SEC_RITY IS NOT COMPLETE WITHOUT U!

Roy Campbell

Lecture 2: How cybersecurity affects us all

Infrastructure, finance, news, reputation, fake news, ransomware, cloud hacks.

So you're telling me a Nigerian prince really didn't leave me any money?
STOP | THINK | CONNECT™
www.stopthinkconnect.org
STOP. THINK. CONNECT. When in doubt, throw it out! Avoid clicking on suspicious emails, links & social media posts - even if you know the source.

REACTIONS TO

- Army University Press 2017 Article on Autonomous Weapons
- https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2017/Pros-and-Cons-of-Autonomous-Weapons-Systems/
- Stuart Russells's remarks
- Slaughter bots
- https://www.youtube.com/watch?v=9fa9lVwHHqg
- IEEE Spectrum's response (Jan 2018) https://spectrum.ieee.org/why-you-should-fear-slaughterbots-a-response
- Paul Scharre comment on IEEE paper (Feb 2018) https://www.cnas.org/publications/commentary/debating-slaughterbots-and-the-future-of-autonomous-weapons
- UN conference fails to agree (Dec 21, 2021) https://nypost.com/2021/12/21/terrifying-rise-of-ai-slaughterbots-programmed-to-kill/

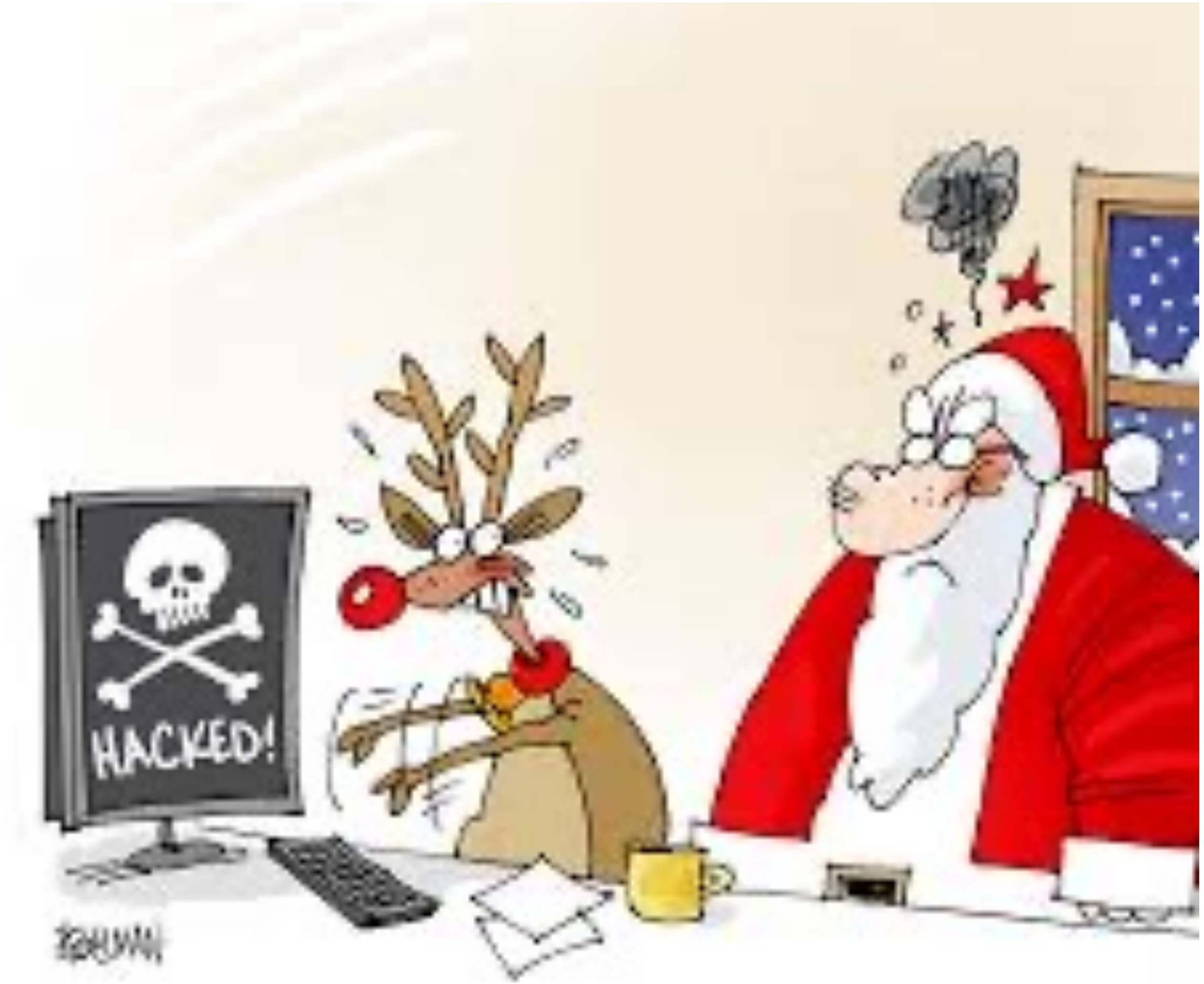
WEEK 2:HOW CYBERSECURITY AFFECTS US ALL

1) Cybersecurity – The broader picture
   a) Infrastructure, Finance, Supply Chains and Denial of Service [5,16]
   b) News, Reputation, Privacy, Disinformation, Fake News, Clicks into Votes [17,42]
2) Encryption [43,47]
3) Russia/Ukraine Cyberwar – Part 2 [48]

"That was a cyberattack? I thought it was the latest Windows update."

1A. INFRASTRUCTURE (ACCORDING TO WIKIPEDIA)

Airports Bridges Broadband Canals Coastal management Critical infrastructure Dams Electricity	Energy Hazardous waste Hospitals Irrigation schemes Levees Lighthouses Parks Pipeline transport	Ports Mass transit Public housing State schools Public spaces Rail Roads Sewage treatment	Sluices Solid waste Telecommunication Utilities Water supply Weirs



Rudolph the red-faced reindeer.

FINANCE- SURVEY OF BANKING INSTITUTIONS

- 57% noted an increase of wire transfer fraud
- 54% experienced destructive attacks
- 41% increase in brokerage account takeover
- 51% attacks that targeted market strategies -- nonpublic market information that can be used to facilitate digital insider trading and front running
- 38% increase of island hopping -- an organization’s information supply chain is commandeered to attack the institution from within its trusted supply chain
- 41% manipulation of time stamps -- evade detection by manipulating time

vmwcb-report-modern-bank-heists-2021.pdf

Sorry but your password
must contain
an uppercase letter,
a number, a haiku,
a gang sign, a hieroglyph
and the blood
of a virgin.

MAJOR TOOLS USED TO ATTACK FINANCIAL ORGANIZATIONS

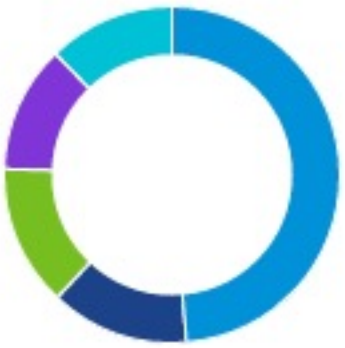


FIGURE 1: The top five malware families found in the last two weeks of January 2021.

