Hacking the Voter

Lessons From a Decade of Russian Military Operations

Nate Beach-Westmoreland

Booz | Allen | Hamilton®

black hat® USA 2020

AUGUST 5–6, 2020

BRIEFINGS

Agenda

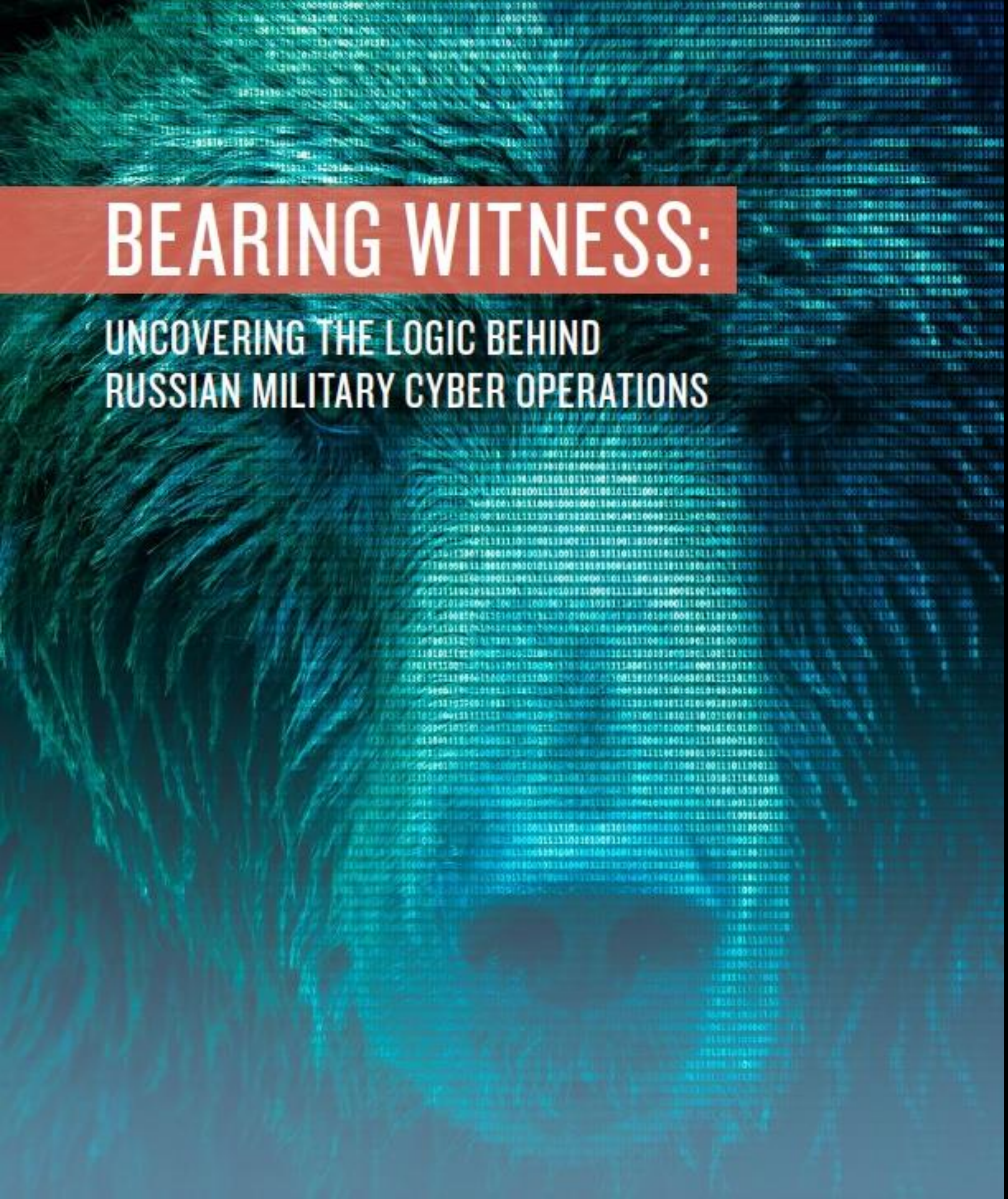
- "Why," not just "how"
- Information conflict
- Tactics in context
- What's next

Who Am I?

- Head of Strategic Cyber Threat Intelligence @ Booz Allen Hamilton
- Prior experience in elections, diplomacy, & law
- CTI by way of social sciences
    - B.A. History @ Cornell
    - M.A. International Relations @ Yale

Now Just How, but Why?

- Why conduct an operation?
- Why act at this time?
- Why use these tactics?
- What was the objective?
- How do operations relate to each other?



BEARING WITNESS:

UNCOVERING THE LOGIC BEHIND
RUSSIAN MILITARY CYBER OPERATIONS

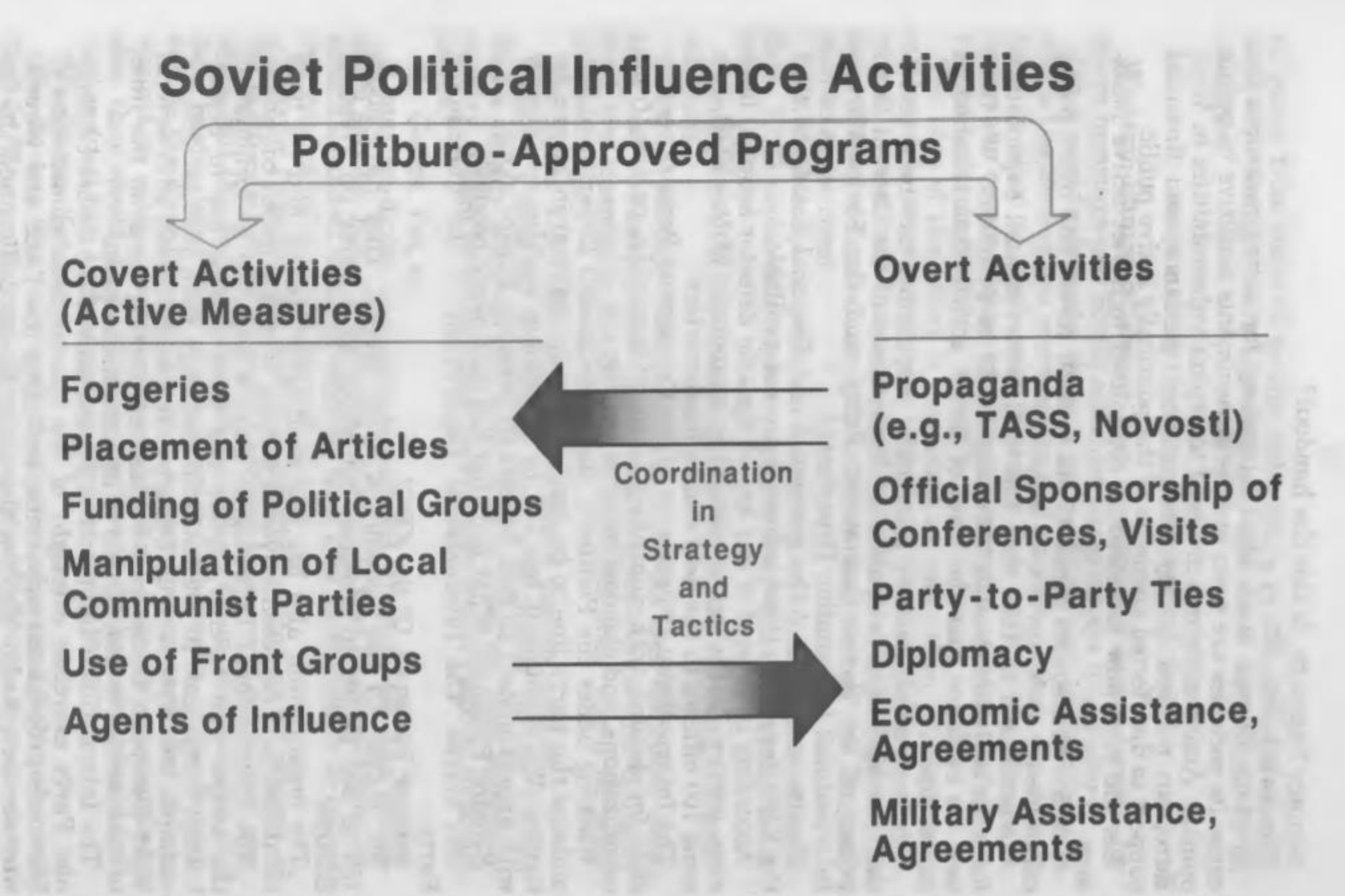
Background Reading

- Russia’s Military Doctrine explains the tactics, targets, and timing of GRU cyber operations
- TL;DR: the GRU has often done exactly what it said it would do

