# 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)



・ロト ・回ト ・ヨト ・ヨト

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



Institute of Technology

#### Distributed Incident Management System (DIMS)





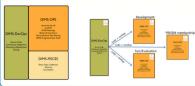
dittrich@u.washington.edu, linda.parsons@nextcentury.com

#### Summary

The Distributed Incident Management System (DMS) project is intended to take semi-automated sharing of structured intera information (MTRIG) STN structure), building on the seconds of the Public Migraul Inflatanticus security predistorials known as Tolefort, and calls it to the next level. DMS Takes advantage of the spon nexage that articular operationals known as Tolefort, and calls it to the next level. DMS Takes advantage of the spon nexage that articular operationals have made the spon nexage of the spon nexage that advantage of the spon nexage that the spon nexage of the spon nexage that advantage of the spon nexage that the spon nexage of the spon nexage that advantage of the spon nexage that the spon nexage that the spon nexage that advantage of the spon nexage of the spon nexage that the spon nexage that the spon nexage that an advantage of the spon nexage of the spon nexage that the spon nexage that an advantage of the spon nexage of the spon nexage that the spon nexage of the spon nexage of the spon nexage that the spon nexage of the spon nexage that the spon nexage of the spon nexage and the spon nexage of the spon nexage of the spon nexage of the spon nexage of the spon nexage and the spon nexage of the spon nexage. The spon nexage of the spon nexage o

#### System Architecture

The DMS project integrate over a dozen independent open source system components, some develoed by the DMS tana and many more by other open source projects into the functional use bysets. DMS-DE-Ody, sare a continuous integration environment using Jenkins for othware build and dedownent. Ansile for automated system comparation and othere installation, feffin forly eight sparsant GB 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.

(historia)	And in case of some line in case of	and the second se	in succession in the second se
		and the second se	

#### 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.



Research State Alexan A

#### 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

イロト イヨト イヨト イヨト

ISBN in factor by the Department of Heresteed Society and economic HERESCO. 13-C 4000 DIES Crass Sectors: Devices BAD Society and An Taxonomic Ministeries • Ministeries DC • Department Holds 2016



## 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

# 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?

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

・ロト ・回ト ・ヨト ・ヨト

Э

**Stakeholders** Targets Attention

## Who are the Stakeholders?

D. Dittrich. <u>The Ethics of Social Honeypots</u>. 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 trickstors

#### Self-Interested Parties

・ロト ・回ト ・ヨト ・ヨト

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



**Stakeholders** Targets Attention

## Who are the Stakeholders?

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

Election Officials	The Electorate	
Secretaries of State, County Elections Boards	The voting public (the primary and key	
	stakeholders)	criminals, terrorists

ヘロト 人間 とくほ とくほう

**Stakeholders** Targets Attention

## Who are the Stakeholders?

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

Election Officials	The Electorate	Political Campaigns &	
Secretaries of	The voting	Candidates	
State, County Elections Boards	public (the primary and key stakeholders)	Candidates, National and state political parties, staff,	
		volunteers, dirty tricksters	œ

ヘロト 人間 とくほ とくほう

**Stakeholders** Targets Attention

## Who are the Stakeholders?

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

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

・ロト ・ 日 ・ ・ 日 ・ ・ 日 ・

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	recording and tabulation of votes cast	



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		



æ

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

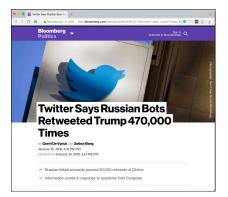
#### Attention!





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

#### Attention!





ヘロン 人間 とくほ とくほ とう



Э

is being done? erations with D2 Summary

Attention!

Integrity of voter	Integrity of election results	Availability of your ballot	Confidentiality of party com-
perceptions	Lots of	<del>Less</del> Getting	munications
Lots of	attention	more attention	Less attention
attention			