- Emotet –a Trojan that mainly spreads through spam emails containing malicious macro-enabled documents or links. Emotet allows criminals to monetize attacks via information stealing, email harvesting, and ransomware distribution.
- 2. Dridex –a banking Trojan that acts as a banking credential stealer, a ransomware delivering system, and a remote access control tool. This threat is often delivered through macro-enabled Office documents attached to emails.
- 3. Trickbot –a threat that targets the financial sector, providing modules that support the theft of banking credentials and cryptocurrency, as well as ransomware. This threat was the target of a takedown initiative in October 2020. Even though the threat infrastructure took a hit, the cybercriminal gang behind it recovered and restarted its activities.
- 4. Qbot –supports a number of modules (from remote access to credential theft. Can observe email threads and inject themselves in existing threads, increasing the chances that a user would deem the corresponding attachment as a legitimate one.
- 5. Hancitor –a delivery mechanism for a plethora of other threats, and it has often used DocuSign documents to entice the victim into activating the email's

"I sent my bank details and Social Security number in an e-mail, but I put 'PRIVATE FINANCIAL INFO' in the subject line so it should be safe."

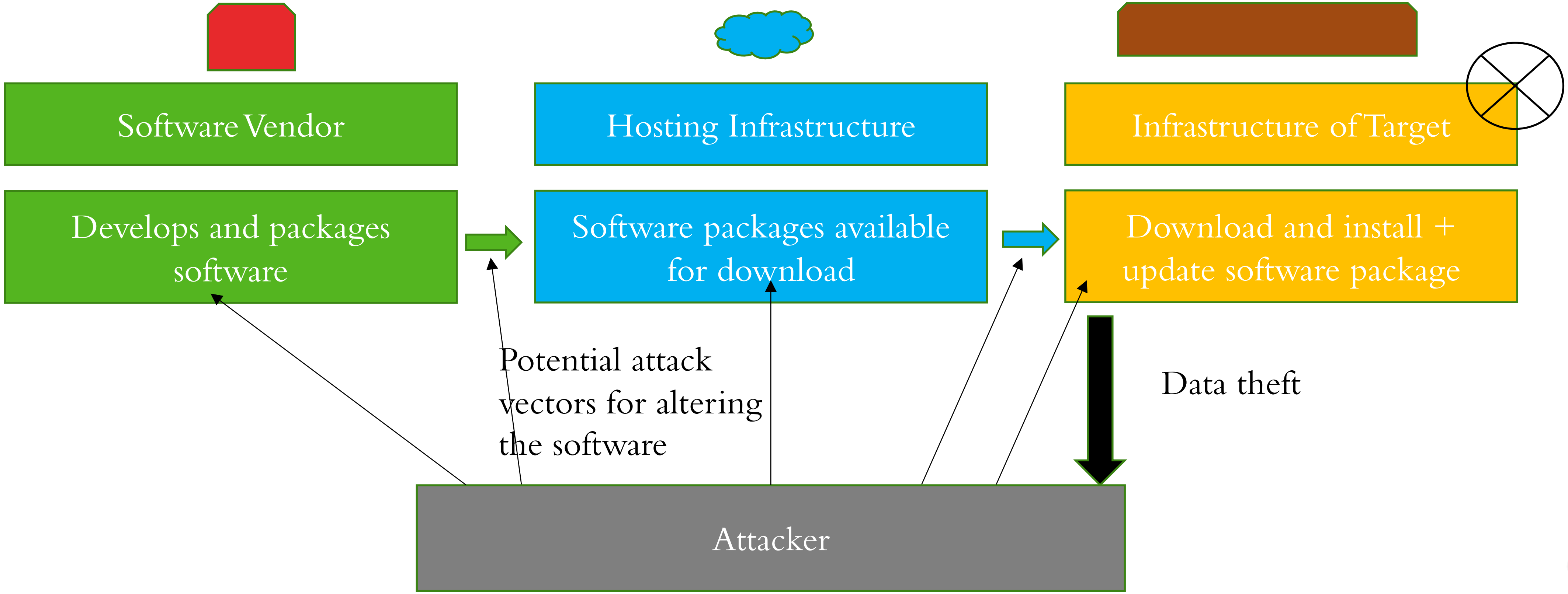
ISLAND HOPPING

- ***Network-based island hopping*** is one of the most frequently used forms of island hopping. With network-based island hopping, attackers infiltrate one network and use it to hop onto an affiliate network. The SolarWinds attack is an example of this stratagem.
- In ***watering-hole attacks***, the adversary hijacks a website or mobile app used for e-finance by customers.
- ***Reverse business email compromise*** (RBEC) attacks occur when a hacker successfully takes over a victim's Office 365 environment and executes fileless malware attacks against the C-suite of the financial institution and the board.
- ***Island hopping as a service***, or access mining, is a tactic where an attacker leverages the footprint and distribution of commodity malware, and uses it to mask a hidden agenda of selling system access to targeted machines on the dark web.

SUPPLY CHAINS

- Compromised software building tools or updated infrastructure.
- Stolen code-sign certificates or signed malicious apps using the identity of developer company.
- Compromised specialized code shipped into hardware or firmware components.
- Pre-installed malware on devices (cameras, USB, phones, etc.)

