <u>"Cybersecurity</u> Campaign Playbook"
- Tech Solidarity "Security Guidelines for Congressional Campaigns"



.. **to assure X**? The Gap

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

イロト イヨト イヨト



.. **to assure X**? The Gap

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

ヘロト ヘヨト ヘヨト ヘヨ



.. **to assure X**? The Gap

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

ヘロト ヘヨト ヘヨト ヘヨ



.. **to assure X**? The Gap

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

< □ > < □ > < □ > < □ >



What is being done?

to assure X?

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. Lise 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 M-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 36-17)

4. Create strong, long passwords:

For your passwords, create somethingssallyLongLIKETHISETHING, 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 LOIS OF SymBOIS. A password manager can help, too, (scopage D)

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.

"Cybersecurity Campaign Playbook"

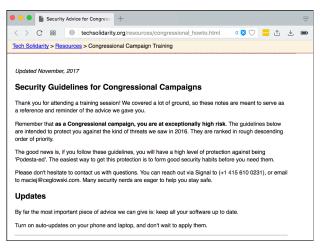
- 1. Take this seriously
- Use commercial cloud services
- 3. Use Two-Factor Authentication

- 4. Create strong passwords
- 5. Have a plan and be ready



... to assure X? The Gap

Tech Solidarity Congressional Campaign Training





... to assure X? The Gap

Outline



- 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
- Securing Operations with D2
 What is D2?
 - Service Components



... to assure X? The Gap

The Gap



Michael McFaul 51.7K Tweets

13 Michael McFaul Retweeted



Michael McFaul @ @Mc... · 3d ~ Thanks @KatyTurNBC for giving me the time on your show to address 4 (not just 1) kinds of policy responses to the Russian attack in 2016: (1) attribution, (2) resilience, (3) combatting propaganda, and (4) deterrence. So far, @realDonaldTrump doing very little on any of them.

Q 29 1,119 1

- Some talk of *what to do*
- Less talk about technology enabling how to do it

イロト イヨト イヨト イヨト



... to assure X? The Gap

The Gap



Michael McFaul 51.7K Tweets

13 Michael McFaul Retweeted



Michael McFaul @ @Mc... · 3d ~ Thanks @KatyTurNBC for giving me the time on your show to address 4 (not just 1) kinds of policy responses to the Russian attack in 2016: (1) attribution, (2) resilience, (3) combatting propaganda, and (4) deterrence. So far, @realDonaldTrump doing very little on any of them.

Q 29 1,119 1

• Some talk of what to do

 Less talk about technology enabling how to do it

イロト イヨト イヨト イヨト



... to assure X? The Gap

The Gap



Michael McFaul Retweeted Michael McFaul @ @Mc... · 3d Thanks @KatyTurNBC for giving me the time on your show to address 4 (not just 1) kinds of policy responses to the Russian attack in 2016: (1) attribution, (2) resilience, (3) combatting propaganda, and (4) deterrence. So far, @realDonaldTrump doing very little on any of them.

Michael McFaul 51.7K Tweets

- Some talk of what to do
- Less talk about technology enabling how to do it

イロト イヨト イヨト イヨト



... to assure X? The Gap

The Gap



t Michael McFaul Retweeted Michael McFaul ♥ @Mc... · 3d → Thanks @KatyTurNBC for giving

Michael McFaul 51.7K Tweets

me the time on your show to address 4 (not just 1) kinds of policy responses to the Russian attack in 2016: (1) attribution, (2) resilience, (3) combatting propaganda, and (4) deterrence. So far, @realDonaldTrump doing very little on any of them.

- Some talk of what to do
- Less talk about technology enabling how to do it

A 3 3

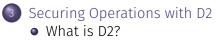


What is D2? What can it do?

Outline



- 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



Service Components



What is D2? What can it do?

What is D2?



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

What is D2? What can it do?

What is D2?



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

What is D2? What can it do?

What is D2?



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

What is D2? What can it do?

What is D2?



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



What is D2? What can it do?

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? What can it do?

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? What can it do?



- 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? What can it do?

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? What can it do?

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? What can it do?

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

A = A = A = A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A



What is D2? What can it do?

Outline



- 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

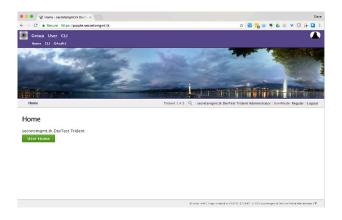


Service Components



What is D2? What can it do?

D2 Service Components Trident Portal







What is D2? What can it do?

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/





What is D2? What can it do?