2

ヘロア 人間 アメヨア 人間 アー

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

## Outline





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



... 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

FONWYDEN				CONNET	TEED.
OBJORN				CONTRACTOR OF	Provent.
NAMES OF TAXABLE PARTY.	THE ON	Advised Obstan	Charles .		
(BANK)		United States		Salt Constant	molination.
A CANTER PART AND	ALC: NO.	WASHINGTON, DC 205	10-5795	APP COMPTS	the advector
COMPACTOR IN 1983)		December 12, 28			
		December 12, 29	17		
Assistant of The White 1600 Perm		e National Security Affairs			
Dear Gene	nd McMaster:				
I write to a government		immediate action to socure fo	deral elections	from backing by for	rign
periously, or government election co	thers are serious it cybenitaeks. A borsecurks to the	a cor election infrastructure. Is lagging behind and remain a such, the federal governme statos is irresponsible and a in matters of national security	weefully values of must take a total abdication	senable to feetign ction: leaving federal	
electronic unbeoded, directly int and cannot electronic November or conchine	soting machines a Fourisen states at o the machines' o be subsequently sote tailly. Moreor's clottloss on vo is conning. Windo	complained for decades obve- and the need for paper and/t (if use Direct Recording Elle digital memory: These voting audiool If voting officials ha ver, according to the //ww fit ting machines ranning. Wind yes XP. These two openting ator, which leaves them repe	trails. Their we thonic voting prachines de- ve any reason ek 71mes, Geo irws 2000; par systems are d	mings have largely g machines that record not produce a paper to to doubt the validity o rgin conducted to of Pennsylvania rel to cades old and no iron	notes will of the ied
governmen foreign adv in election complex th Attorney C	t is not doing enc resulties. When a s, Atkomey Gener at for most of us leveral Sexions'	her, Attorney General Jeff So sogh to prevent future olocide sked if the government is tai al Sextions stated that "we'r we're not able to fally graup testimery suggests that the <i>i</i> ing sufficient resources to flo	in interference ing adequate a e-ret," and the the technical Vdministration	by Russia and other action to prevent med- t "the matter is so fangers that are out th is not taking this issue	ere."
			27222	monte-tarte	
AN LOW MENT					
in construct all sta manual strategy boles and	ALL DATE OF ALL DATE	LARSE IN CASES OF STREET	an on role	IT SPORTORICAE SHE HT RESULTS THE DOLLAR-THE	NT AL ON

- 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

・ロト ・回ト ・ヨト ・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

FONWYDE	N.			COMME	
AVABLE OF BELLEVILLE	NETE OF	United Stat	rs Senate	COMPTER OF ENGLY	
		WASHINGTON DC		10100413	E IN WHITEH
DUCTOR DATE OF T	E BULLENC				
All a lot a lot a		December 12	2017		
Assistant The Whit		e National Security Affa	in:		
	ice, D.C. 20500	*			
Dear Ger	end McMaster				
1 write to governme		incrediate action to socc	ee federal election	is from hacking by for	cign
up call to cybersect seriously, governmo election o	the U.S. griveran arity weaknesses in others are serious not cyberatueks. A phorsecurity to the	Dansian government duri ent. Moving Sorward, lin a cur election infrastruct by lagging behind and re a such, the federal gover e status in irresponsible a in matters of national sev	eign government are. While some s main woefully ve mescet must take nd a total abdicat	s will continue to expl tates have taken the th inesable to feetign action: leaving federal	oit ceats
electrocic unbeeded directly is and camp electrocic Novembe on machi-	voting machines - Fourtoen states o to the machines' of he sobsequently vote taily. Moreo r's elections on ve res receiving Wied	complained for decoders and the need for paper a El use Direct Recording digital memory. These v audited if voting official ver, according to the /ve ting machines running V vers JAP. These two opes ator, which leaves them	adit trails. Their v Electronic voting rting machines do Is have any reaso w Yark Times, Ge Vindows 2000; pu sting systems are	sumings have largely p g machines that record o not produce a paper to to doubt the validity orgin conducted atts of Pennsylvania re decades old and no int	one votas mil of the lied
governme foreign as in electio complex Automey	nt is not doing en humaties. When a ns, Adomey Gene that for most of us General Semions'	her, Attorney General Jo sugh to prevent fature of sked if the government al Sessions stated that " we're net able to fully p testimory suggests that ing sufficient resources t	oction interference is taking adequate we're not," and the map the technical the Administration	e by Russia and other action to prevent med of 'the matter is so dangers that are out if n is not taking this isso	ding
CONCUMPORTER NO.	and the second s	N. AND BEDRO	10.007507	THE OWNER AND INC.	*****
CHILDR.	STREET, STREET	ADDING OF THE OWNER	ACCRET OF A		and a country of
10-00-000	04140-624	PROFESSION INCOME.		241.08-114	DELIG-ME