SUPPLY CHAIN ATTACKS DIAGRAM



Software Vendor

Develops and packages software

Hosting Infrastructure

Software packages available for download

Infrastructure of Target

Download and install + update software package

Potential attack vectors for altering the software

Data theft

Attacker

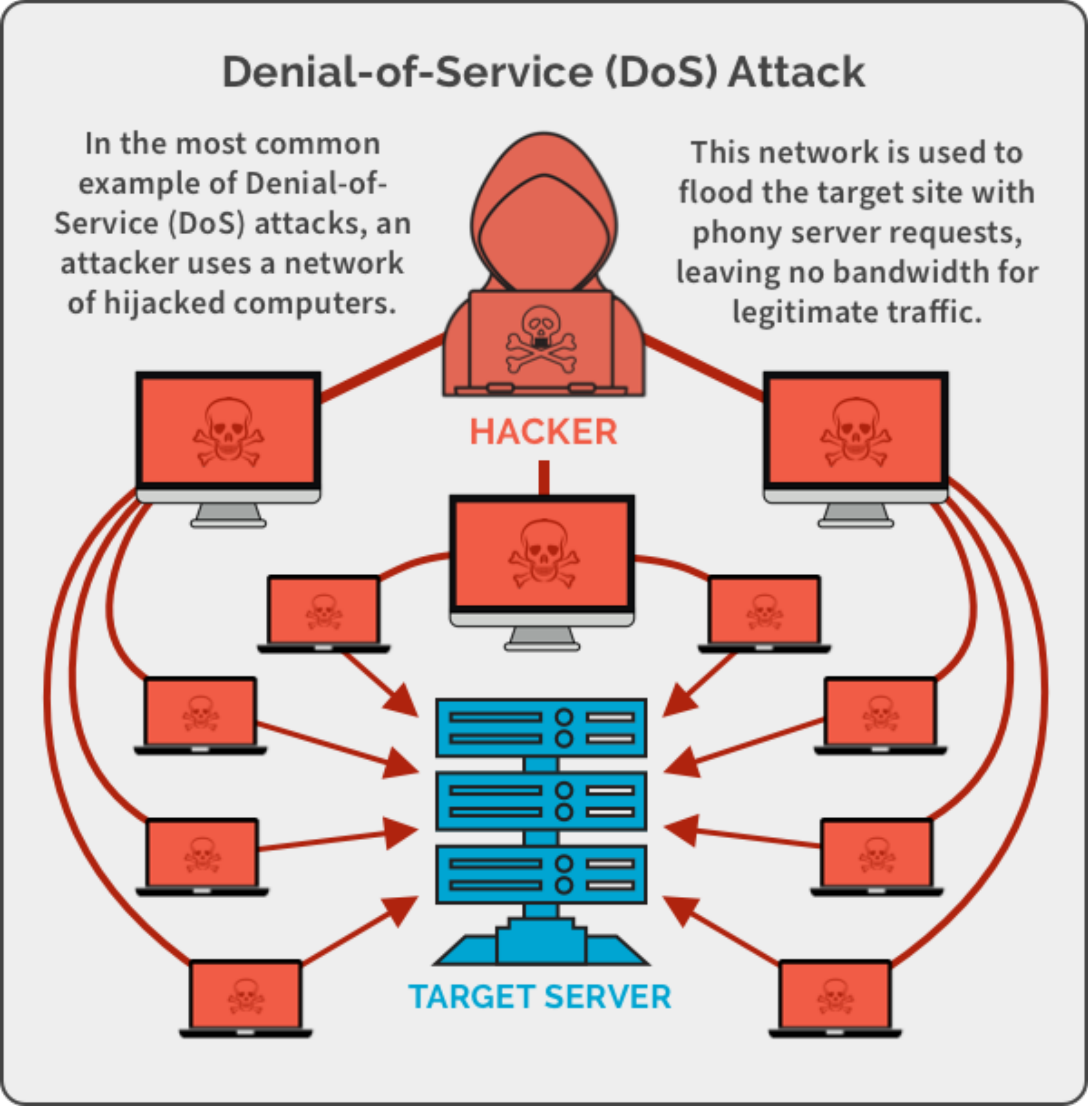
SUPPLY CHAIN ATTACK & EXAMPLES

- A ***supply chain attack*** is a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain.
- Cybercriminals typically tamper with the manufacturing process of a product by installing a rootkit or hardware-based spying components.
- The Target security breach Around 40 million customers credit and debit cards became susceptible to fraud after malware was introduced into the POS system in over 1,800 stores.
- Eastern European ATM malware The malware displays information on how much money is available in every machine and allows an attacker to withdraw 40 notes from the selected cassette of each ATM
- The Stuxnet computer worm are examples of supply chain attacks. The worm specifically targets systems that automate electromechanical processes used to control machinery on factory assembly lines or equipment for separating nuclear material. Introduced into the supply network via an infected USB flash drive

SUPPLY CHAIN CONT.

- ***NotPetya / M.E.Doc*** the financial package "M.E.Doc" used in Ukraine was infected with the NotPetya virus and subsequently downloaded by subscribers. (Ransomeware)
- ***British Airways*** British Airways website payment section contained code that harvested customer payment data. The injected code was written specifically to route credit card information to a website in a domain baways.com
- ***SolarWinds*** Afflicted Windows operating system (OS) hosts were those monitored by the SolarWinds Orion monitoring software.
- ***Microsoft Exchange Server*** In March 2021 more than 20,000 US organizations were compromised though a back door which was installed via flaws in Exchange Server.

  Brian Barrett (6 Mar 2021) China's and Russia's spying spree will take years to unpack


Denial-of-Service (DoS) Attack
In the most common example of Denial-of-Service (DoS) attacks, an attacker uses a network of hijacked computers.
This network is used to flood the target site with phony server requests, leaving no bandwidth for legitimate traffic.
HACKER
TARGET SERVER

DENIAL OF SERVICE

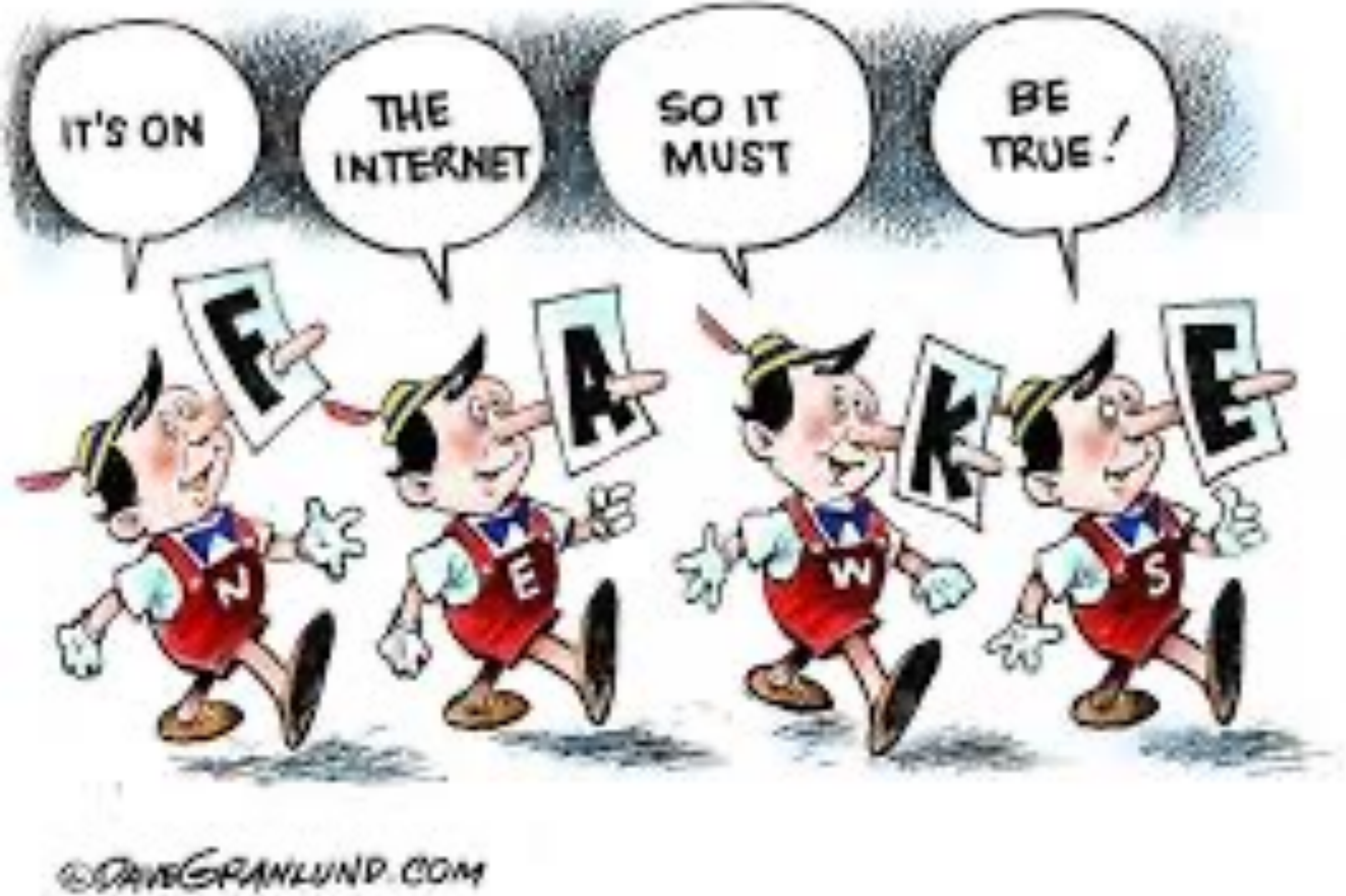
A Denial-of-Service (DoS) attack is ***an attack meant to shut down a machine or network, making it inaccessible to its intended users***. ... Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organization

1B) NEWS – CYBERATTACKS –SEE ALSO FAKE NEWS

52% of news media companies Newscycle Solutions canvassed were either hacked or suffered a data breach from the beginning of 2014.

