CASE STUDY – RUSSIAN ATTACK ON 2016 PRESIDENTIAL ELECTION

1

Session Objectives

- Examine the use of political informatics to influence the results of the 2016 US Presidential election
- Analyze the concepts of social media, microtargeting, and election security in the context of an actual election

2

References

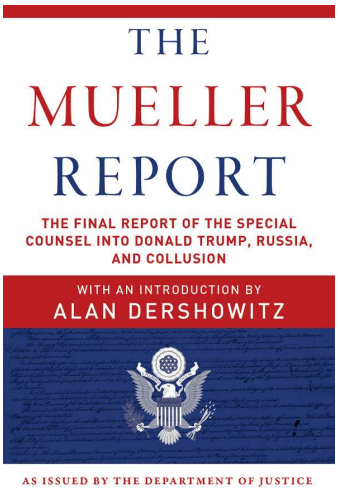
- Assessing Russian Activities and Intentions in Recent US Elections, National Intelligence Council, January 6, 2017
- #Digital Deceit: The Technologies Behind Precision Propaganda on the Internet, Harvard Kennedy School on Media, Politics, and Public Policy, January, 2018
- The Plot to Hack America, Malcolm Nance, Skyhorse Publishing, October 10, 2016, ISBN-13: 978-1510723320
- Indictment – USA v. Internet Research Agency, February 16, 2018
- Commanding the Trend: Social Media as Information Warfare, Jarred Prier, Strategic Studies Quarterly, Winter 2017, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf
- NSA Directive (unclassified summary), https://assets.documentcloud.org/documents/3766950/NSA-Report-on-Russia-Spearphishing.pdf
- Barr Report, https://www.nytimes.com/interactive/2019/03/24/us/politics/barr-letter-mueller-report.html
- House Permanent Select Committee on Intelligence, https://intelligence.house.gov/social-media-content/

3

Major Information Sources

- 2016 Election Results Assessment – 1/6/17
- Mueller indictment of IRA – 2/16/18
- Worldwide Threat Assessment
  - Released 1/29/19
  - Associated briefing to the Senate Intelligence Committee
- Barr Report – 3/24/19
- Mueller Report – 4/18/19

Unless attributed elsewhere, quotes in the slides are taken from the Mueller Report



4

© Robert F. Kelly, 2026

2016 Election Results

- Donald Trump wins US Presidential election, despite receiving 2.8M fewer overall votes than Hillary Clinton
- Margin of victory in US electoral College resulted from 79,646 votes in 3 states

Image: CNN

5

© Robert F. Kelly, 2026

2016 Election Results Assessment (1/6/17)

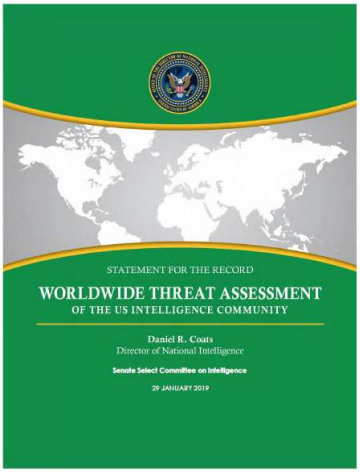
- US intelligence agencies made no assessment of the impact that Russian activities had on the election results
- Ordered by Russian President Vladimir Putin
- Russian efforts consistent with efforts to undermine US-led democratic order
- Russian goals
  - Undermine public faith in US democratic process
  - Denigrate Hillary Clinton, harming her electability and potential presidency
  - Preference for Donald Trump

Note: Russian aims were furthered by the attack, independent of which candidate won the 2016 election

6

Worldwide Threat Assessment

- "Russia's social media efforts will continue to focus on aggravating social and racial tensions."
- "Adversaries and strategic competitors probably will attempt to use deep fakes or similar machine learning technologies to create convincing – but false- image, audio, and video files to augment influence campaigns directed against the US and our allies and partners'"



7

Scope of Special Counsel

- "authorized to conduct the investigation confirmed by then-FBI Director James B. Comey in testimony before the House Permanent Select Committee on Intelligence on March 20, 2017, including:
  - Any links and/or coordination between the Russian government and individuals associated with the campaign of President Donald Trump; and
  - Any matters that arose or may arise directly for the investigation; and
  - Any other matters within the scope of 28 C.F.R. 600.4(a).