#### 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

・ロト ・回ト ・ヨト ・ヨト



... to assure X? The Gap

#### Letter from Senator Ron Wyden To: The White House

	N.		CONSISTING IN PORT
			COMPTE OF BARKET
AVABLE REALT CONTRACT	NETEOR	United States Senate	COMPLEX CONTRACTS IN CONTRACTORS
		VANDATION DC 2010-3203	ARE COMPTE IN TRADUCT
DUCTION ADDRESS OF TAXABLE PARTY OF TAXA	R BULLEVO		
100.000		Depember 12, 2017	
	orable Lt. Gen. H.I		
Assisted The Shir		e National Security Affairs	
	te House tarchania Ave., N		
	tos, D.C. 20500	*	
Dear Ger	send McMaster:		
1 write to governme		immediate action to secure federal elections	from backing by foreign
up call to cybersect seriously, governmo election o	the U.S. greenm only weaknesses in others are serious out cyberatueks. A phorsecurity to the	bassian government during the 2016 electic ext. Moving Euromet, Energy governments is our election infrastructure. While some m by lagging behaving and moverhilly with a such, the foderal government must take a status is irresponsible and a total abdicate is matters of mational security.	will continue to exploit nos have taken the threats senable to foreign ction: leaving federal
electronic unbeeded directly in	e vorkog machinen 1. Fourtoen states o nto the machinen' o ot be subsequently a vore taily. Moreo tr's elections on ve	complained for decades about the risks and and the need for paper andit trails. Their we like the Direct Recenting Electronic wolfing fighth memory. These voluge mechanises do wolfield if vorting officials have any reason- ver, according to the Jiver Jave Threes, Geo taing machines maning Windows 2000; pro wo J2. These two openating systems are do	mings have largely gone machines that record votes out produce a paper trail to doubt the validity of the rgis conducted to of Pennsylvania selind
electronic November on pachi	nes running Winds titcal security upd	ates, which leaves them especially vulneral	ile to cyberattacks.
electronic Novembe on machi- receive cr	ritical security upd		le to cyberattacks.
electronic Novembe on enachi receive co At a Sena	ritical security upd ate bearing in Octo	ber, Altorney General Jeff Sessions conced	le to cyberattacks. ed that the U.S.
electronic Novembe on machi nective cr At a Sena governme	ritical security upd ate bearing in Octo ant is not doing an		le to cyberattacks. ed that the U.S. by Russia and other
electrania Novembe on cauchi nective ci At a Sena governma foreign as in electio	ritical security upd se bearing in Octo ent is not doing en dversaties. When a ns, Attorney Gene	her, Altorney General Jeff Semions concell ough to prevent future election interference skiel if the government is taking adequate i al Semions stated that "we're rest," and the	el that the U.S. by Russia and other action to prevent meddling of the matter is so
electratia Novembe on machi receive et At a Sena generation foreign au in electio complex i	ritical security upd ate hearing in Octo ont is not doing on downaaties. When a na, Adorney Gene that for most of us	ber, Attorney General Jeff Sessions conced ough to prevent fature election interference sked if the government is taking adequate a al Sessions stated that "we're root," and the wa're net able to fully grang the sechnical i	le to cyberattacks. ed that the U.S. by Russia and other ection to prevent meddling i "the matter in so langers that are out there."
electratia Noverabe on mashi receive ci At a Sena governma foreign as in electro complex : Miterery	ritical security upd ne bearing in Octo ent is not doing en dwersaties. When a ns, Atlorney Gene that for most of us General Servisors'	ber, Atterney General Jeff Sensions consent sugh to prevent future election interference dated if the government is taking adequate a nl Sensions stated that "we've rest," and the we've net able to fully graup the technical technical systement suggests that the Administrational	ele to cybernitacio. ed that the U.S. by Kuunia and other action to proven meddling t "The matter is so langers that are out there." is not taking this issue
electratia Noverabe on mashi receive ci At a Sena governma foreign as in electro complex : Miterery	ritical security upd ne bearing in Octo ent is not doing en dwersaties. When a ns, Atlorney Gene that for most of us General Servisors'	ber, Attorney General Jeff Sessions conced ough to prevent fature election interference sked if the government is taking adequate a al Sessions stated that "we're root," and the wa're net able to fully grang the sechnical i	ele to cybernitacio. ed that the U.S. by Kuunia and other action to proven meddling t "The matter is so langers that are out there." is not taking this issue
electratia Noverabe on mashi receive ci At a Sena governma foreign as in electro complex : Miterery	ritical security upd ne bearing in Octo ent is not doing en dwersaties. When a ns, Atlorney Gene that for most of us General Servisors'	ber, Atterney General Jeff Sensions consent sugh to prevent future election interference dated if the government is taking adequate a nl Sensions stated that "we've rest," and the we've net able to fully graup the technical technical systement suggests that the Administrational	ele to cybernitacio. ed that the U.S. by Kuunia and other action to proven meddling t "The matter is so langers that are out there." is not taking this issue
electratic Novembe or machi- rective of At a Sena governm foreign a m discus complex complex Attorney antionaly	ritical security upd ne hearing in Octo ent is not doing en downauties. When a ns, Adorney Gene that for most of an General Serviens' enough or dedicat	her, Alterney General Jeff Semions concer- ough to percent flatase election instructions call of the government is saling adequate all Semions stated that "we're rest," and the very net call to of Hilly graup the schedual testimory suggestio that the Administration flat staticture tomoraces to Focing It. That m	ite to cybernstacks. of that the U.S. by Ramin and other notice to provent modifiing of the market is no langues that are one there." is not taking this issue at change.
electracia Novembe ou maché necelive ci Al a Sem governa foneign a m decelio complex Advernation Advernation	ritical security upd ate bearing in Octo ent is not doing en devesaries. When a na, Adomey Gene that for most of an General Servisons' enough or dedicat	her, Alterney General Jeff Semions concell only to percent flates election interference shell of the government is saling adequate a la Senione mated that "were rest," and that territary suggests that the Administration of an et al-box hill by grant that suchadual territary suggests that the Administration generative territories to fully 1. That m	in to cyberntacks. of the the U.S. by Rumin and their scion to prevent meddling "the matter to a languest that are out there." is not taking this issue at change.
electratic Novembe or machi- rective of At a Sena governm foreign a m discus complex complex Attorney antionaly	ritical security upd ne hearing in Octo ent is not doing en downauties. When a ns, Adorney Gene that for most of an General Serviens' enough or dedicat	her, Alterney General Jeff Semions concell only to percent flates election interference shell of the government is saling adequate a la Senione mated that "were rest," and that territary suggests that the Administration of an et al-box hill by grant that suchadual territary suggests that the Administration generative territories to fully 1. That m	it to cyberstack. of that to U.S. by Runit and ther schen to prevent modifies the matter is on tangen that are out there. <sup>1</sup> is not taking this issue are change. 2010/2010/2010/2010/2010/2010/2010/2010