D2 Service Components Trident Portal

Statistics Private	2.4
A COLUMN TWO IN COMPANY	• • • • • • • • • • • • • • • • • • •
A Description (10)	•
internet and	and a local second different forest
	Plan 1970, native provided, New Mercure & Galebraic Law
New	
LN HORE	

Trust group management (nomination & vouching automation)

• PGP encrypted email lists, group keyring

- Secure wiki and file upload
- Second-factor authentication support

https://trident.li/



・ロト ・回ト ・ヨト ・ヨト



What is D2? What can it do?

D2 Service Components Trident Portal

ALC: Lines of the	1.0
A CONTRACTOR OF A DESCRIPTION OF A DESCRIPANTE A DESCRIPANTE A DESCRIPANTE A DESCRIPTION OF A DESCRIPTION OF	• • • • • • • • • • • • • • • • • • •
And Description and	•
	AND STREET
Internet 2	
8.1	Plan 1973, many year to full from standards in Saladhada Kaan
None.	
ACCOUNTS OF ALL PARTY	
100.000	

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

https://trident.li/



・ロト ・回ト ・ヨト ・ヨト



What is D2? What can it do?

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



・ロト ・回ト ・ヨト ・ヨト

• Low cost to deploy and administer



What is D2? What can it do?

D2 Service Components Trident Portal

The Advances of the	10
	1 8 8 4 8 6 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
And Description of the	•
Con Care -	AND ADDRESS OF THE OWNER
Internet and	
No.	Part (17), concepted, for details a bibliote con-
NO RECEIPTION OF AN ADDRESS	

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



▶ < 注 ▶ < 注 →

What is D2? What can it do?

D2 Service Components Trident Portal: Wiki and Files





Summarv

What is D2? What can it do?

D2 Service Components Trident Portal: Wiki and Files

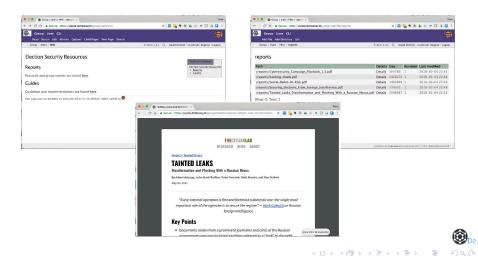


- C O Secure https://puple.dotteekay.bl/proup/rein/16/eporta/	x 🔛 🐂 🕈 🍇 🕹 🕹 🖓 🗔 🔂			
Group User CL				E
AM THE AM DIRECTOR US				
Group > main > Files > reports	Indem 3.4.	0, 07	ed Dittmch	UhartHode: Regular Logos
reports				
Path	Details	Size	Revision	Last modified
/reports/Cybersecurity_Campaign_Playbook_1.3.pdf	Details	364780	1	2018-02-04 22:45
/reports/hacking-chads.pdf		2428476		2018-02-04 22:44
/reports/Secret-Ballot-At-Risk.pdf	Details	3488889	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	\$346987	1	2018-02-04 22:52
Difect: 0. Total: 5				
Add a new file Add a new directory				



What is D2? What can it do

D2 Service Components Trident Portal: Wiki and Files



What is D2? What can it do?

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:

- 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.
- 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.
- 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 nedium-intensity incident, [CHIPF ILECTION OFFICIAL] will need o make a judgement call about whether to active the CCLF, but if the incident likely to become public and raise questions about trues in the dection systems. [CHIPF ILECTION OFFICIAL] should error the side of activation. You can always advective if the intensity declines. One activated, [CHIPF ILECTION OFFICIAL] along with [DIRECTOR OF ILECTIONS], will decide which level apple, subs on an initial assessment. One (CHIPF ILECTIONS], will decide activate the CCRT, all key response team members will be notified of the activation [INEERT STATE'S HITTOR OF REACHING THAN HERERES].

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



What is D2? What can it do?

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.



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



What is D2? What can it do?

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.





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.

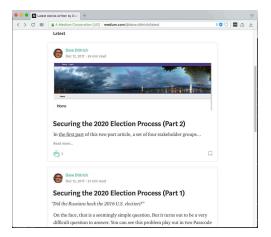
https://www.esquire.com/news-politics/politics/news/a55603/ russia-hack-voting-totals/

58.5K f 🗾 🖂



What is D2? What can it do?

Securing the 2020 Election Process



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



What is D2? What can it do?

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.



・ロ と ・ 一日 と ・ 日 と ・ 日 と

What is D2? What can it do?

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!



・ロン ・四 ・ ・ ヨ ・ ・ ヨ ・ ・

What is D2? What can it do?

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!



ヘロア 人間 アメヨア 人間 アー

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!



<ロト <回ト < 回ト < 回ト

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)

< 口 > < 🗇 >

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