Image: time.com

8

© Robert F. Kelly, 2026

Scope of Investigation

- "Office
  - issued more than 2,800 subpoenas under the auspices of a grand jury sitting in the District of Columbia;
  - executed nearly 500 search-and-seizure warrants;
  - obtained more than 230 orders for communications records under 18 U.S.C. § 2703(d);
  - obtained almost 50 orders authorizing use of pen registers;
  - made 13 requests to foreign governments pursuant to Mutual Legal Assistance Treaties; and
  - interviewed approximately 500 witnesses, including almost 80 before a grand jury."

Pen register - A device (or SW) which records or decodes electronic or other impulses which identify the numbers called or otherwise transmitted on the telephone line to which such device is dedicated

9

© Robert F. Kelly, 2026

Findings

- Barr Report summarized findings of the Mueller special investigation into Russian interference in the 2016 election
  - Russian interference – Russian government actors hacked into computers and conducted disinformation and social media operations aimed to interfere with election
  - Conspiracy – "investigation did not establish that members of the Trump Campaign conspired or coordinated with the Russian government in its election interference activities"
  - Obstruction of justice – no prosecutorial judgement
- Major conclusions of Mueller Report concerning Russian activities
  - "numerous links between individuals with ties to the Russian government and individuals associated with the Trump campaign"
  - "evidence not sufficient to support criminal charges"

10

© Robert F. Kelly, 2026

General Background

- Some concerns with the US voting systems following the 2000 Presidential election
- Limited coordinated attempt to modernize/update US voting systems
- Voter suppression efforts
- Partisan disputes of voter eligibility
- Questions of legitimacy of voter registration data
- Proposed voter ID laws

11

© Robert F. Kelly, 2026

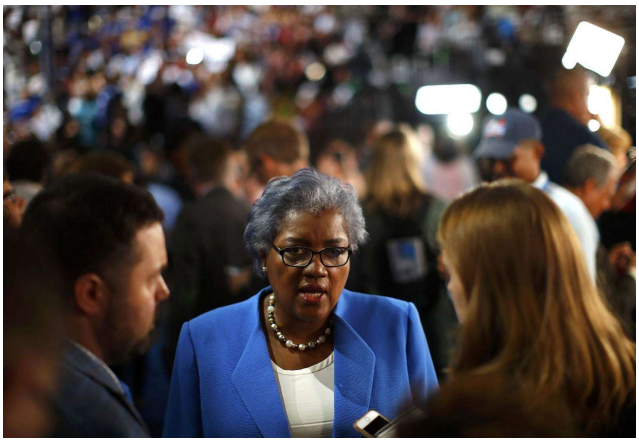
Relevant Laws

- Illegal for foreign nationals and foreign governments to make contributions or spend money to influence an election
- Bars agents of any foreign entity from engaging in political activities without registering with the US Attorney General

12

DNC

- Democratic National Committee
- Early subject of attack
- Coordinates strategy to support Democratic election candidates
- Private political organization (not a government agency)
- Protected only by private IT staff (not subject to NSA/FBI cyber protection)
- Infosec Institute tests revealed massive security flaws



13

Scope of Russian Attack on DNC

- Coordinated teams of attackers, reportedly numbering in the hundreds
- Multi-year attack, probably originating in 2014
- "activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations"

14

© Robert F. Kelly, 2026

Timeline

- Fall 2015 – NSA and FBI detect unusual DNC traffic
- Spring 2016 – Hack detected at DNC, showing massive loss of contributors, opposition research, chats, and e-mails
- Summer 2016 – DNC acknowledges a hack, claimed by Guccifer 2.0, who states he leaked DNC e-mails to WikiLeaks
- Summer 2016 – Spear-phishing attack on DCCC
- Summer-Fall 2016– documents released at the start of the Democratic National Convention
- 1/17/17 – US National Intelligence Council Report states "We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election."
- 2/16/18 – Indictment against Russian connected individuals

15

© Robert F. Kelly, 2026

Attack Participants

- Bears - security term for various Russian intelligence affiliated organizations
- Internet Research Agency – Putin affiliated organization
- Guccifer 2.0 – persona of Russian hackers
- DC Leaks – Publishes leaked e-mail messages (linked to Fancy Bear)
- WikiLeaks – Publisher of leaked documents
- Democratic National Committee (DNC) – political arm of Democratic Party
- CrowdStrike – Internet security company