Although the two most common types of reported cyber-attack involved phishing (59%) and malware (51%) it was the 49% of Distributed Denial of Service (DDoS) attacks by so-called hacktivists that are said to have posed a particular concern. They have attempted to take over media websites for political purposes.

www.guardian.com


IT'S ON
THE INTERNET
SO IT MUST
BE TRUE!
F
A
K
E
N
E
W
S
©DAVEGRANLUND.COM

REPUTATION

- Capital One, for example, which recently suffered a data breach involving 100 million customers in the US and Canada and issued a statement confirming the likely costs to its business of dealing with the incident would be around US$100-US$150 million to pay for customer notifications, credit monitoring, technology costs, and legal support.

- Some companies in the Pentland Analytics report showed a fall of 25% in their market value over the year following an attack.

- https://www.aon.com/reputation-risk-cyber-social-media-pentland-analytics-aon/index.html

PRIVACY AND K-ANONYMITY

(1) Identified:

- Unique identifiers, such as ID numbers, names, social security numbers, phone numbers, or other information, that point to a specific individual.

(2) Re-identifiable (also called pseudonymous or linkable):

- Information that matches the user with some other information that is uniquely tied to the individual. E.g. medical records (Sweeney 2002) and movie ratings.

(3) Anonymous:

The user information available is insufficient for re-identification, no matter what inference is performed. When it is shown to be insufficient to limit the set of identities to a set of less than k elements, the term k-anonymous is used (Sweeney 2002).

Latanya Sweeney. 2002. k-anonymity: A model for protecting privacy. Int. J. Uncertain., Fuzz. Knowl.-Based Syst. 10, 05 (2002), 557–570.

FAKE
NEWS

FAKE NEWS

Fake news is the promotion and propagation of news articles via social media. These articles are promoted in such a way that they appear to be spread by other users, as opposed to being paid-for advertising. The news stories distributed are designed to influence or manipulate users' opinions on a certain topic towards certain objectives.

For example, by manipulating the balance of how a particular topic is reported (whether that concerns politics, foreign affairs, or something more commercial), the views on that topic can be changed. This can be done either with inaccurate facts or with accurate ones twisted to favor a particular view or side.

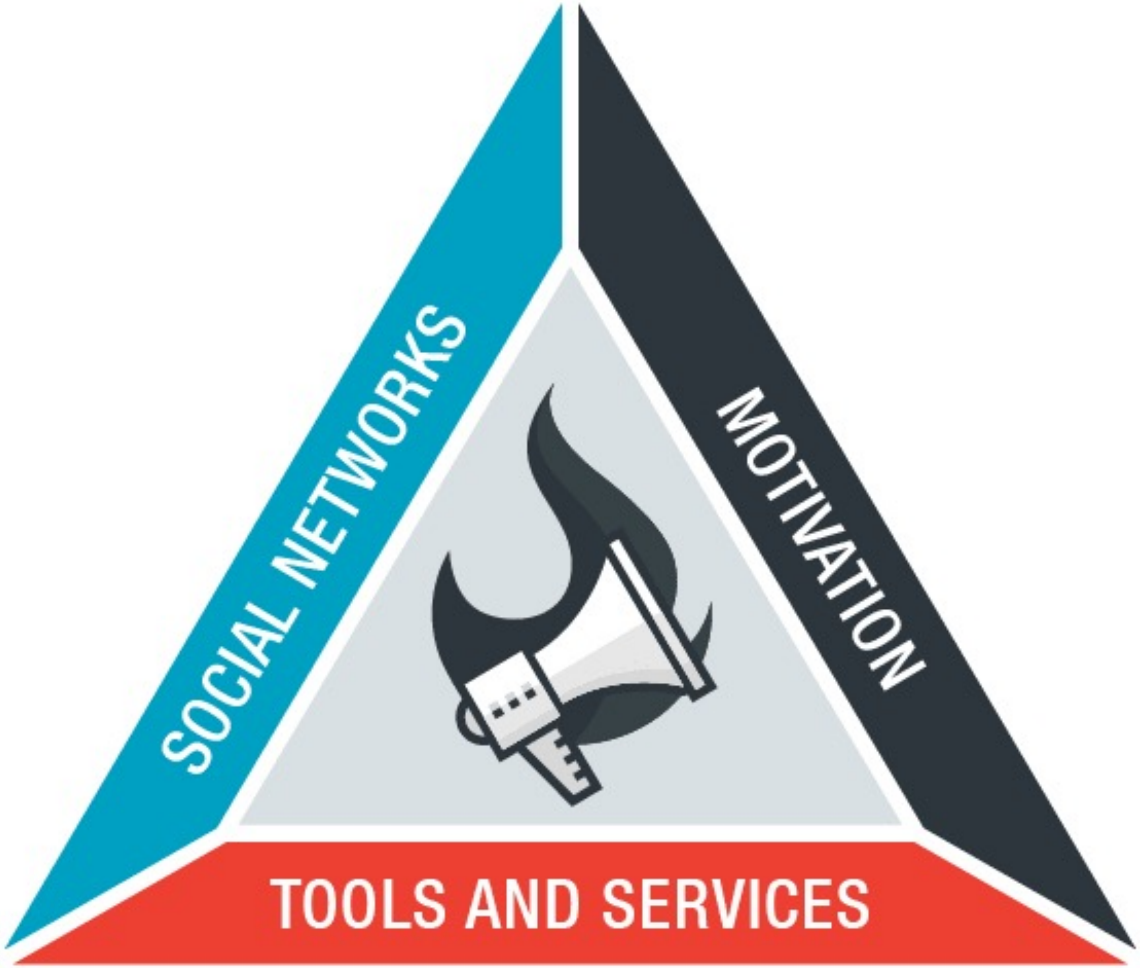
The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public
A TrendLabs Research Paper
https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media

ADVANTAGES OF FAKE NEWS

- Cost. For the reach demanded of fake news campaigns, legitimate advertising is more expensive compared to the costs of fake news (which is important to smaller, less-funded actors)
- Anonymity. It is much easier to hide the origin of a fake news campaign compared to paid advertising.
- Credibility. News sources may prefer stories spreading “virally” from users, as opposed to spreading through advertisements.

The Fake News Machine

FAKE NEWS



MARKETPLACES SELLING TOOLS AND SERVICES FOR PUBLIC OPINION MANIPULATION CAMPAIGNS

- "Manufacturing fake news requires tools, and the online underground is rife with them."
- "These offerings are available in online underground markets and in some ways can be considered an outgrowth of existing services such as Black Hat Search Engine Optimization (SEO), click fraud, and the sale of human and bot traffic."
- "An examination of the Chinese, Russian, Middle Eastern, and English-based underground marketplaces will reveal a range of services available to anyone looking to distribute fake news and launch public opinion manipulation campaigns."