- 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 -		COMMITTEES.
AVABLE REPORT OF CON-	NETTER	United States Senate	COMPTER OF ENDING & MOUNT AND
		WASHINGTON, DC 28510-3785	ARE COMPTE IN YOURSE
DI CRAZON ROATE OFF	X BULLEYC		
ite din lan		December 12, 2017	
The Hen	orable Lt. Gen. H.F.	McMaster, Jr.	
The Whi	te House	r National Security Affairs	
	terybania Ave., N <sup>4</sup> tes, D.C. 20500	<i>x</i> ′	
Dear Ge	send McMaster:		
1 write to governme		menediate action to socure federal election	s from hacking by foreign
up call to cybersec seriously governme election	the U.S. griverness urity weaknesses in others are serious out cyberatueks. A phorsecurity to the	carsian government during the 2016 election. Moving forward, firetign government can also an infrastructure. While some is 9 lagging behavior and mean some weekly we is such, the foderal government must take is status in irresponsibile and a trutal abdication matters of mational security.	will continue to exploit atos have taken the threats neable to foreign ation: leaving federal
electronic unbeedee directly is and came	e vorkag machines a 1. Fourtoen states at nto the machines' c ot he subsequently a vore taily. Moreover's cloctices on vo	complained for decades about the risks as and the need for paper andit trails. Their w II use Direct Receiving Tacheols voting light memory. These voting machines do andited if voting officials have any neare rea, according to the New York Takes, Ger ling machines maning Windows 2000, put w 3D. These two openating systems are v	anings have largely gone machines that record votes not produce a paper trail to doubt the validity of the egis conducted ts of Pennsylvania toliad iscades old and no longer
Novemb on path	nes running Wands ritical security upda	nes, which leaves them especially vulners	hie to cyberattacks.
Novemb on machi neenive c At a Sen governm foreign a in dectie complex Attorney	ritical security upda ne hearing in Octol ent is not doing enc dwersaties. When a ns, Adomey Gener that for most of us General Services'	tion, which leaves them expectally vulner wer, Alterney General Jeff Sessions conse up to gorvener fature obtaion interference sked if the government is taking adequate al Sessions mixed that "we're net." and the var're net able to fully group the sochacida textinaney suggests that the Administration go stiff-left success to Toding 2. "That m	led that the U.S. by Romia and other action to provent meddling it "ble matter is so dangers that are out there." is not taking this issue
Novemb oc mach neetive o At a few groetme foreign a in electer complex Antoeney actionally	ritical security upda ate bearing in Octol ent is not doing me downaries. When a ray, Adomny Gener that for most of ua General Sections' enough or dedicati	ter, Alterney General Jeff Semions conce- ogh to percent flatte election interfermos del (f the government is tailing adequate al Senions mated that "we're reet," and the restinancy suggests that the Administration of sufficient toronomous to folge 8. That re biogenetation	Idel that the U.S. by Roatin and other action to provent mediding at The metaler in so dampen that are out there." In not taking this issue art change.
Novemb oc mach nective c At a Sem governm foreign a m directi complex Attorney antimudy	ritical security upda ne hearing in Octol ent Is not doing enc downauies. When a ns, Atlorney Gener that for most of un General Sensions' enough or dedicari	ter, Alterney General Jeff Semions conce- ogh to percent flatte election interfermos del (f the government is tailing adequate al Senions mated that "we're reet," and the restinancy suggests that the Administration of sufficient toronomous to folge 8. That re biogenetation	led that the U.S. by Romain and other action to prevent meddling at The reather is so dampen that are out there." is not taking this issue and 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