16

© Robert F. Kelly, 2026

RT

- Formerly Russia Today
- Media arm of the Russian government
- Paid American contrarians (e.g., Michael Flynn and Jill Stein) at RT dinner
- Themes
  - Criticism of western governments
  - Promotion of radical dissent
  - Promotion of alternate US parties
  - Change of US system through revolution
  - Anti-fracking

12/2015 dinner celebrating 10th birthday of RT

Image: NBC News

Michael Flynn pleaded guilty to lying to FBI, pardoned, then settled for 1.25M – plus more to come

17

© Robert F. Kelly, 2026

CrowdStrike

- American cyber security company located in Silicon Valley
- Worked counter-measures in several high-profile cyber-attacks
- Identified details of the attack on the DNC
- Valuation over $1B

CROWDSTRIKE

18

Russian Attack Targets

1. Email and document servers
2. Voter rolls
3. Social media

We introduce these political targets now and explore in more detail later

19

Coordination, Not Conspiracy

- "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing"
- Within 5 hours,
  - GRU officers targeted for the first time Clinton's personal office
  - Unit 26165 created and sent malicious links targeting 15 email accounts
  - No evidence found of earlier penetration attempts
  - Not clear how GRU able to identify these non-public accounts

Image: Yahoo! News

20

Email and Document Attacks

Image: Macaws Infotech

21

Cyber War Attackers

- Cyber Bears are Russian hack groups allied with Russian intelligence, but operating independently
- Advanced Persistent Threats (APTs) are usually
  - nation-state actors because of the size and scope of their operations
  - associated with malware
- Conducted attacks against other Russian adversaries (e.g., Estonia)
- Relatively easy to identify
- Cyber Bears were referred to by CrowdStrike as:
  - Cozy bear (APT29)
  - Fancy bear (APT28)
  - Venomous bear – 2008 cyber-attack on US CentCom

Cyber bears are described as aligned with Russian organized crime

22

© Robert F. Kelly, 2026

Attack Components

- In July 2015, Russian Intelligence gained access to DNC networks and maintained access until at least June 2016
- GRU (General Staff Main Intelligence Directorate) began cyber operations on the US election by March 2016
- GRU operations resulted in the compromise of personal e-mail accounts of Democratic Party officials and political figures
- By May 2016, GRU exfiltrated large volumes of data from the DNC
- GRU used the Guccifer 2.0 persona, DCLeaks, and WikiLeaks to release US victim data (also used media outlets)
- Spring 2016 – Clinton campaign chairman, John Podesta, was victimized by a spear-phishing attack, and inadvertently disclosed his e-mail password

Actions and dates taken from 1/17 Intel Report

23

© Robert F. Kelly, 2026

Intrusion into DCCC and DNC Networks

- Access to DCCC used credentials stolen from an employee
- Compromised 29 computers on the DCCC network
- Gained access to a DNC network via a VPN from DCCC
- More than 30 computers on DNC network were compromised
- Installed malware on DNC and DCCC networks
  - Credential harvesting tool
  - Tool to compile and compress info for exfiltration
  - Logged keystrokes, took screenshots, and gathered other info
  - Activity of malware controlled by at least 2 sets of GRU-controlled computers

The Arizona based “AMS Panel” served as the nerve center through which GRU officers monitored and directed the malware

24

© Robert F. Kelly, 2026

Russian Hacking

- Mueller Report refers to the Russian hacking units as Military Units (not referred to by Bear designation)
- Unit 26165 – GRU cyber unit dedicated to targeting organizations outside of Russia
  - Develops malware, Spearphishing and bitcoin mining
- Unit 74455
  - Release of documents stolen by Unit 26165
  - Promotion of document releases
  - Publication of anti-Clinton content on social media accounts
  - Hacking into state computers and US companies

Bitcoins used to purchase computer infrastructure and in hacking operations

25

© Robert F. Kelly, 2026

Nature of Stolen Material

- Truly negative material, for example
  - Strategies that should be neutral, but favor one candidate
  - Disparaging remarks about some candidates
- Material that suggests wrongdoings, but contains little actual damaging information
  - Example – Hillary e-mail references
- Innocuous material that could be twisted to suggest wrongdoing
  - Example Cheese Pizza = Child Pornography

Items 2 and 3 require attackers to suggest negative views of otherwise neutral information