The Fake News Machine

HOW TO OPERATE FAKE NEWS

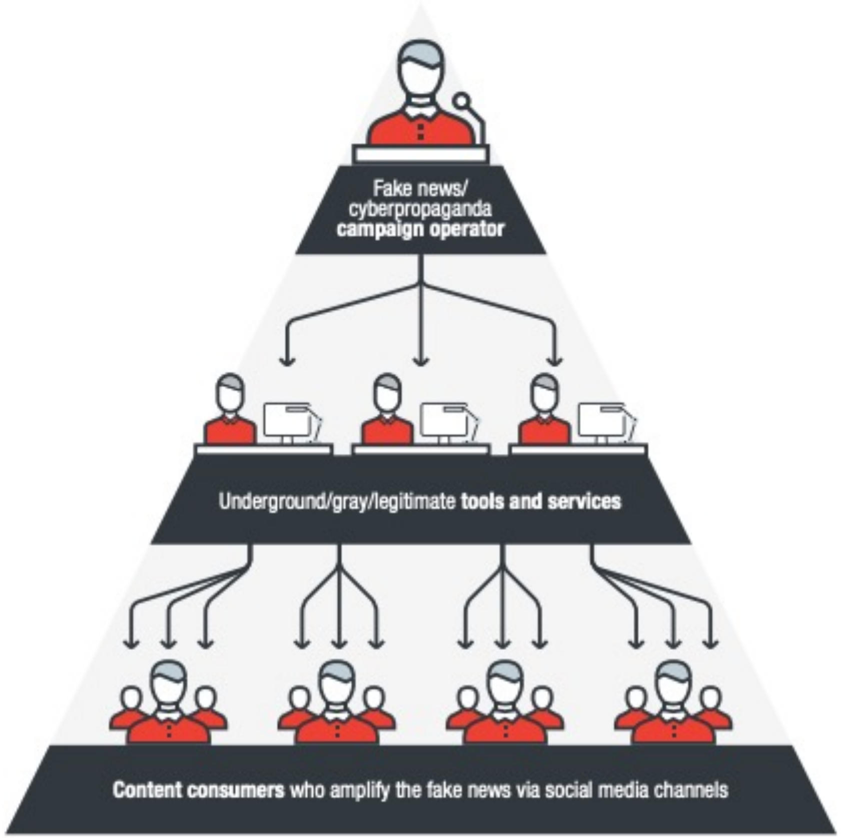

Fake news/
cyberpropaganda
campaign operator
Underground/gray/legitimate tools and services
Content consumers who amplify the fake news via social media channels

Figure 2. How an operator employs or abuses underground, gray, and legitimate marketplaces to disseminate fake news

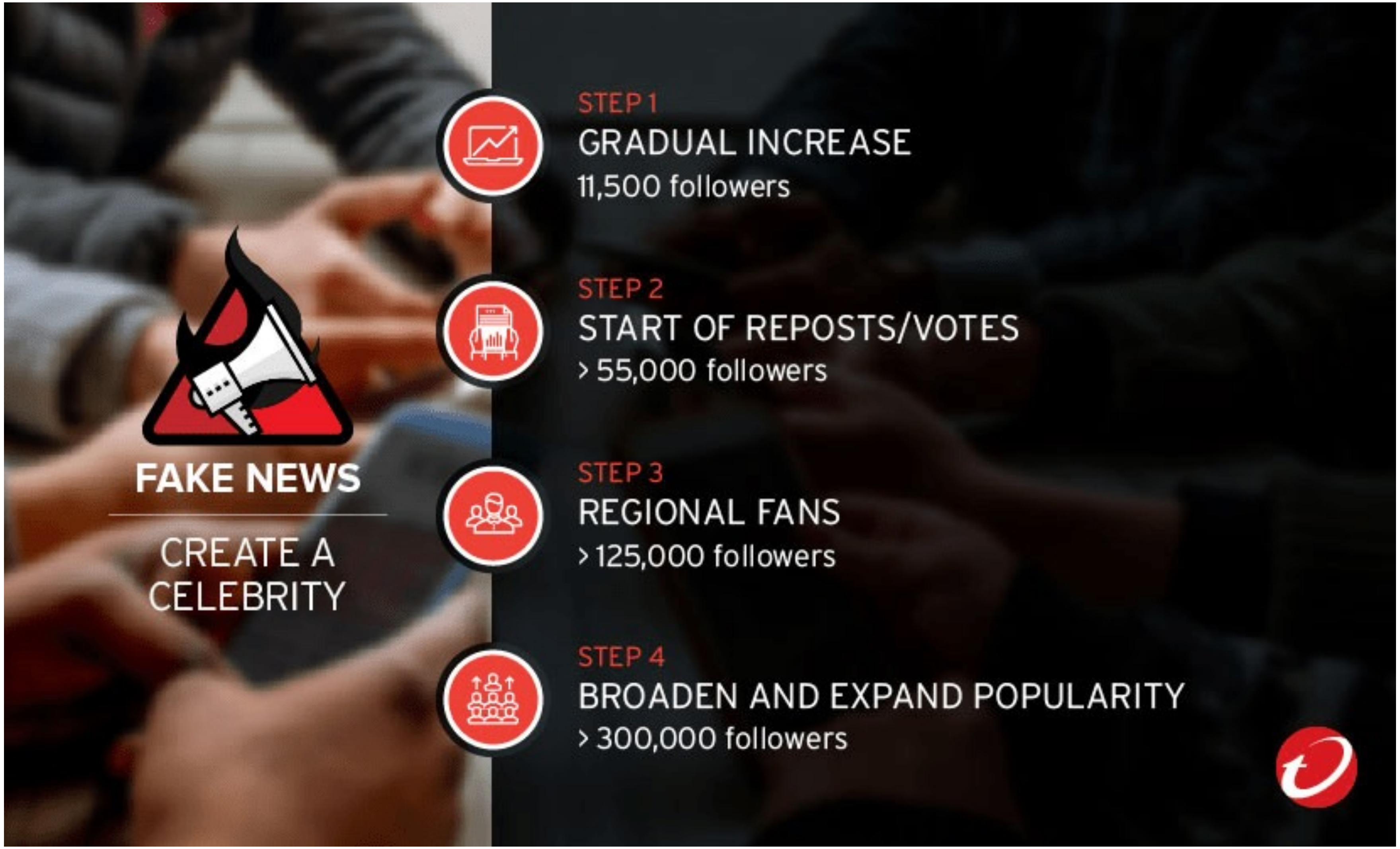
The Fake News Machine

CONTENT TAKEDOWN

- “While some Chinese underground services offer the creation, distribution, and proliferation of fake news, some also offer to do the opposite—taking down content. 118t Negative News (大良造负面信息理) offers such a service. News or a post in a given URL would need one to five days to be taken down, and the fee depends on the content’s popularity and where it’s published.”