Soviet-Era Election Interference

Image Source: Everett Herald

Familiar Tactics, but Shifting Responsibilities



Soviet Political Influence Activities

Politburo-Approved Programs

Covert Activities (Active Measures)

- Forgeries
- Placement of Articles
- Funding of Political Groups
- Manipulation of Local Communist Parties
- Use of Front Groups
- Agents of Influence

Coordination in Strategy and Tactics

Overt Activities

- Propaganda (e.g., TASS, Novosti)
- Official Sponsorship of Conferences, Visits
- Party-to-Party Ties
- Diplomacy
- Economic Assistance, Agreements
- Military Assistance, Agreements

Image Source: U.S. Senate Intelligence Committee (1985)

Information Confrontation

The continuous competition over beliefs, opinions, perceptions, and feelings to enable the furthering of states’ agendas

“So, tell me more about how bad life is here! (translation)

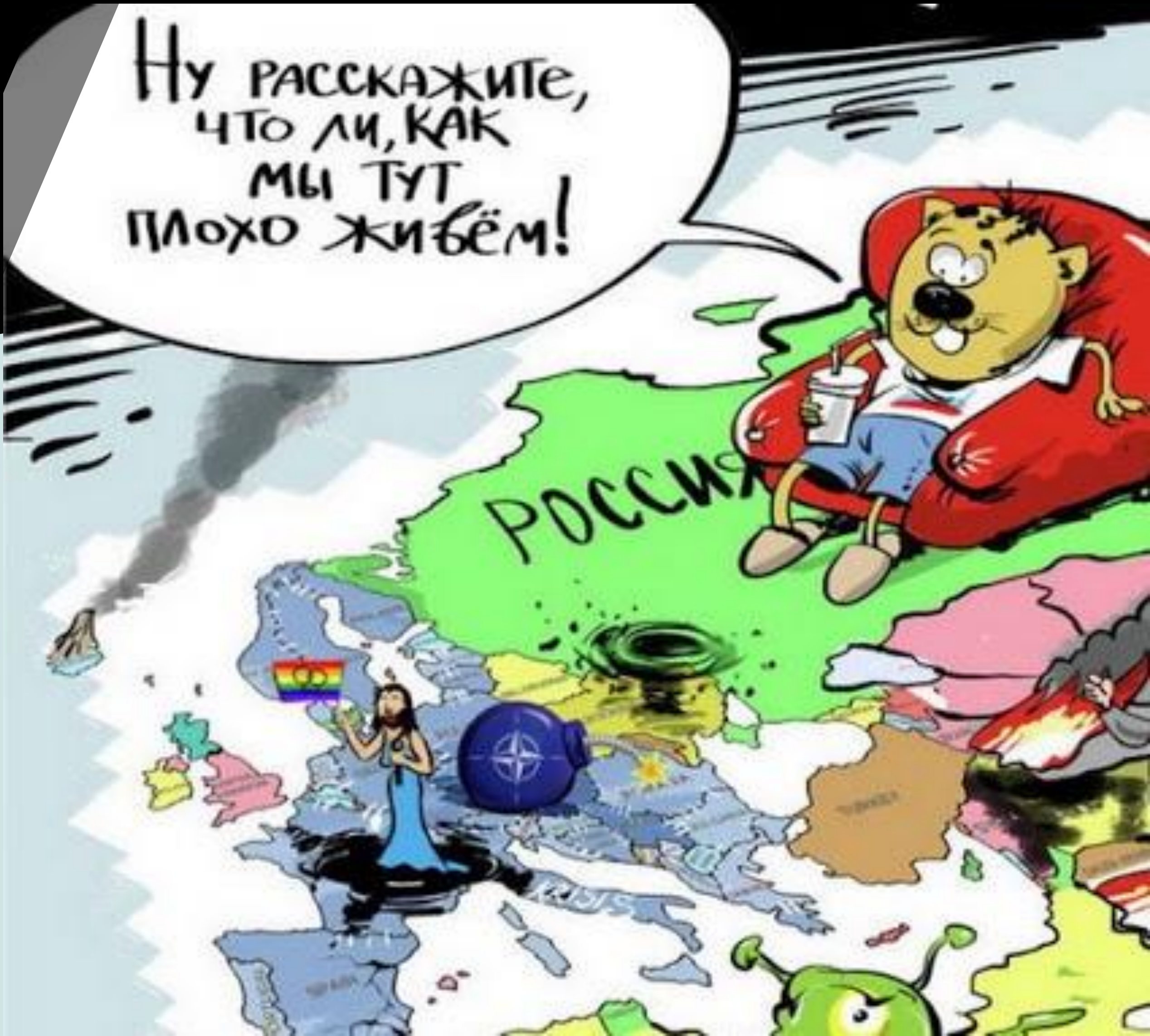


Image Source: Unknown

ХАОСОМЯТЕЖ – СИМВОЛ ЭПОХИ
США ОТРАБАТЫВАЮТ СТРАТЕГИЮ «МЯГКОЙ СИЛЫ» стр.4
УРОКИ ИСТОРИИ
ОБУХОВСКОМУ ЗАВОДУ – 150 ЛЕТ стр.42
БРОСОК НА ХАРБИН
УНИКАЛЬНАЯ ОПЕРАЦИЯ В АВГУСТЕ 1945 ГОДА стр.72
Национальная оборона
Si vis pacem, para bellum
6+
Информационное противоборство – задача стратегическая

Russian Military Bought Into Information Confrontation

- Codified into core military doctrinal documents since 2000
- Addition of new missions like protecting “historical, spiritual, and patriotic traditions”

“Information Confrontation – a Strategic Challenge”
- National Defense (March 3, 2013)

Information Confrontation's Two Sides

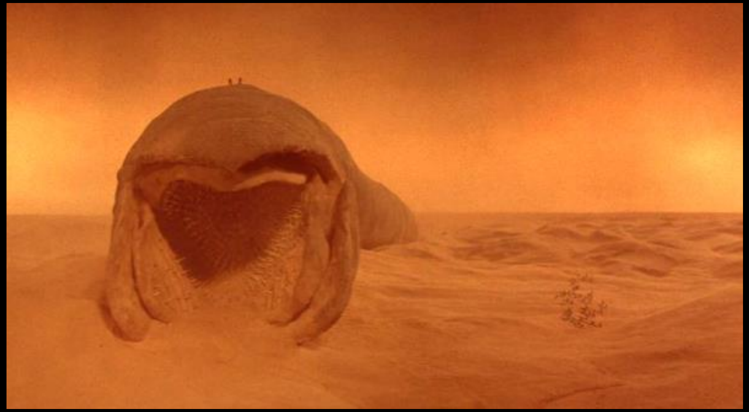
"Informational-Psychological" Capabilities

"Informational-Technical" Capabilities

≈

Fancy Bear //
APT28 //
Sofacy

≈



Sandworm

Image Source: Universal Pictures

Greater Utility Than Just Changing Outcomes

Undermine Opponents

Create New Opportunities

Shape Domestic Opinions

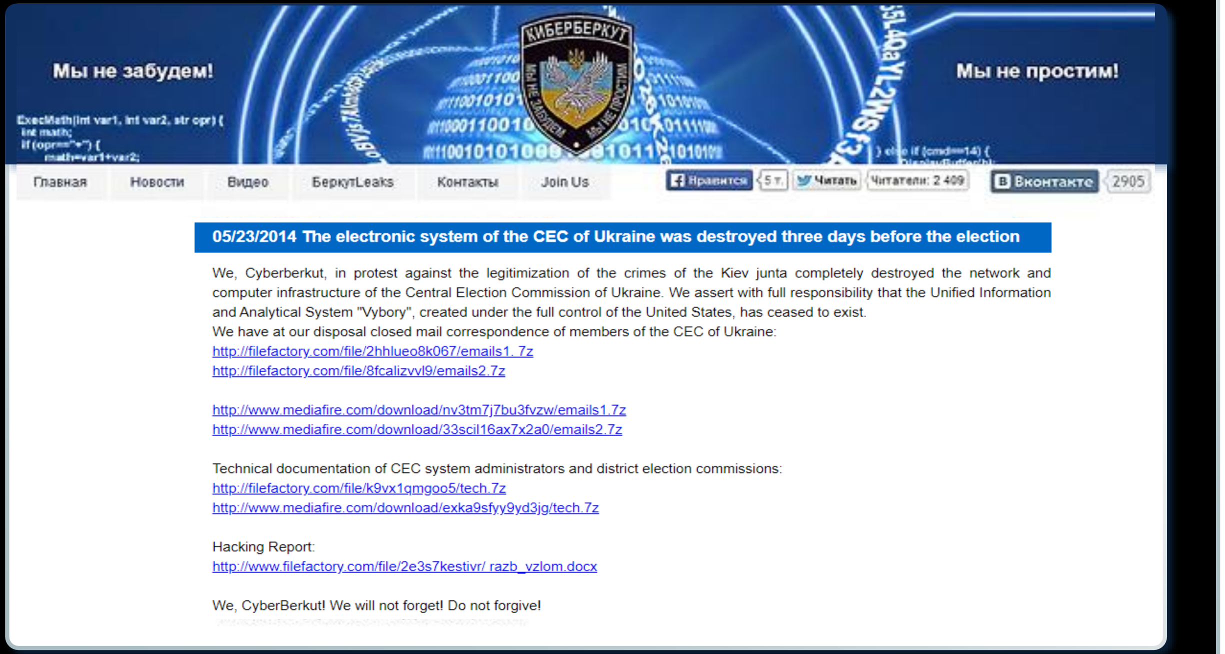
Ukraine (2014)