26

Public Release of Stolen Documents

- Effective use of stolen material requires
  - Analysis of content for damaging material
  - Use of a cutout (third party, used to distance the release from the attackers)
- Timed release - aligned with events in 2016 election campaigns
  - Timed for maximum election effect
  - The degree of coordination with people inside the US is unknown
- Released through
  - Guccifer 2.0
  - WikiLeaks
  - DCLeaks
  - RT

27

Dissemination of Hacked Materials

- Released initially through DCLeaks and Guccifer 2.0
- Later released through WikiLeaks
- DCLeaks (dcleaks.com)
  - Registered in April 2016 through a service that anonymized the registrant
  - Paid for using a pool of bitcoins mined by the GRU
  - Landing page enabled easy access to the material
  - Some pages password protected to control timing of released info
  - GRU used Facebook, Twitter, and a Gmail account to communicate privately with reporters to give them early access to archives of leaked material

28

© Robert F. Kelly, 2026

Guccifer 2.0

- Persona (i.e., façade) of group that hacked the DNC
- Assessed as being created by Russian intelligence services to cover for interference in 2016 election
- Self-reported as Romanian
- Name refers to Gucccifer
  - Marcel Lazar Lehel
  - Romanian hacker responsible for some US attacks
- Twitter briefly suspends Guccifer 2.0 account in August 2016

"we assess with high confidence that Russian military intelligence used the Guccifer 2.0 persona and DCLeaks.com to release US victim data" – 1/17 intel report

29

© Robert F. Kelly, 2026

WikiLeaks

- Founded in 2006 by Julian Assange – hacker who penetrated secure networks
- Outlet for leaked documents
- Assange jailed (5 years), and released in 2024
- "GRU and WikiLeaks sought to hide their communications" indications of encryption between organizations
- Stolen documents transferred from GRU to WikiLeaks using a method redacted in Mueller Report
- Subsequently, GRU transmitted documents to WikiLeaks
- PGP used to encrypt some files

Image: Daily Beast

30

Attack on Voter Rolls

Image: Kelly Minars/Flickr

31

Attacker Goals

- Cause voting disruptions
- Delegitimize the voting process
- Create concerns of voter fraud

"types of systems Russian actors targeted or compromised were not involved in vote tallying" - 1/17 Intelligence Report

32

© Robert F. Kelly, 2026

Actions

Appears that the intent of the August 2016 attack was to obtain info useful in later spear phishing attacks

- "Since early 2014, Russian intelligence accessed elements of multiple state or local electoral boards"
- "Since early 2014, Russian intelligence has researched US electoral processes and related technology and equipment"
- Successful attack on Illinois voter registration (personal data on 200,000 voters)
- Cyber-attack in August 2016 against a US company to obtain information on election HW/SW
  - Resulted in a voter registration themed spear-phishing campaign targeting local US government organizations
- October 2016, attackers offered election-related products and services
- Attackers sent test e-mails, testing attacks against absentee ballot system

Results of the 2016 attack unknown, but likely resulted in at least one compromised system

33

© Robert F. Kelly, 2026

Potential Voter Registration Attacks

- Many state voter registration DBs are on-line
  - E.g., - electronic poll books (used to check voters in)
  - NSA document refers to a company that makes electronic poll books
- Possible attack strategies
  - Disrupt the electoral process
  - Names could be deleted from the voter rolls
  - Changes to voter roll data are possible

34

Social Media Attacks

Image: SecurityZap.com

35

Attack Goals

- Weaponize stolen information by routing it to selected groups and amplifying it
- Create chaos through the distribution of false information
- Target people within a society, influencing their beliefs and behaviors
- Reduce trust in US government
- Increase chaos
- Discredit public and private institutions

36

© Robert F. Kelly, 2026

Bots and Trolls

- Trolls – Humans who generate fake news stories, e-mails, messages, etc.
- Bots (software robot or web robot) – software app that runs automated tasks over the internet

Image: Valentina Kulagina, 1930

37

© Robert F. Kelly, 2026

Attack Strategies

- Access streams of online information to influence networked groups
  - Inserted propaganda must fit the narrative of the networked group (e.g., Clinton Foundation or Benghazi)
- Use the trend mechanism in social media (mainly Twitter)
  - Insert propaganda into a social media platform
  - Using bots, create a trend
  - Social media users will notice the trend and further increase the awareness of the trend
- Combination of 1 and 2

Twitter estimated that 15% of its accounts were bots

If the topic is successfully trending, the propaganda is sometimes continued in mainstream media