・ロト ・回ト ・ヨト ・ヨト



... to assure X? The Gap

#### Letter from Senator Ron Wyden To: The White House

	N.		CONSISTING IN PORT
			COMPTE OF BARKET
AVABLE REALT CONTRACT	NETEOR	United States Senate	COMPLEX CONTRACTS IN CONTRACTORS
		VANDATION DC 2010-3203	ARE COMPTE IN TRADUCT
DUCTION ADDRESS OF TAXABLE PARTY OF TAXA	R BULLEVO		
100.000		Depember 12, 2017	
	orable Lt. Gen. H.I		
Assisted The Shir		e National Security Affairs	
	te House tarchania Ave., N		
	tos, D.C. 20500	*	
Dear Ger	send McMaster:		
1 write to governme		immediate action to secure federal elections	from backing by foreign
up call to cybersect seriously, governmo election o	the U.S. greenm only weaknesses in others are serious out cyberatueks. A phorsecurity to the	bassian government during the 2016 electic ext. Moving Eurosed, Energy governments is our election infrastructure. While some m by lagging behand and remain workfully with a such, the foderal government must take a status is irresponsible and a total abdicate is matters of mational security.	will continue to exploit nos have taken the threats senable to foreign ction: leaving federal
electronic unbeeded directly in	e vorkog machinen 1. Fourtoen states o nto the machinen' o ot be subsequently a vore taily. Moreo tr's elections on ve	complained for decades about the risks and and the need for paper and trails. Their we lie use Direct Recenting Electronics welling fighth memory. These voting machines do waited if voting officials have any reason we, according to the Jiver Jave Theory, Geo taing machines maning Windows 2000; pro w320. These two openating systems are do	mings have largely gone machines that record votes out produce a paper trail to doubt the validity of the rgis conducted to of Pennsylvania selind
electronic November on pachi	nes running Winds titcal security upd	ates, which leaves them especially vulneral	ile to cyberattacks.
electronic Novembe on machi- receive cr	ritical security upd		le to cyberattacks.
electronic Novembe on enachi receive co At a Sena	ritical security upd ate bearing in Octo	ber, Altorney General Jeff Sessions conced	le to cyberattacks. ed that the U.S.
electronic Novembe on machi nective cr At a Sena governme	ritical security upd ate bearing in Octo ant is not doing an		le to cyberattacks. ed that the U.S. by Russia and other
electrania Novembe on cauchi nective ci At a Sena governma foreign as in electio	ritical security upd se bearing in Octo ent is not doing en dversaties. When a ns, Attorney Gene	her, Altorney General Jeff Semions concell ough to prevent future election interference skiel if the government is taking adequate i al Semions stated that "we're rest," and the	el that the U.S. by Russia and other action to prevent meddling of the matter is so
electratia Novembe on machi receive et At a Sena generation foreign au in electio complex i	ritical security upd ate hearing in Octo ont is not doing on downaaties. When a na, Adorney Gene that for most of us	ber, Attorney General Jeff Sessions conced ough to prevent future election interference sked if the government is taking adequate a al Sessions stated that "we're root," and the wa're net able to fully grang the sechnical i	le to cyberattacks. ed that the U.S. by Russia and other ection to prevent meddling i "the matter in so langers that are out there."
electratia Noverabe on mashi receive ci At a Sena governma foreign as in electro complex : Miterery	ritical security upd ne bearing in Octo ent is not doing en dwersaties. When a ns, Atlorney Gene that for most of us General Servisors'	ber, Atterney General Jeff Sensions consent sight to prevent future election interference dated if the government is taking adequate a nal Sensions stated that "we've rest," and the we've net able to fully graup the technical technical systemic suggests that the Administrational	ele to cybernitacio. ed that the U.S. by Kuunia and other action to proven meddling t "The matter is so langers that are out there." is not taking this issue
electratia Noverabe on mashi receive ci At a Sena governma foreign as in electro complex : Miterery	ritical security upd ne bearing in Octo ent is not doing en dwersaties. When a ns, Atlorney Gene that for most of us General Servisors'	ber, Attorney General Jeff Sessions conced ough to prevent future election interference sked if the government is taking adequate a al Sessions stated that "we're root," and the wa're net able to fully grang the sechnical i	ele to cybernitacio. ed that the U.S. by Kuunia and other action to proven meddling t "The matter is so langers that are out there." is not taking this issue
electratia Noverabe on mashi receive ci At a Sena governma foreign as in electro complex : Miterery	ritical security upd ne bearing in Octo ent is not doing en dwersaties. When a ns, Atlorney Gene that for most of us General Servisors'	ber, Atterney General Jeff Sensions consent sight to prevent future election interference dated if the government is taking adequate a nal Sensions stated that "we've rest," and the we've net able to fully graup the technical technical systemic suggests that the Administrational	ele to cybernitacio. ed that the U.S. by Kuunia and other action to proven meddling t "The matter is so langers that are out there." is not taking this issue
electratic Novembe or machi- rective of At a Sena governm foreign a m discus complex complex Attorney antionaly	ritical security upd ne hearing in Octo ent is not doing en downauties. When a ns, Adorney Gene that for most of an General Serviens' enough or dedicat	her, Alterney General Jeff Semions concer- ough to percent flaton election instructions call of the government is saling adequate all Semions stated that "we're rest," and the very net calls to itally graup the schedual testimory suggests that the Administration flat static statements to fixing it. That m sufficient statements to fixing it. That m	ite to cybernstacks. of that the U.S. by Ramin and other notice to provent modifiing of the market is no langues that are one there." is not taking this issue at change.
electracia Novembe ou maché necelive ci Al a Sem governa foneign a m decelio complex Advernation Advernation	ritical security upd ate bearing in Octo ent is not doing en devesaries. When a na, Adomey Gene that for most of an General Servisons' enough or dedicat	her, Alterney General Jeff Semions concell only to percent flates election interference shell of the government is saling adequate a la Senione mated that "were rest," and that territary suggests that the Administration of an et al-box hill by grant that suchadual territary suggests that the Administration generative territories to fully 1. That m	in to cyberntacks. of the the U.S. by Rumin and their scion to prevent meddling "the matter to a languest that are out there." is not taking this issue at change.
electratic Novembe or machi- rective of At a Sena governm foreign a m discus complex complex Attorney antionaly	ritical security upd ne hearing in Octo ent is not doing en downauties. When a ns, Adorney Gene that for most of an General Serviens' enough or dedicat	her, Alterney General Jeff Semions concell only to percent flates election interference shell of the government is saling adequate a la Senione mated that "were rest," and that territary suggests that the Administration of an et al-box hill by grant that suchadual territary suggests that the Administration generative territories to fully 1. That m	it to cyberstack. of that to U.S. by Runit and ther schen to prevent modifies the matter is on tangen that are out there. <sup>1</sup> is not taking this issue are change. 2010/2010/2010/2010/2010/2010/2010/2010