Amplify divisive and delegitimizing narratives

Image Source: Getty Images

Ukraine (2014)

Disrupt election infrastructure



05/23/2014 The electronic system of the CEC of Ukraine was destroyed three days before the election

We, Cyberberkut, in protest against the legitimization of the crimes of the Kiev junta completely destroyed the network and computer infrastructure of the Central Election Commission of Ukraine. We assert with full responsibility that the Unified Information and Analytical System "Vybory", created under the full control of the United States, has ceased to exist.
We have at our disposal closed mail correspondence of members of the CEC of Ukraine:
http://filefactory.com/file/2hhlueo8k067/emails1. 7z
http://filefactory.com/file/8fcalizvvl9/emails2.7z

http://www.mediafire.com/download/nv3tm7j7bu3fvzw/emails1.7z
http://www.mediafire.com/download/33scil16ax7x2a0/emails2.7z

Technical documentation of CEC system administrators and district election commissions:
http://filefactory.com/file/k9vx1qmgoo5/tech.7z
http://www.mediafire.com/download/exka9sfyy9yd3jg/tech.7z

Hacking Report:
http://www.filefactory.com/file/2e3s7kestivr/ razb_vzlom.docx

We, CyberBerkut! We will not forget! Do not forgive!

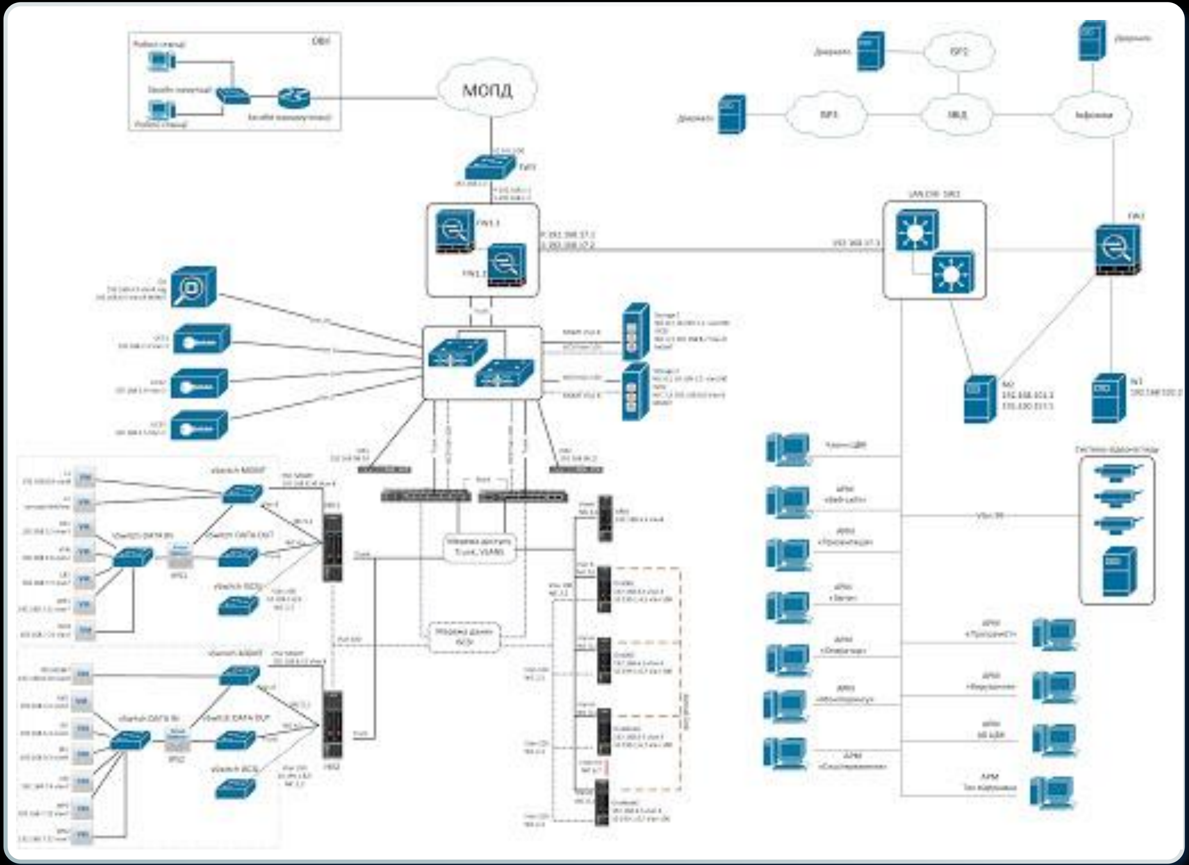
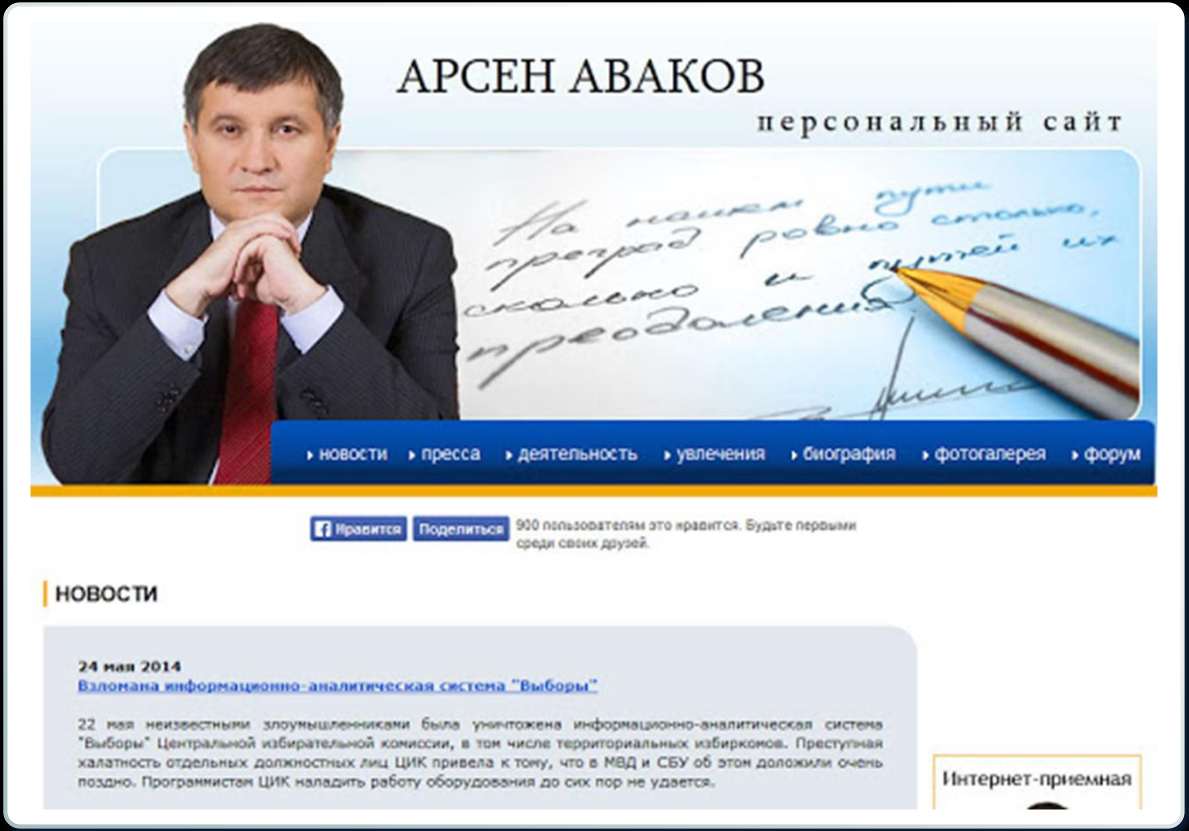