FAKE NEWS

The Fake News Machine



FAKE NEWS

CREATE A CELEBRITY

STEP 1
GRADUAL INCREASE
11,500 followers

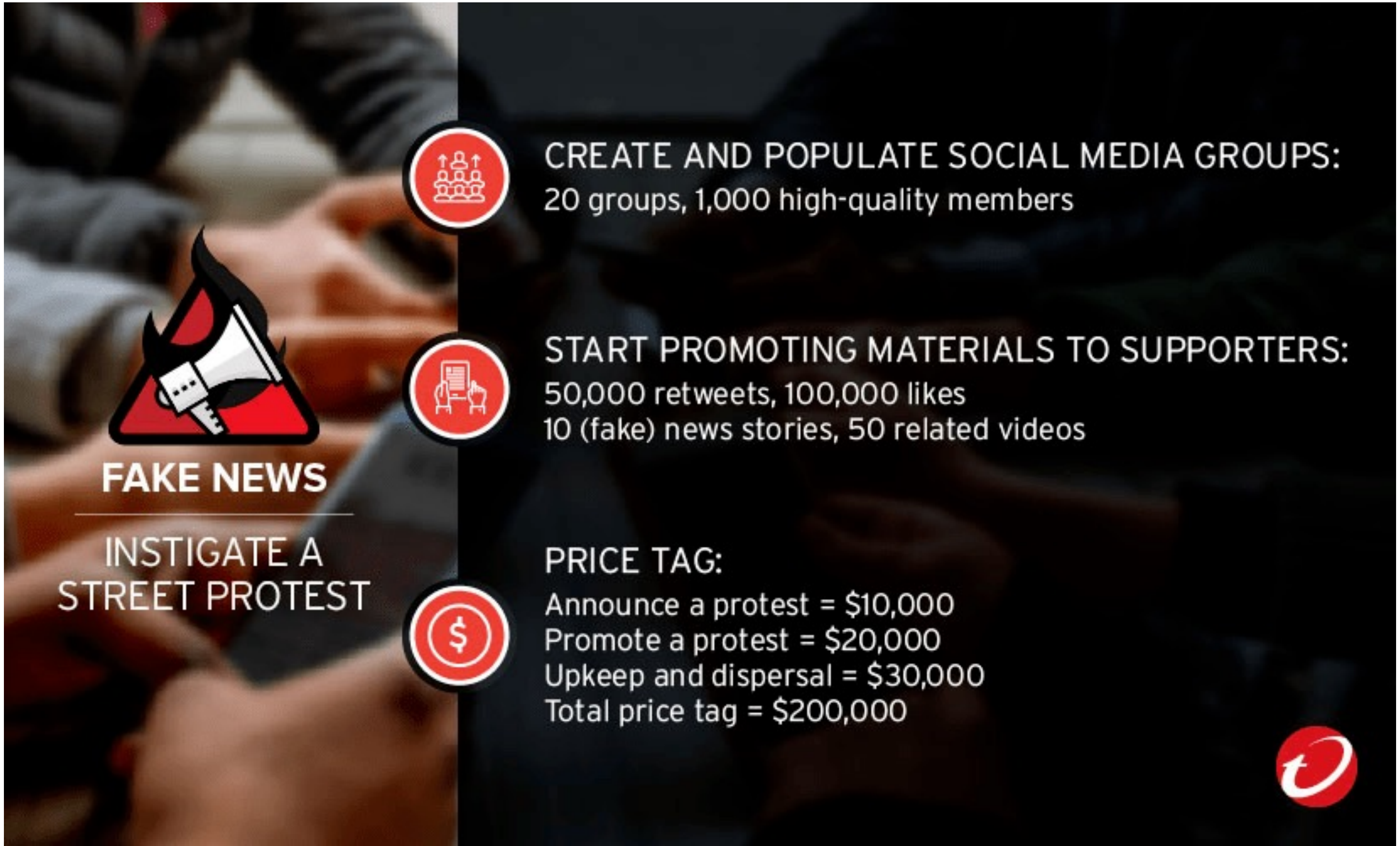
STEP 2
START OF REPOSTS/VOTES
> 55,000 followers

STEP 3
REGIONAL FANS
> 125,000 followers

STEP 4
BROADEN AND EXPAND POPULARITY
> 300,000 followers

FAKE NEWS

The Fake News Machine



FAKE NEWS

INSTIGATE A STREET PROTEST

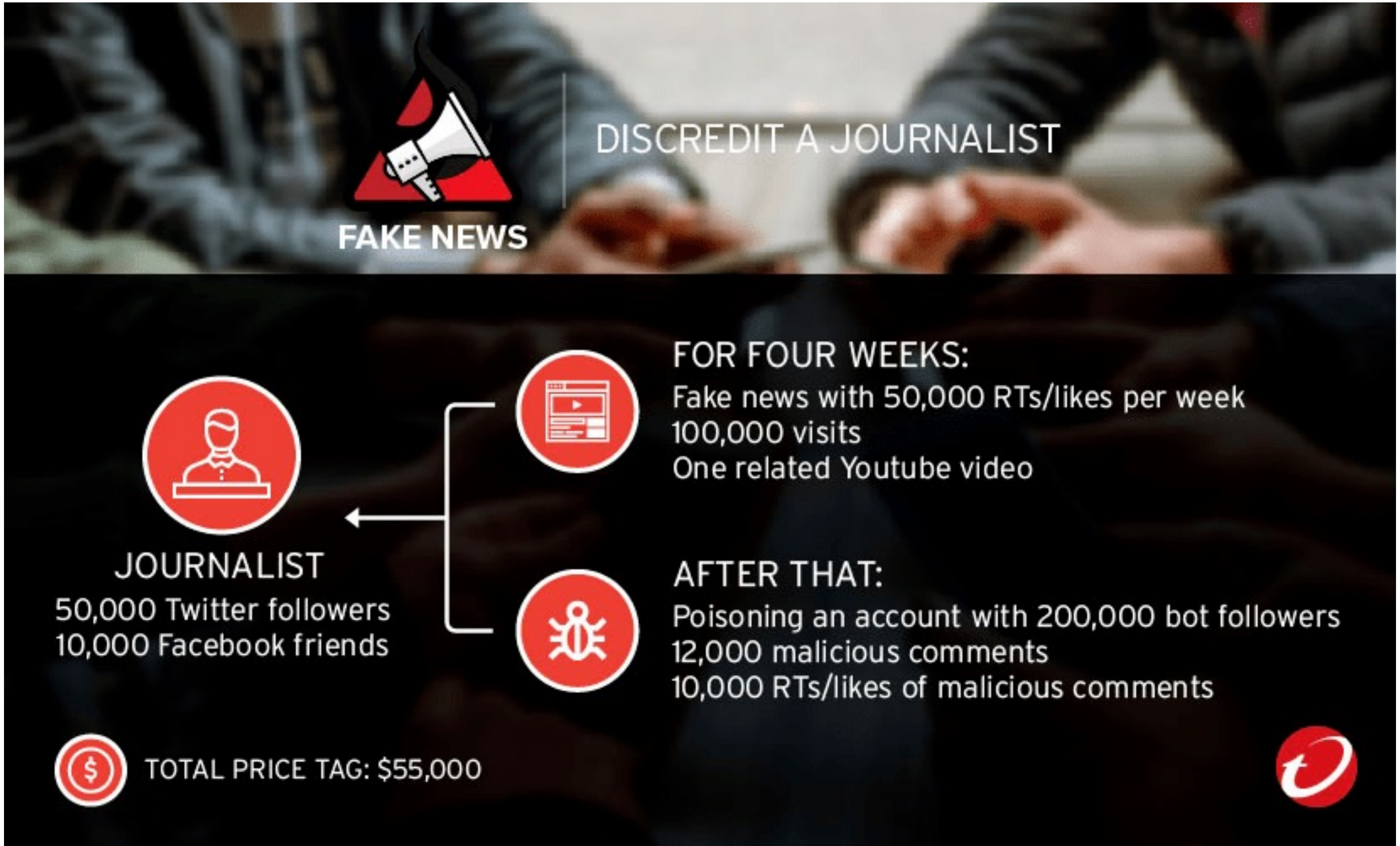
CREATE AND POPULATE SOCIAL MEDIA GROUPS:
20 groups, 1,000 high-quality members

START PROMOTING MATERIALS TO SUPPORTERS:
50,000 retweets, 100,000 likes
10 (fake) news stories, 50 related videos

PRICE TAG:
Announce a protest = $10,000
Promote a protest = $20,000
Upkeep and dispersal = $30,000
Total price tag = $200,000

FAKE NEWS

The Fake News Machine



DISCREDIT A JOURNALIST

JOURNALIST

50,000 Twitter followers

10,000 Facebook friends

FOR FOUR WEEKS:

Fake news with 50,000 RTs/likes per week

100,000 visits

One related Youtube video

AFTER THAT:

Poisoning an account with 200,000 bot followers

12,000 malicious comments

10,000 RTs/likes of malicious comments

TOTAL PRICE TAG: $55,000

POLITICAL MOTIVATIONS

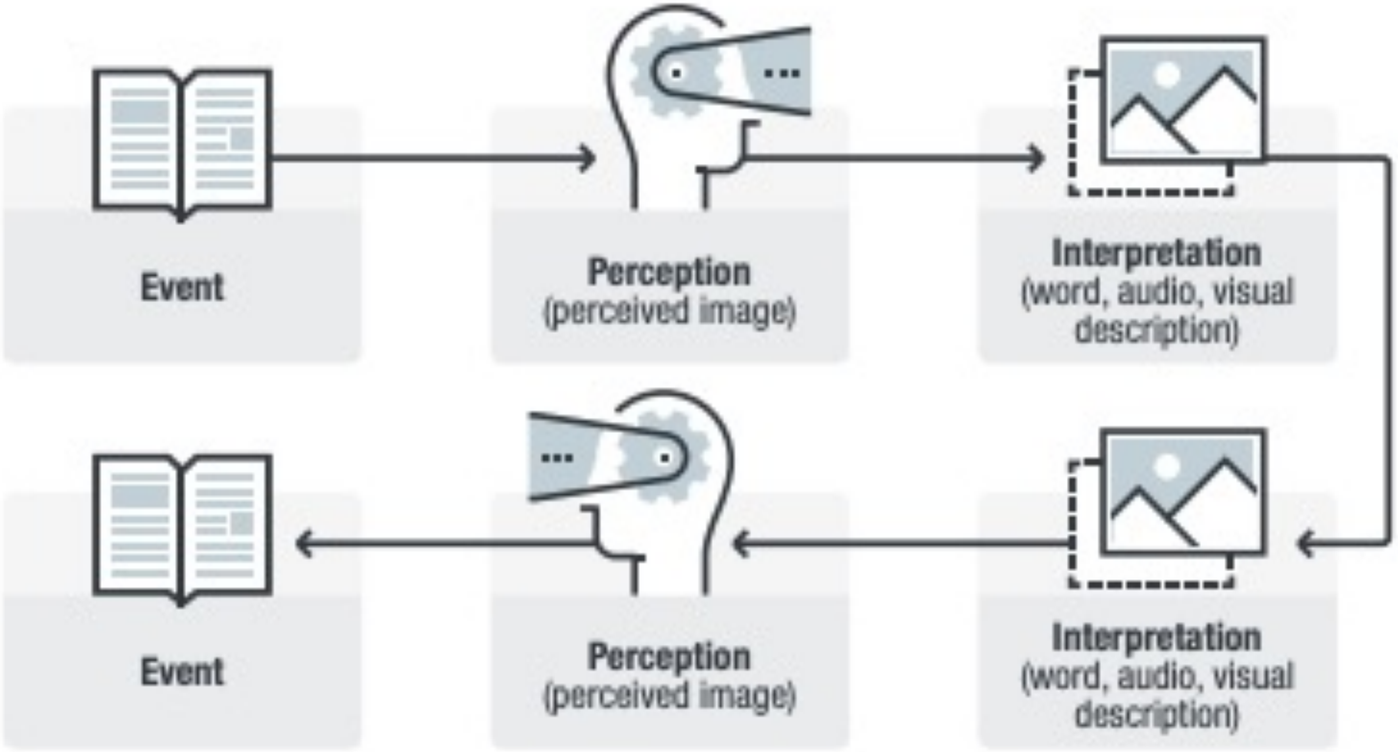


Figure 70. Ideal opinion formation process

The Fake News Machine

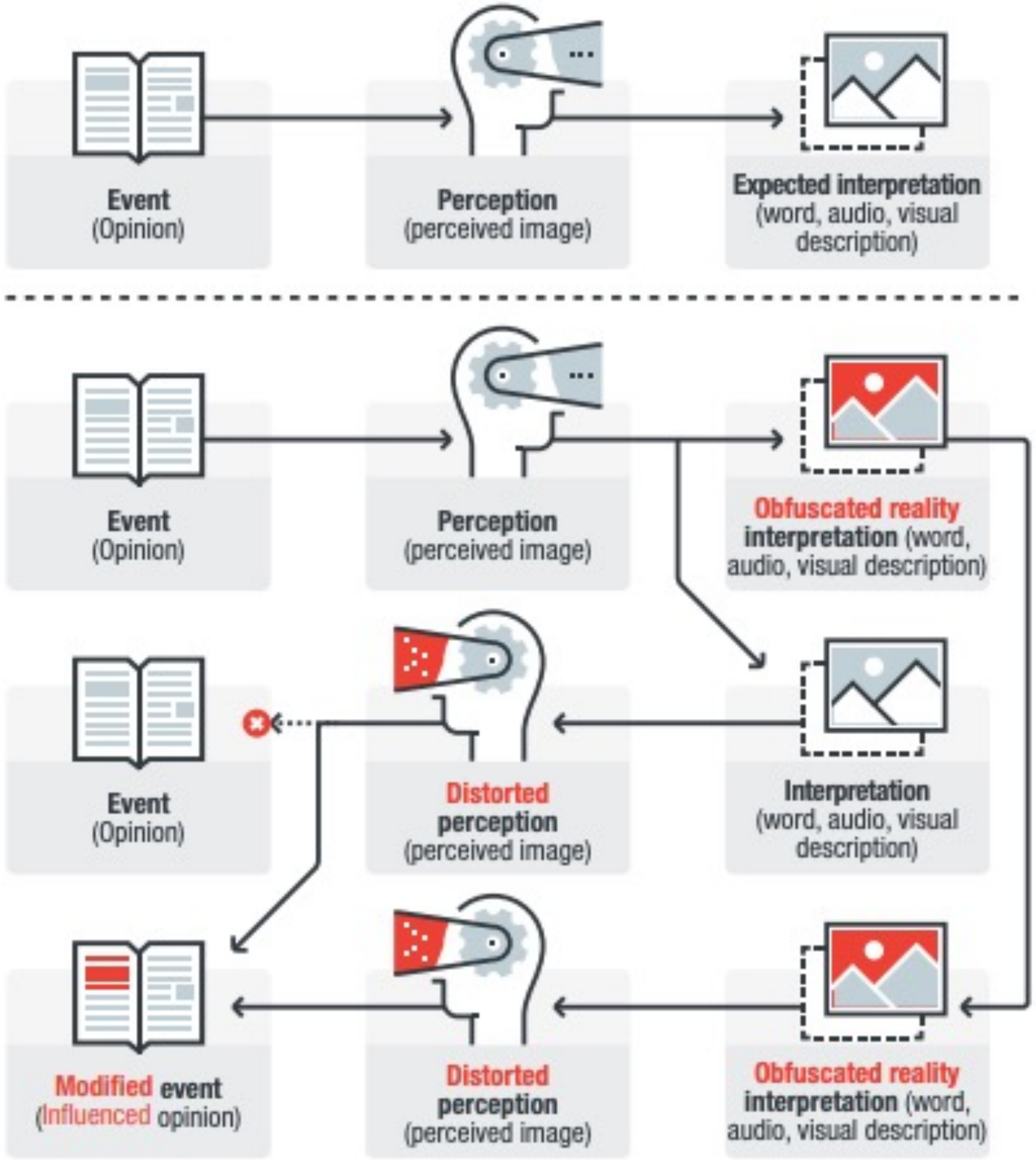


Figure 71. Opinion process formation, with propaganda

The Fake News Machine

DISCREDIT A JOURNALIST FOR $55,000

- Popular journalist has a Twitter account with 50,000 followers, a Facebook account with 10,000 friends, and a blog that publishes at least three articles a week that garners around 200 comments per post
- Four-week fake news campaign purchasing 50,000 retweets or likes and 100,000 visits. These cost around $2,700 per week.
- Buy four related videos and turn them into trending videos on YouTube, each of which can sell for around $2,500 per video.
- Buy comments; Spending $1,000 for this kind of service will translate to 4,000 comments.
- $240 for poisoning a Twitter account with 200,000 bot followers. Ordering a total of 12,000 comments with most bearing negative sentiment and references/links to fake stories against the journalist will cost around $3,000. Dislikes and negative comments on a journalist's article, and promoting them with 10,000 retweets or likes and 25,000 visits, can cost $20,400 in the underground.