- 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.

 "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)



... 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 integrity of election results.

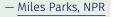
- Senate Select Committee on Intelligence releases <u>election security</u> recommendations
- U.S. Senate and House (H.R.4884) have both introduced the "Defending Elections from Threats by Establishing Redlines Act of 2018"
- Omnibus budget has \$380 Million for election security grants to states
- Current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



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

#### 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.



ヘロマ ヘロマ ヘロマ イ



... 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.

- Riseup <u>Message</u> <u>Security</u> <u>OpenPGP Best</u> <u>Practices</u>

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



... to assure X? The Gap

# What is being done so far?

... to ensure confidentiality of party communications.

- Riseup <u>Message</u> <u>Security</u> <u>OpenPGP Best</u> <u>Practices</u>

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



... to assure X? The Gap

# What is being done so far?

... to ensure confidentiality of party communications.

- Riseup <u>Message</u> <u>Security</u> <u>OpenPGP Best</u> <u>Practices</u>

- Electronic Frontier Foundation's <u>Surveillance Self</u> 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 <u>Belfer Center</u> "Cybersecurity 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



.. **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

< □ > < □ > < □ > < □ >



... to assure X? The Gap

#### 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 outpr 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 Nicrosoft65 that will provide all your basic office functions and a safe place to store information. (sec pages 34/5)

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

Require 2/A for all important accounts, including your office suite, any other email or strange services, and your social media accounts. Use a mobile app or physical key for your second factor, not text messaging. (sec pages 36-17)

#### 4. Create strong, long passwords:



For your passwords, travits SetERESTENDERLIFTCHOLLERETELERETEIN, not sensiting, really short like "L11, Contrary to popular belief, a long string of random words without symbols is more difficult to break time something short, with L01S Of SymBOLS A password manager can help. too. (scenage ID)

#### 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. (veroswer) 2-22) "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



... 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

tl 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.