Image Source: CyberBerkut

Ukraine (2014)

Publicize and authenticate narrative of unreliable elections infrastructure



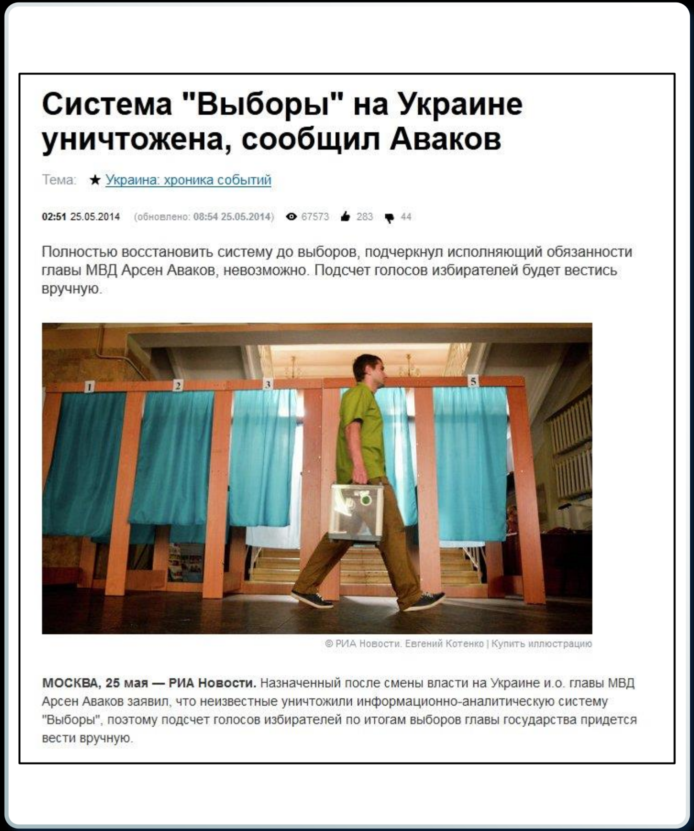
900 пользователям это нравится. Будьте первыми среди своих друзей.

НОВОСТИ

24 мая 2014

Взломана информационно-аналитическая система "Выборы"

22 мая неизвестными злоумышленниками была уничтожена информационно-аналитическая система "Выборы" Центральной избирательной комиссии, в том числе территориальных избиркомов. Преступная халатность отдельных должностных лиц ЦИК привела к тому, что в МВД и СБУ об этом доложили очень поздно. Программистам ЦИК наладить работу оборудования до сих пор не удается.



Система "Выборы" на Украине уничтожена, сообщил Аваков

Тема: ★ Украина: хроника событий

02:51 25.05.2014 (обновлено: 08:54 25.05.2014) 67573 283 44

Полностью восстановить систему до выборов, подчеркнул исполняющий обязанности главы МВД Арсен Аваков, невозможно. Подсчет голосов избирателей будет вестись вручную.

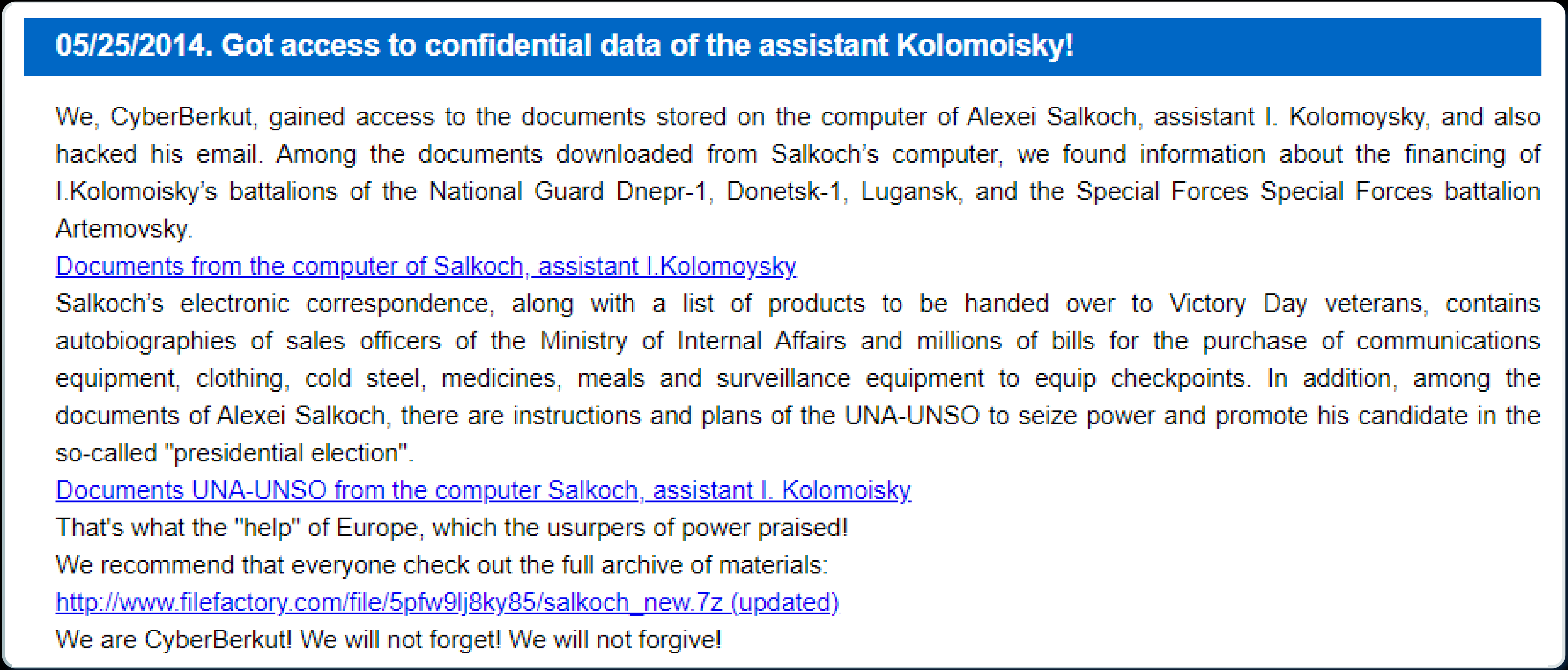
© РИА Новости. Евгений Котенко | Купить иллюстрацию

МОСКВА, 25 мая — РИА Новости. Назначенный после смены власти на Украине и.о. главы МВД Арсен Аваков заявил, что неизвестные уничтожили информационно-аналитическую систему "Выборы", поэтому подсчет голосов избирателей по итогам выборов главы государства придется вести вручную.

Image Source: Arsen Avakov, RIA Novosti

Ukraine (2014)

Leak documents allegedly showing a conspiracy to rig an election



05/25/2014. Got access to confidential data of the assistant Kolomoisky!

We, CyberBerkut, gained access to the documents stored on the computer of Alexei Salkoch, assistant I. Kolomoysky, and also hacked his email. Among the documents downloaded from Salkoch's computer, we found information about the financing of I.Kolomoisky's battalions of the National Guard Dnepr-1, Donetsk-1, Lugansk, and the Special Forces Special Forces battalion Artemovsky.

Documents from the computer of Salkoch, assistant I.Kolomoysky

Salkoch's electronic correspondence, along with a list of products to be handed over to Victory Day veterans, contains autobiographies of sales officers of the Ministry of Internal Affairs and millions of bills for the purchase of communications equipment, clothing, cold steel, medicines, meals and surveillance equipment to equip checkpoints. In addition, among the documents of Alexei Salkoch, there are instructions and plans of the UNA-UNSO to seize power and promote his candidate in the so-called "presidential election".

Documents UNA-UNSO from the computer Salkoch, assistant I. Kolomoisky

That's what the "help" of Europe, which the usurpers of power praised!