38

© Robert F. Kelly, 2026

Social Media Trending

- Social media sites use an algorithm to analyze text to create a list of popular topics
- Trend Attack Methods
  - Trend distribution – apply a message (propaganda) to every trending topic
  - Trend hijacking – taking over a trending topic through the use of bots
  - Trend creation – amplifying a propaganda topic with bots
- Bots are programmed to
  - Tweet at various intervals
  - Respond to certain words
  - Retweet when directed by a master account

Twitter launched a "bot purge" following the 2/16/18 indictment of IRA officials
Other purges since early 2018

39

© Robert F. Kelly, 2026

Russian Social Media Campaign

- Conducted by the Internet Research Agency (IRA)
- Funded by Yevgeniy Prigozhin
- Mid 2014 – sent IRA employees to the US for intelligence gathering
- Used social media accounts and interest groups to sow discord in the US through what it termed "information warfare"
- By early 2016 it favored Trump and targeted Clinton
- No evidence that any US persons conspired or coordinated with the IRA

Prigozhin killed in a plane crash in 2023 after leading a failed mutiny

40

© Robert F. Kelly, 2026

Internet Research Agency (IRA)

- Troll farm with main location in St. Petersburg, Russia
- Reportedly employs 600 people across Russia
- Ex-employees and indictment reported tasks
  - Fake social media accounts (Facebook, Twitter, Instagram, YouTube)
  - Use stolen identities to post on social media
  - Circulate pro-Kremlin propaganda
  - Spread derogatory information about Russian opponents
- Likely financed by a former Putin ally (Yevgeny Prigozhin), now deceased, with ties to Russian intelligence services
- Defendants travelled to US and procured US infrastructure to hide Russian origin of work
- Departments – graphics, data analysis, search engine optimization, IT, and finance

41

© Robert F. Kelly, 2026

IRA Social Media Attacks

- Specialists impersonated US people in bogus accounts
- Sensitive to US work times and holidays
- Supported radical groups oppositional social movements
- Increased dissatisfaction with social and economic situation
- Many created groups had hundreds of thousands of followers:
  - Secured borders
  - Blacktivist – Organized Baltimore rally to mark death of Freddie Gray
  - South united
  - Heart of Texas – Promotes Texas secession
  - United Muslims of America
  - Tennessee GOP (@TEN_GOP) – 100,000 followers

42

Example – Creating Social Unrest

- Houston, May, 2016
- One group protested the threat of radical Islam, while a larger group of counter-protestors gathered nearby
- Both groups were organized by IRA attackers

"130 rallies were promoted by 13 Russian pages, which reached 126 million Americans with provocative content on race, guns, immigration and other volatile issues" – NYT, 2/18/18

43

Example - Twitter / WikiLeaks

- 7/23/16 – Trump tweeted "The WikiLeaks e-mail release today was so bad to Sanders that it will make it impossible for him to support her, unless he is a fraud"
- Assange immediately replied to the Trump tweet and linked to the DNC document cache, with the message "everyone can see for themselves"

44

© Robert F. Kelly, 2026

Disinformation Campaign

- 9/17 disclosure by Facebook that it sold $100K in ads to Russian troll farm (3,300 ads)
- Ads
  - Named Trump and Clinton
  - Focused on amplifying dissent (LGBT, race, immigration, fun rights) and directed at people interested in the subjects
  - Targeted geographically and to people susceptible to political messaging
- 2/18 indictment of IRA revealed details of campaign

Huge ethical conflict for Facebook (and other social media organizations)

45

© Robert F. Kelly, 2026

IRA Activities

- IRA infrastructure
  - Purchased space on US servers
  - VPNs connect Russian servers to US servers to mask activities - opening accounts, communicating with US persons, and accessing social media accounts
  - Registered and controlled hundreds of Web-based email accounts to appear to be US-based
- IRA used stolen or forged identities
  - Opened accounts at PayPal
  - Created false identification (e.g., driver's license)
  - Used fake identities for social media posts
  - Maintained accounts and purchased ads on social media

46

2/18 Indictment Charges

- Staged political rallies inside US
- IRA employees posed as US grassroots entities and US persons, and
  - Solicited and compensated US persons to promote or disparage candidates
  - "Communicated with unwitting individuals associated with the Trump Campaign and with other political activists to seek to coordinate political activity"