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

・ロト ・回ト ・ヨト ・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.

#### • 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



Michael McFaul 51.7K Tweets

tl 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 (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

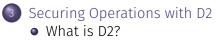


What is D2? What can it do?

# 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?

#### 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



**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?

# 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

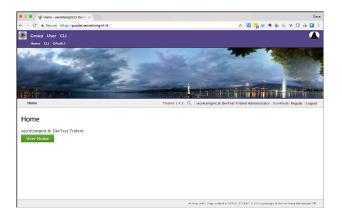


Service Components



What is D2? What can it do?

#### D2 Service Components Trident Portal



Trident Portal



<ロ> <同> <同> < 同> < 同>

What is D2? What can it do?

#### D2 Service Components Trident Portal

the state of the s	1 B B + 4 B + 1 B + 2 F
Theorem Const Coll Annual State Coll	•
	and the second second
Milmon	Carlos and an and a finite statements
item.	
ALL ROOM	

https://trident.li/

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



イロト イヨト イヨト イヨト

• Low cost to deploy and administer



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

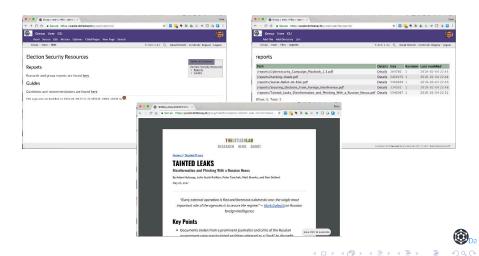


	* 8		6 6 Y 0 6 0
			E
Indem 1.4.	s Q, Dan	ed Dimrich   1	InterNode: Regular   Logos
Details	Size	Revision	Last modified
Details	364780	1	2018-02-04 22:45
Details	2428476	1	2018-02-04 22:44
Details	3488889	1	2018-02-04 22:46
Details	334591	1	2018-02-04 22:48
f Details	5346987	1	2018-02-04 22:52
	Details Details Details Details Details	Details Size Details Size Details 364780 Details 2428476 Details 2428476 Details 334591	Datails         Size         Revision           Details         364780         1           Details         2428476         1           Details         3488889         1



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?

#### D2 Service Components DevOps Services

••/	B Rebbins	Management	( ) ( )	× D															0
) C	0 . 50	cure https	(red se	cretsingin	e Rece	,ti <sub>l</sub> omtidale				÷	8	-	9.3		6 (	5	• 1	0 D	۵
<b>B</b> R		tMQ.		15 Erlan weels		t ianges	Ques	ves Admin	Rafreshed	2018	5-01-S				têre	Virt.	cret	tornet All torners	.tk
Overv																			
Queued re	essages last	t minute 2																	
Durrently i Message ri	die Nes last wi	nute 2																	
Connection of	eta 🛛	hannela: 0	Daths	ngca: 16	90	esta: Ø	Cores	man: 0											
Gisbal cou	na: 0 0	hannsla: 0	Daha	nges: 16	9	eve: 0	Coras	man: 0											
Cistal cou	na: 0 0	hannels: 0		ngen: 16 descriptor		_		most: 0 Mamory	Dek sp	08		Up	ine	are a	<i>f</i> o		less	et stats	
Connection V Noder	nta (2) Mai: O C Mai: O C Mai: O C		Stoke Z		. 61	_	5003			sca			ine 38n	6	fe Lasic		Thé	etate ta etate ta soca si esboa t	
Gisbal cou Comesce * Noder Name	nta (2) Mai: O C Mai: O C Mai: O C	acriptors 3 28 20 constants	Stoke Z	descriptor	. 61	iong proce 360	5003	Mamory 65MB		sca	Part			6	usic		Thé	la noda	
Gisbal cou Comesce * Noder Name	nts 2 max 0 C File de 50 III and contes	acriptors 3 28 20 constants	Stoke Z	descriptor	. 61	iong proce 360	5003	Mamory 65MB		sca	(rail)			6	usic		Thé	la noda	
Gisbal cou Connecto + Noder Harre rabbit@r	nts 2 max 0 C File de 50 III and contes	28 28 in postation the	Stoke Z	descriptor	. 61	iong proce 360	5003	Mamory 65MB		sca	(****			6	usic		Thé	la noda	
Gisbal cou Connecto V Noder Name rabbitor V Parts Listening p	nts 2 max 0 C File de and contex orts	28 28 in postation the Point	Stoke Z	descriptor	. 61	iong proce 360	5003	Mamory 65MB		sca	(real)			6	usic		Thé	la noda	
Connection	nts 7 File de and center erts Bound te 127.0.0.1	28 28 in postation the Point	Stoke Z	descriptor	. 61	iong proce 360	5003	Mamory 65MB		sca	1945			6	usic		Thé	la noda	



What is D2? What can it do?