We recommend that everyone check out the full archive of materials:

http://www.filefactory.com/file/5pfw9lj8ky85/salkoch_new.7z (updated)

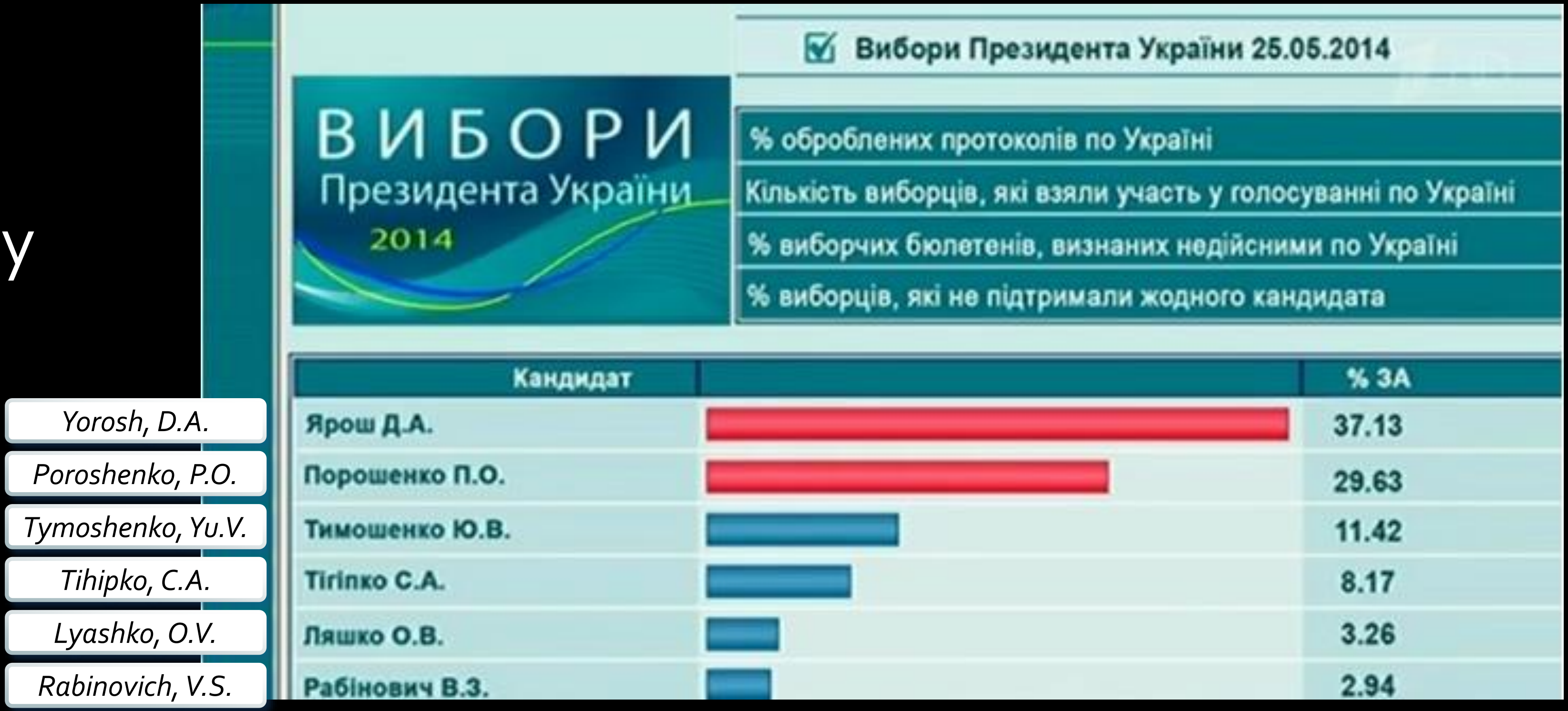
We are CyberBerkut! We will not forget! We will not forgive!

Image Source: CyberBerkut

Ukraine (2014)

- Forge and launder evidence consistent with existing polarizing narratives using sources of authority

- Hinder ability to counter this narrative



☑ Вибори Президента України 25.05.2014

% оброблених протоколів по Україні

Кількість виборців, які взяли участь у голосуванні по Україні

% виборчих бюлетенів, визнаних недійсними по Україні

% виборців, які не підтримали жодного кандидата

	Кандидат	% ЗА
Yorosh, D.A.	Ярош Д.А.	37.13
Poroshenko, P.O.	Порошенко П.О.	29.63
Tymoshenko, Yu.V.	Тимошенко Ю.В.	11.42
Tihipko, C.A.	Тігіпко С.А.	8.17
Lyashko, O.V.	Ляшко О.В.	3.26
Rabinovich, V.S.	Рабінович В.З.	2.94

Image Source: Channel 1 Russia

Bulgaria (2015)

Block access to key sources of election information

Image Source: Bulgarian Free Television (BSTV)

France (2017)

- Time releases to limit campaign's ability to debunk
- Launder leaks through online conspiracy communities
- Target undisclosed elections infrastructure

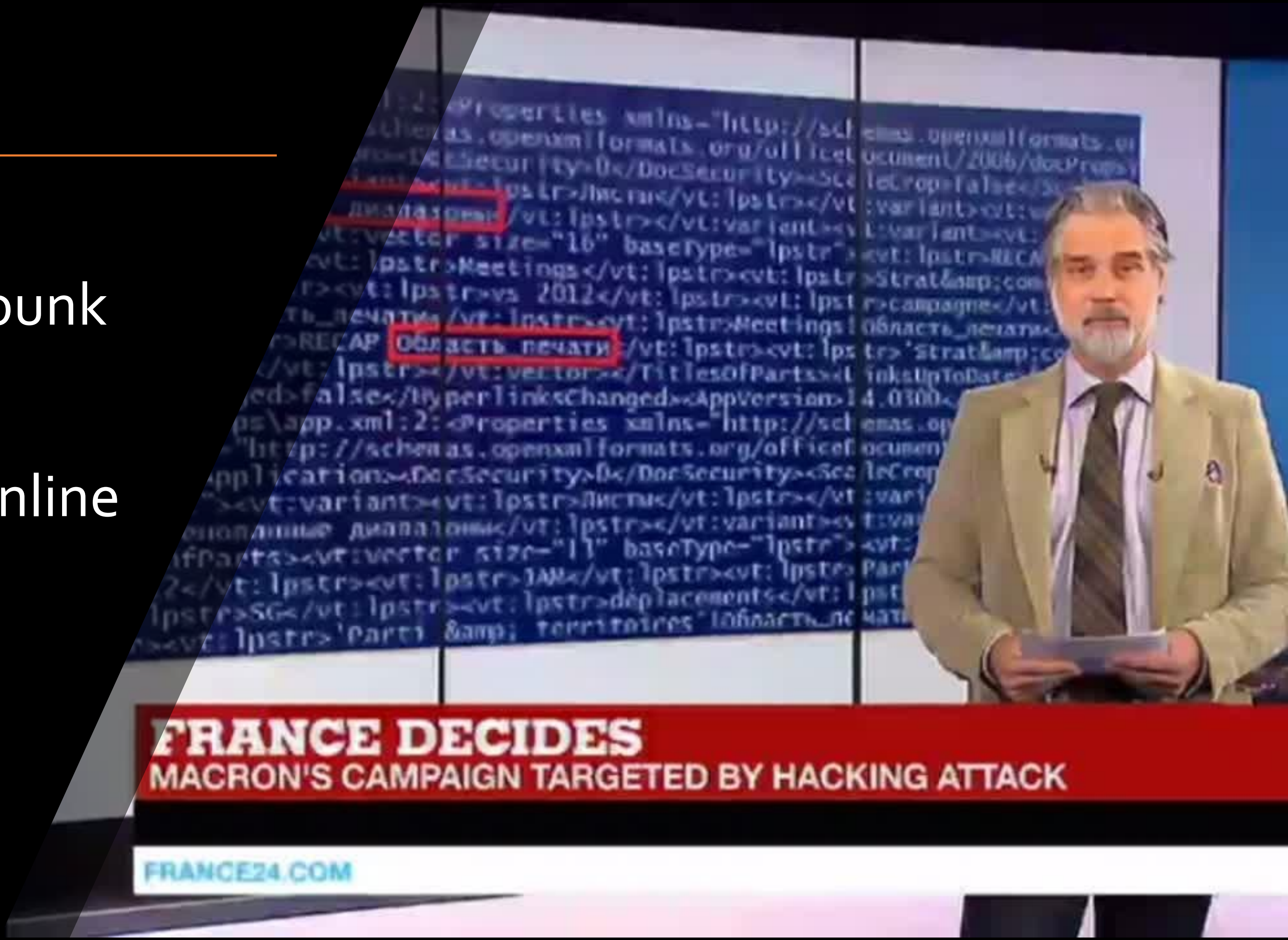


Image Source: France24 (YouTube screencap)

Montenegro (2016)

- Block access to key sources of election information
- Coordinate with community thought leaders
- False-flag violence

Image Source: European Pressphoto Agency

USA (2016)

- Launder leaks via journalists, faketivists, etc.