47

IRA Campaign

- IRA targeted US as early as 2014 – traveled to US to gather information and photos used in social media posts
- Used fictitious US personas initially, later added groups (e.g., @TEN_GOP)
- Operated social media accounts designed to attract US audiences – falsely claiming to be controlled by US activists

Image: Twitter

48

IRA Rally Example

- Poster created by IRA and included in the Mueller Report
- Image of a coal miner who had died of complications of black lung disease
- Photo taken without permission from either the family or the photographer

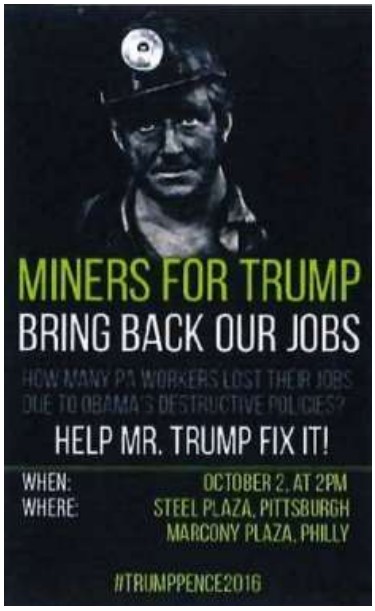


Image: NPR

49

Scope

- By the end of the 2016 election, IRA had the ability to reach millions of US persons through their social media accounts
- IRA controlled social media accounts had hundreds of thousands of US participants; similar Twitter accounts had tens of thousands of followers

Image: Twitter

50

© Robert F. Kelly, 2026

Power of Social Media Campaign

- US political figures retweeted IRA-created content
  - Former Ambassador Michael McFaul
  - Roger Stone
  - Sean Hannity
  - Michael Flynn Jr.

Sean Hannity had over 4 million Twitter followers

Image: Politico

51

© Robert F. Kelly, 2026

Social Media Companies

- Facebook identified
  - 470 IRA controlled Facebook accounts
  - 80,000 posts between 1/15 and 8/17
  - Over 3,500 purchased ads ($100,000)
  - Reached 126 million persons (29 million through direct contact)
- Twitter (X)
  - identified 3,814 IRA controlled accounts
  - Notified 1.4M people that they may have been in contact with an IRA-controlled account
  - IRA posted 175,993 tweets from 3,814 accounts in the 10 weeks before the election

"To those people, who hate the Confederate flag. Did you know that the flag and the war wasn't about slavery, it was all about money." The tweet received over 40,000 responses. @Jenn_Abrams 4/24/17 (2:37 p.m.) Tweet

52

Data Access

- Download at least one of the compressed files containing Russian social media advertisements from https://intelligence.house.gov/social-media-content/social-media-advertisements.htm

PAGE REMOVED

- Read a minimum of 10 ads and be prepared to discuss aspects of the ads you read, including expected goal

Social media ads currently not available to public

Ad ID	782
Ad Text	Brendan Carter decided to pay a visit to his sick uncle and was held by officers in a public RTS bus station in Rochester, New York. Carter said he was at a station waiting for bus. Freeing himself from emotional trauma, Carter decided to hip his soul with music, when he put his headphones on and started to dance. Suddenly, officers approached him and began asking him out of the premises. Apparently he had not committed any crime or violated any order, so he was disturbed and begun to argue with them. Seriously this guy was detained for useless reasons. This is what American police find interest in – unnecessary and useless way of harassing blacks. Very ridiculous. Subscribe to my Channel: https://www.youtube.com/channel/UCSbzPCwUDPvDCR6VRaOcDtg Follow me on Twitter: https://twitter.com/Williams8kalvin
Ad Landing Page	https://www.facebook.com/WilliamsandKalvin/
Ad Targeting	Location: United States Age: 18 - 65+ Placements: News Feed on desktop computers or News Feed on mobile devices People Who Match: People who like Williams&Kalvin, Friends of connections: Friends of people who are connected to Williams&Kalvin
Ad Impressions	760
Ad Clicks	31
Ad Spend	99.78 RUB
Ad Creation Date	03/10/16 01:28:41 AM PST
Ad End Date	03/12/16 01:28:40 AM PST

53

Did We Satisfy the Session Objectives?

- Examine the use of political informatics to influence the results of the 2016 US Presidential election
- Introduce the concepts of social media, microtargeting, and election security in the context of an actual election

54