#### D2 Service Components DevOps Services

	Repping	Managemen	x 🖂							D
C	0 . 50	cure   https	(red secretsmont.)	k/raisbitmq/#/		2 😫	<b>5</b> 9 3	6 6 8	¥ 🛛 0-	۵
<b>B</b> R	_	tMQ.	3.6.15 Erleng: Channels E	20.2 xchanges Que		Refreshed 2018-01-2		v abit@red.	wy 5 wornts rtual host   A secretarigni chinan [69] (	t.tk
ver										
Queued m	essages las	t minute 2								
Currently Pressage r	idle ales last mi	nde 2								
Durrently	dio									
Gisbal cou	inta 7									
Cometti		hannela: 0	Exchanges: 16	Queues: 0 Core	umos: 0					
-	•	hannela: 0	Exchanges: 16		Namory	Disk space	Uptime	arfe -	Reset stats	
- Node	n File de					Disk space 1550 40% tur seternark	Uptime 2h 38m	basic disc 4	Reset stats This node All nodes	
✓ Node Name	n File de	20 20 20 20	Secket descriptors X	Erlang processors	Mamory 65MB	1500		basic	This mode	
✓ Node Name	n File de	20 20 20 20	Secket descriptors X	Erlang processors	Mamory 65MB	1500		basic	This mode	1
v Node Name (2000) v Ports	n File de	28 28 at postable	Secket descriptors X	Erlang processors	Mamory 65MB	1500		basic	This mode	
<ul> <li>Victoria</li> <li>Victoria</li> <li>Victoria</li> <li>Victoria</li> </ul>	a File de	28 28 crowlast Aut	Secket descriptors X	Erlang processors	Mamory 65MB	1500		basic	This mode	
<ul> <li>Node</li> <li>Name</li> <li>robotics</li> <li>Ports</li> <li>Listening p</li> <li>Fratical</li> </ul>	n File de red 15	28 28 crowlast Aut	Secket descriptors X	Erlang processors	Mamory 65MB	1500		basic	This mode	

Ø Jenkins				3	Q search		@ ada	in ling est
Jeriáns -							1583	ATCRIME
🚔 New Item							2	add description
L People		AI						
Build History		5	w	Name :	Last Success	Last Fallure	Last Duration	Far
Manage Jankins			۲	build parameterized	2 tr 2 min - 51	NVA	2.4 sec	2 合
La My Views			۲	build tpc-develop	N/A	N-1A	1.64	2 😭
Open Blue Ocean			۲	build receiped	NA	N'A	Non	2 1
Credentials			*	deploy-rate prod	NA	NA	NA	24
New Vew			*	instal lang	2 hr 2 min - <u>31</u>	NA	0.94 560	②☆
Build Queue	-	0	*	plation	NA	NA	NA	②☆
No builds in the queue.			*	pitchiork-data	N/A	NA	NA	②☆
Build Executor Status	-		-	0003-9057v	NA	2 fr 2 min - <u>#1</u>	0.83 sec	2 1
1 Idle 2 Min			*	nun gilaybook ganameterized	NA	NA	NA	2 1
2 104			*	Indent	NA	NA	NA.	②☆
			۲	trident-axt-arc	NA	NA	NA	2 1
			*	indent_stage	NA	NA	N/A	②☆
			۲	trident 02	N/A	NIA	Politik	②会
		kon:	SML		_	RSS for failures	_	

イロト イヨト イヨト イヨト



2

What is D2? What can it do?

## Securing the 2020 Election Process Improve criminal and counter-intelligence investigations



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



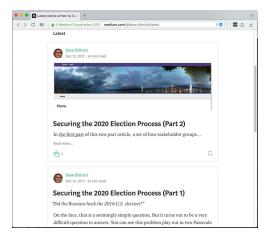
Illinois became Patient Zero in the government's probe, eventually leading investigators to a hacking pandemic that touched four out of every five U.S. states. Using evidence from the Illinois computer banks, federal agents were able to develop digital "signatures" -- among them, Internet Protocol addresses used by the attackers -- to spot the hackers at work. The signatures were then sent through Homeland Scurity 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/



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 > < 回 > < 回 >

# 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>

#### April 27, 2018 ISOI XX v1.5.0

TLP:WHITE (+= megaphone)