- Time releases to maximally inflame political & social divisions, suggesting a rigged election

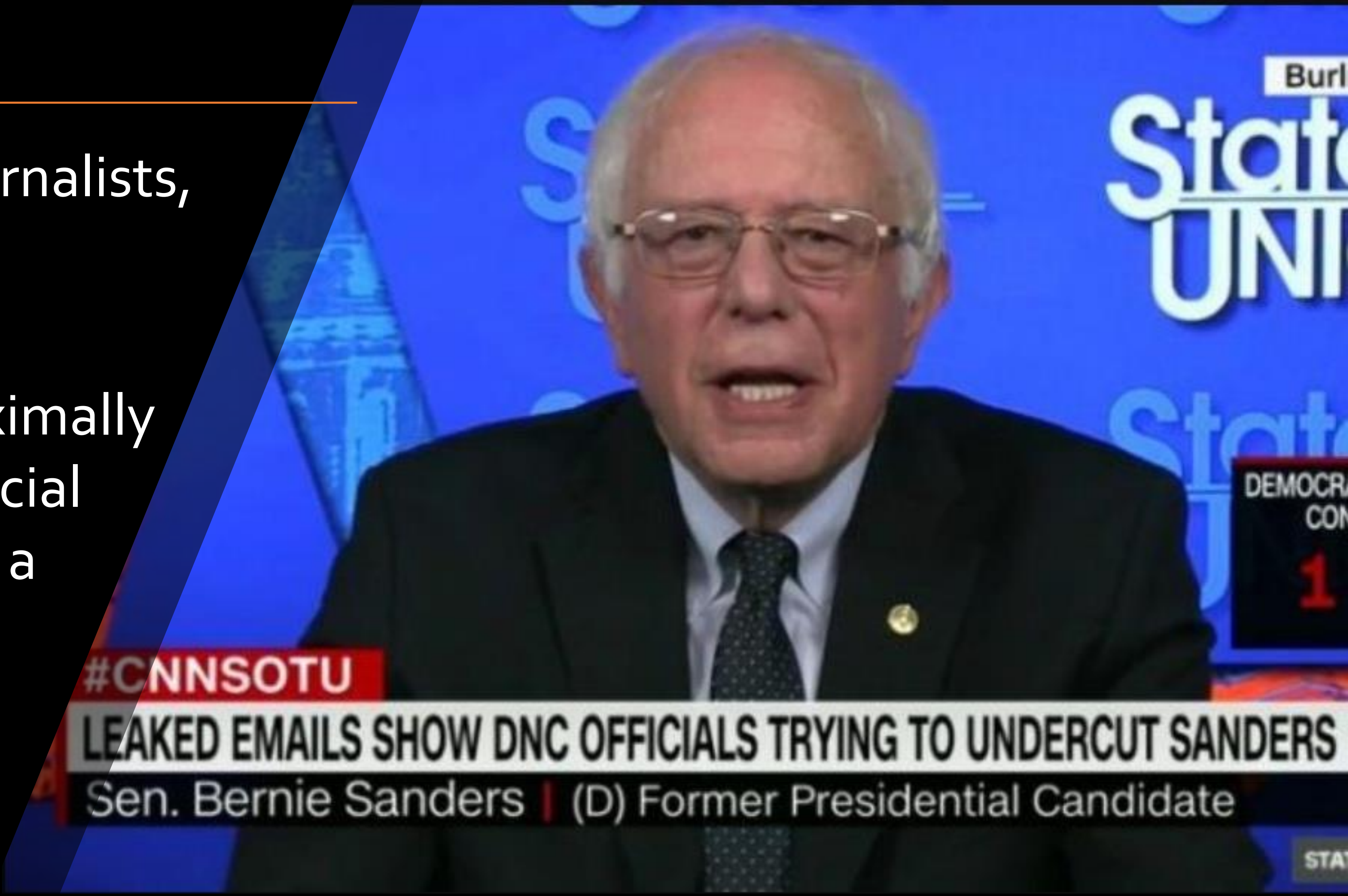
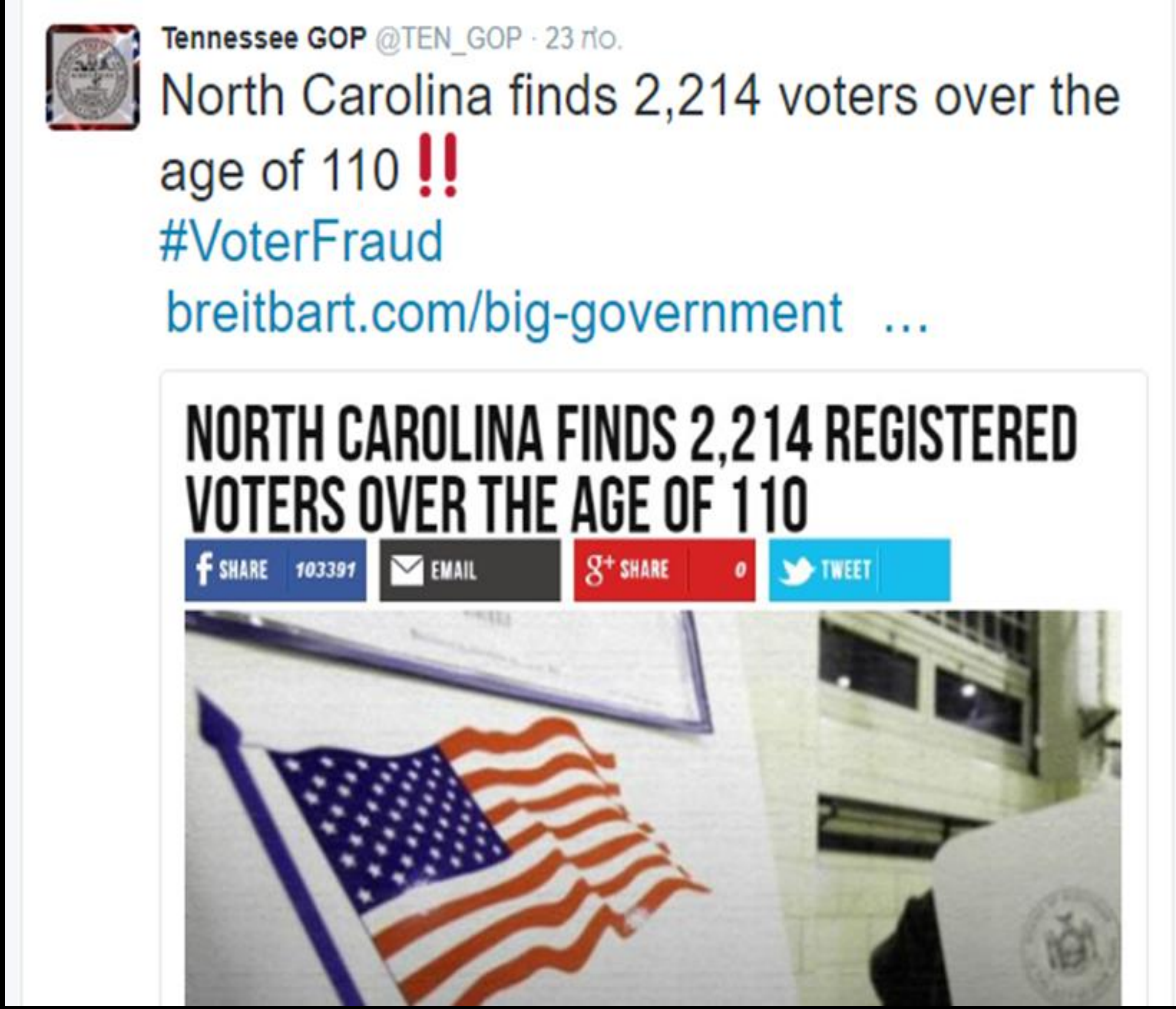

#CNNSOTU
LEAKED EMAILS SHOW DNC OFFICIALS TRYING TO UNDERCUT SANDERS
Sen. Bernie Sanders | (D) Former Presidential Candidate

Image Source: CNN

USA (2016)

- Recon and intrusions in election infrastructure never used

- Narrative of “large scale voter fraud” and “vote rigging” amplified by IRA trolls



Tennessee GOP @TEN_GOP · 23 но.

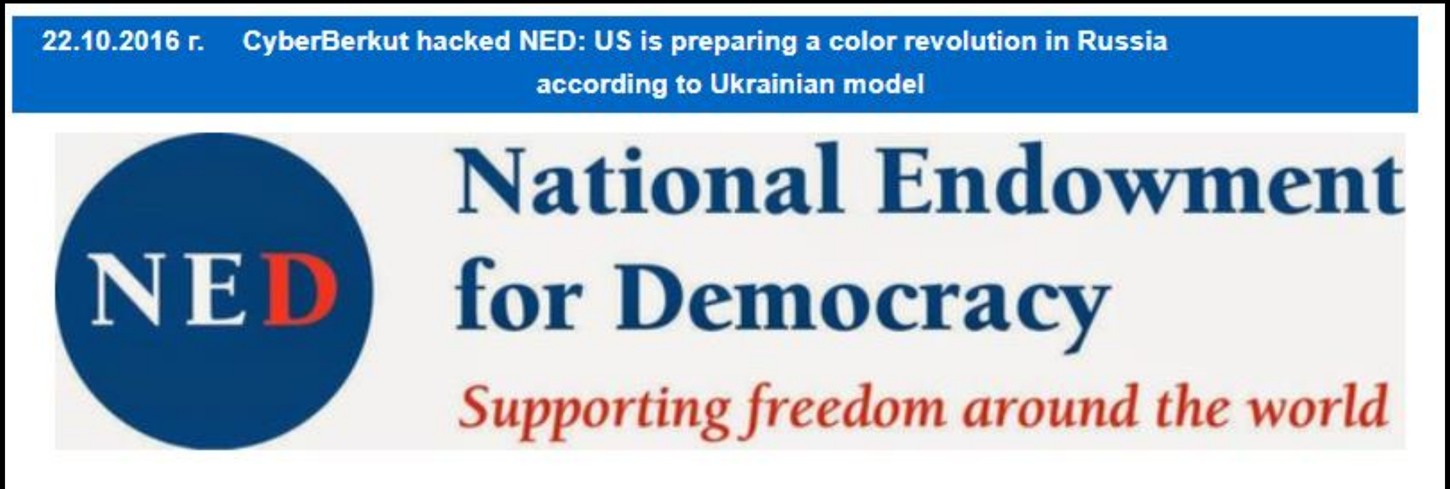
North Carolina finds 2,214 voters over the age of 110 ‼️
#VoterFraud
breitbart.com/big-government …

NORTH CAROLINA FINDS 2,214 REGISTERED VOTERS OVER THE AGE OF 110

Image Source: Internet Archive

USA (2016)

Whataboutism: discrediting critics by charging them with hypocrisy



22.10.2016 г. CyberBerkut hacked NED: US is preparing a color revolution in Russia according to Ukrainian model

NED

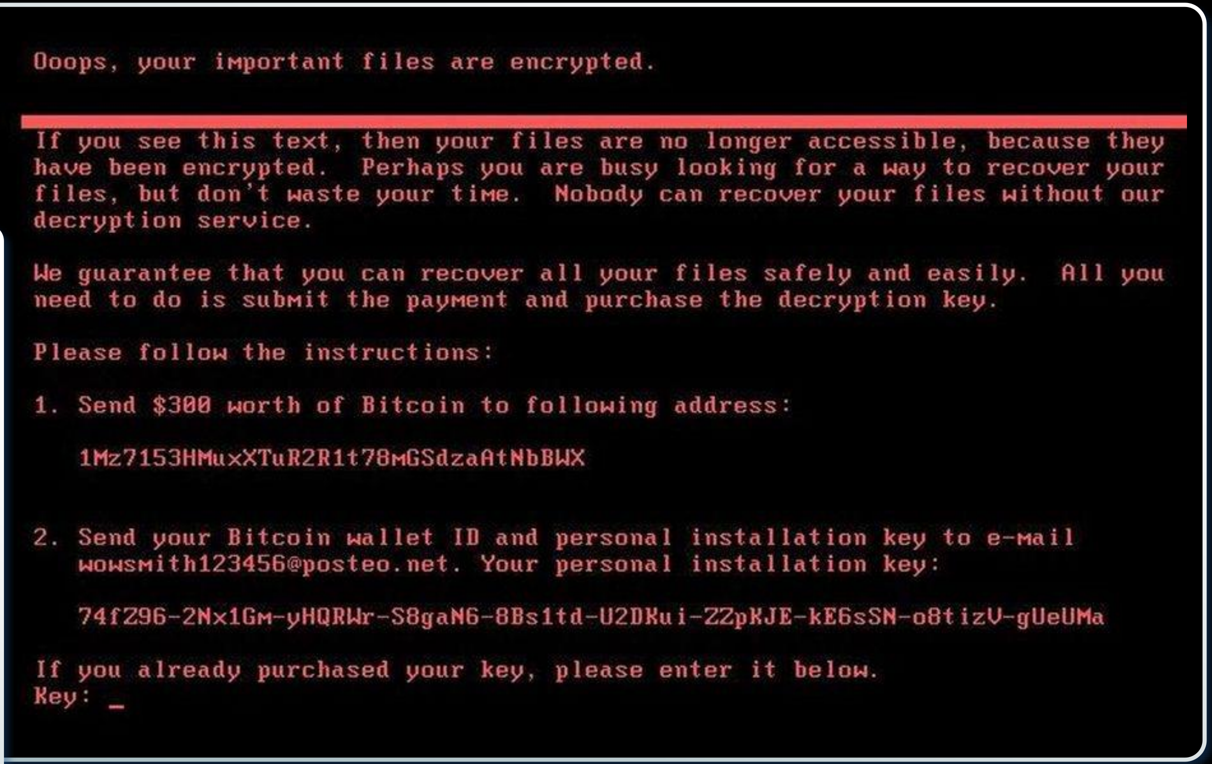
National Endowment for Democracy

Supporting freedom around the world

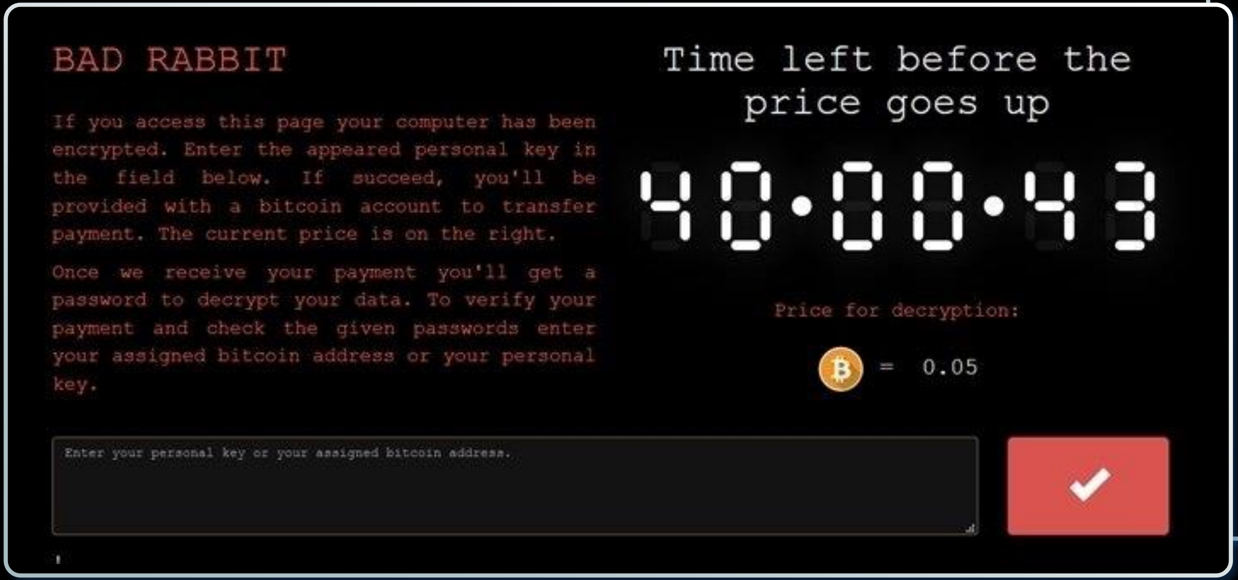
Image Source: DCLeaks, CyberBerkut

Faux-Criminal Ransomware

- Leverage existing narrative of ransomware attacks on state and local governments
- Disable election infrastructure



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74fZ96-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```



BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

40·00·43

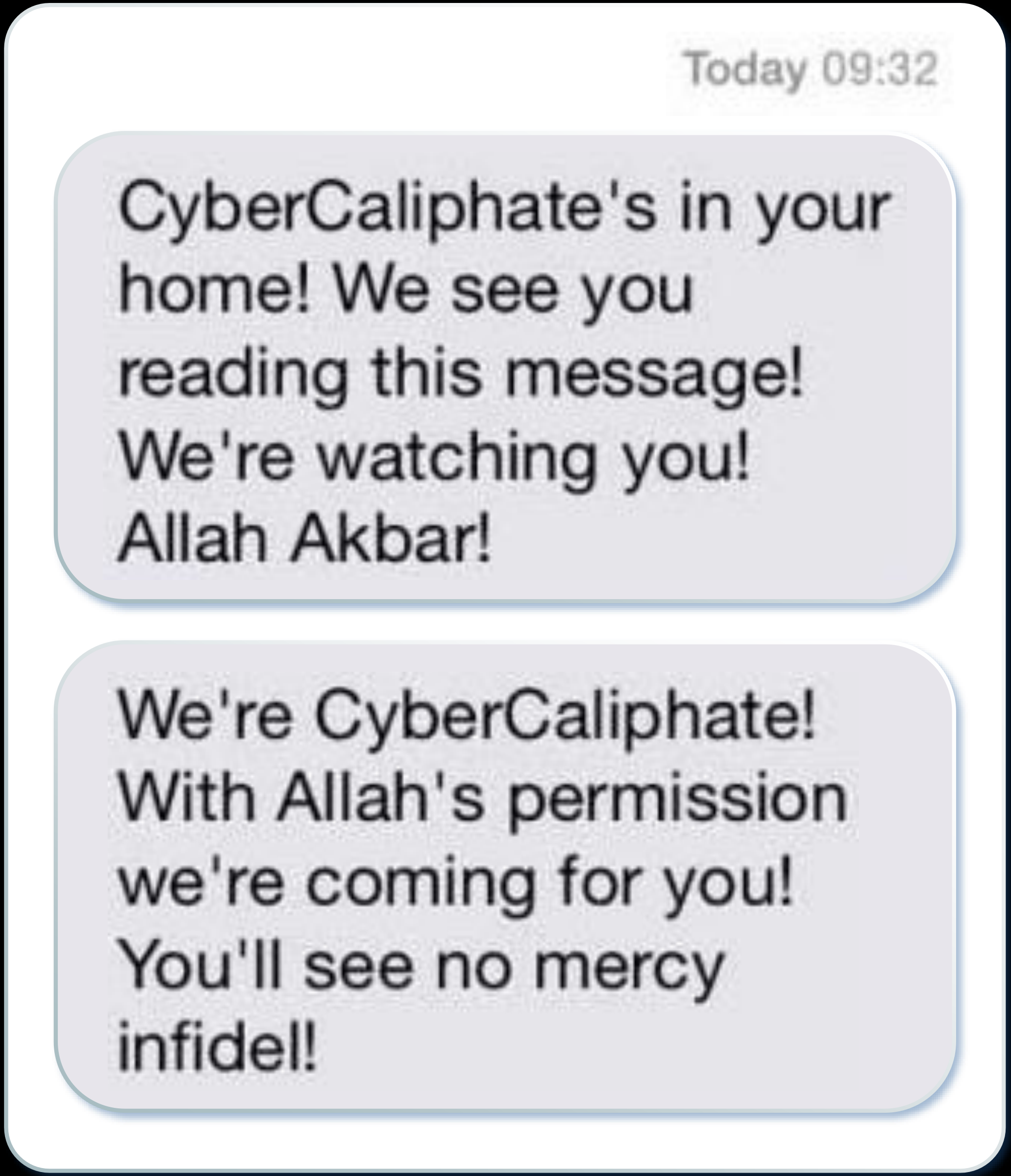
Price for decryption:

₿ = 0.05

Enter your personal key or your assigned bitcoin address.

Push Alert System Abuse

Hijack trusted sources to disseminate disinformation



Today 09:32

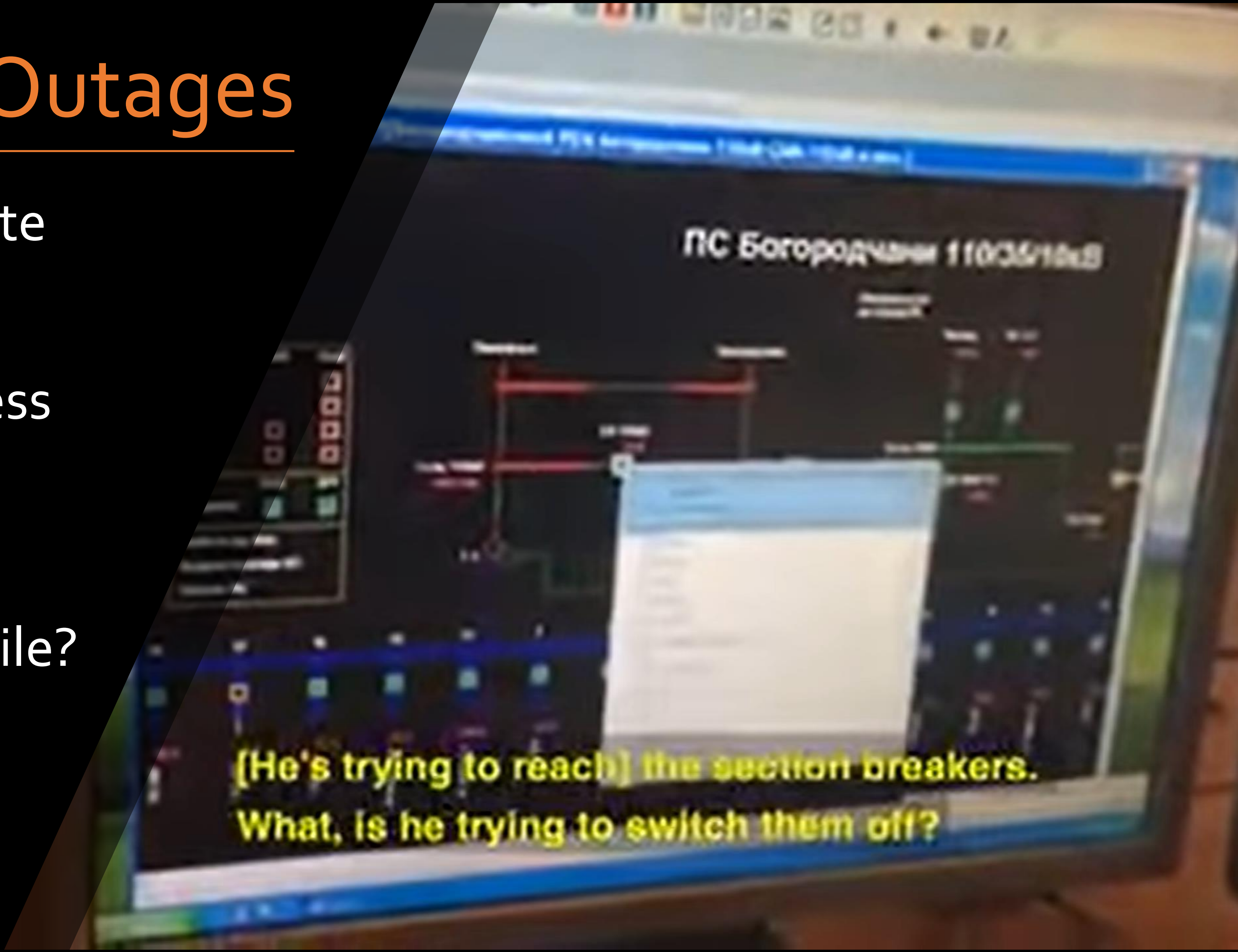
CyberCaliphate's in your home! We see you reading this message! We're watching you! Allah Akbar!

We're CyberCaliphate! With Allah's permission we're coming for you! You'll see no mercy infidel!

Image Source: WBOR (2015)

Limited Power Outages

- Hinder the ability to vote
- Exacerbate voting access concerns
- Cost / benefit worthwhile?



[He's trying to reach] the section breakers.
What, is he trying to switch them off?

Image Source: Wired

Consider Your Informational Utility

Organizational profile shapes utility to adversaries

Location

Function

Relationships

Data

Reputation

Digital Resources

Consider Your Informational Context

Informational adversaries leverage confirmation bias phenomenon

- Rumors & Conspiracy
- News and Social Media Narratives
- Stereotypes and Cultural Biases

Learn From Operations Against "Accepted" Targets

Cyber and information conflict actors often first use tactics internally and against historic opponents

Sound Bytes

- Election interference isn’t just about changing election outcomes
- Attackers maximize strategic value of tactics, targets, and timing
- Strategic opponents demand strategic defenses

Nate Beach-Westmoreland

@NateBeachW