MANIPULATE A DECISIVE COURSE OF ACTION FOR $400,000

- A campaign operator, for instance, can buy news websites focused on his targeted region and topic of interest. This service can cost around $3,000 per website. At least five websites that crossreferences each other can be bought to provide a semblance of reliability to the reader.
- A campaign operator would then start populating these websites with fake news masquerading as trustworthy sources of information. This is available as a service for $5,000. Maintaining these websites with more fake content and incorporating features such as account support and moderation will cost around $5,000 per month, which means the overhead of the websites' upkeep will be $60,000 in a year.
- These websites can then be promoted on social media with a targeted focus group in mind. Including promotional efforts in platforms like YouTube, this service can cost around $36,000 (or $3,000 per month).

CAMBRIDGE ANALYTICA: CHANGING CLICKS INTO VOTES?

“All you need to know is a little bit about data science, a little bit about bored rich women, and a little bit about human psychology…“ Chris Wylie

Guardian

CAMBRIDGE ANALYTICA: HOW 50M FACEBOOK RECORDS WERE HIJACKED

1 Approx. 32,000 US voters ('seeders') were ***paid $2-5 to take a detailed personality/ political test*** that required them to log in with their Facebook account
2 The app also ***collected data such as likes and personal information*** from the test-taker's Facebook account, as well their ***friends'*** data, amounting to over 50m people's raw Facebook data
3 The ***personality quiz results*** were paired with their Facebook data – such as ***likes*** – to seek out psychological patterns Friend's Data User's data
4 Algorithms combined the data with other sources such as voter records to ***create a superior set of records (initially 2m people in 11 key states*)***, with hundreds of data points per person.

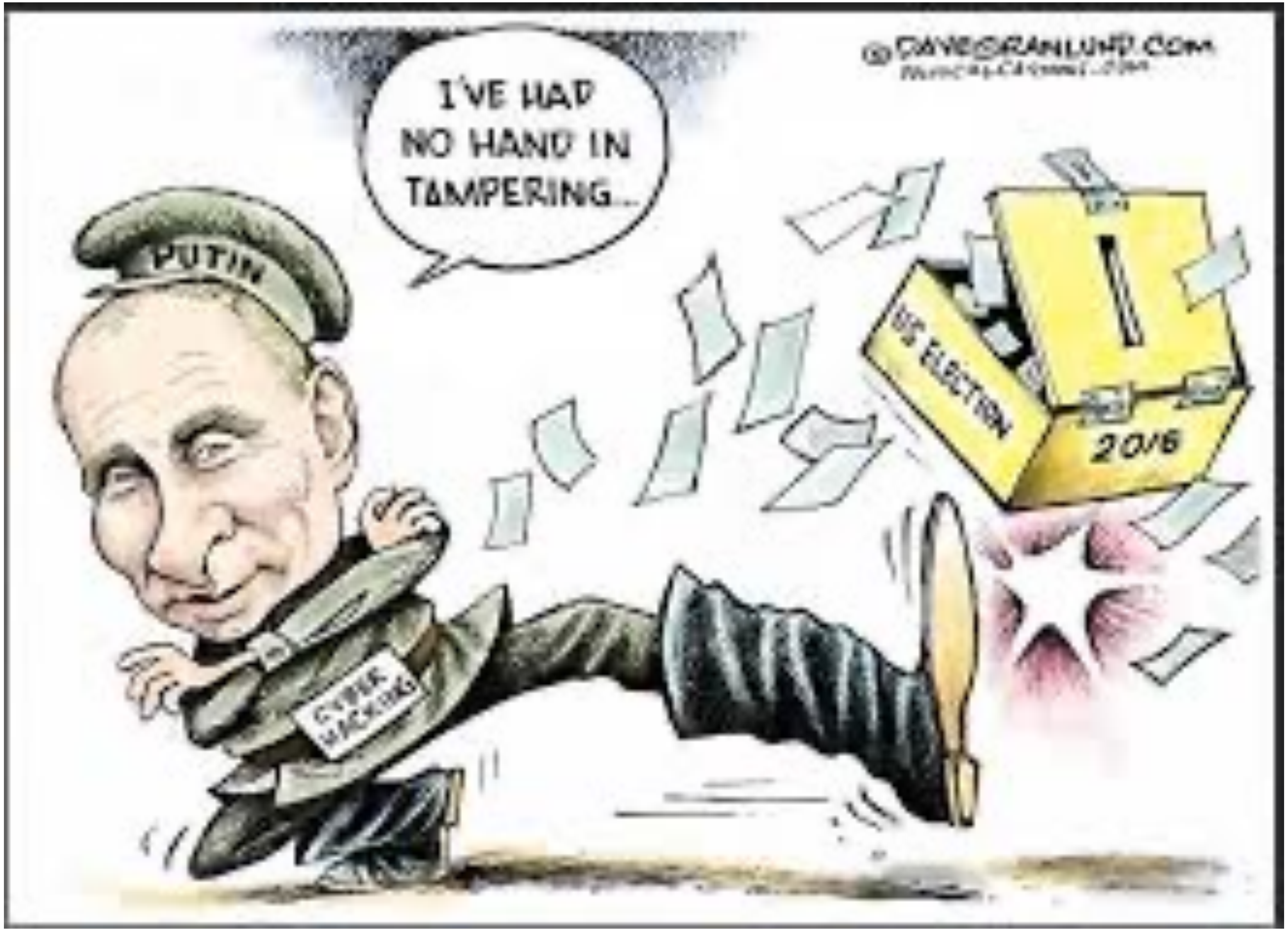
These individuals could then be targeted with ***highly personalised advertising*** based on their personality data
https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

IS PSYCHOLOGICAL TARGETING AN EFFECTIVE TOOL OF DIGITAL PROPAGANDA?

"I've been warning about these risks for years," says Michal Kosinski, a psychologist and assistant professor of organizational behavior at Stanford Graduate School of Business.

Psychological Targeting as an Effective Approach to Digital Mass Persuasion
By S.C. Matz, Michal KosinskiG. NaveD. J. Stillwell. https://www.gsb.stanford.edu/faculty-research/publications/psychological-targeting-effective-approach-digital-mass-persuasion

"Recent research, however, shows that people's psychological characteristics can be accurately predicted from their digital footprints, such as their Facebook Likes or Tweets. Capitalizing on this form of psychological assessment from digital footprints, we test the effects of psychological persuasion on people's actual behavior in an ecologically valid setting. "


©DAVEGRANLUND.COM
I'VE HAD NO HAND IN TAMPERING...
PUTIN
CYBER HACKING
US ELECTION
2016

WEBSITES THAT LET USERS CREATE THEIR OWN "BREAKING NEWS

Break Your Own News

Break Your Own News - Breaking News Meme Generator
https://breakyourownnews.com

ClassTool's Breaking News Generator
https://www.classtools.net/breakingnews/

LIVE CHAMPAIGN

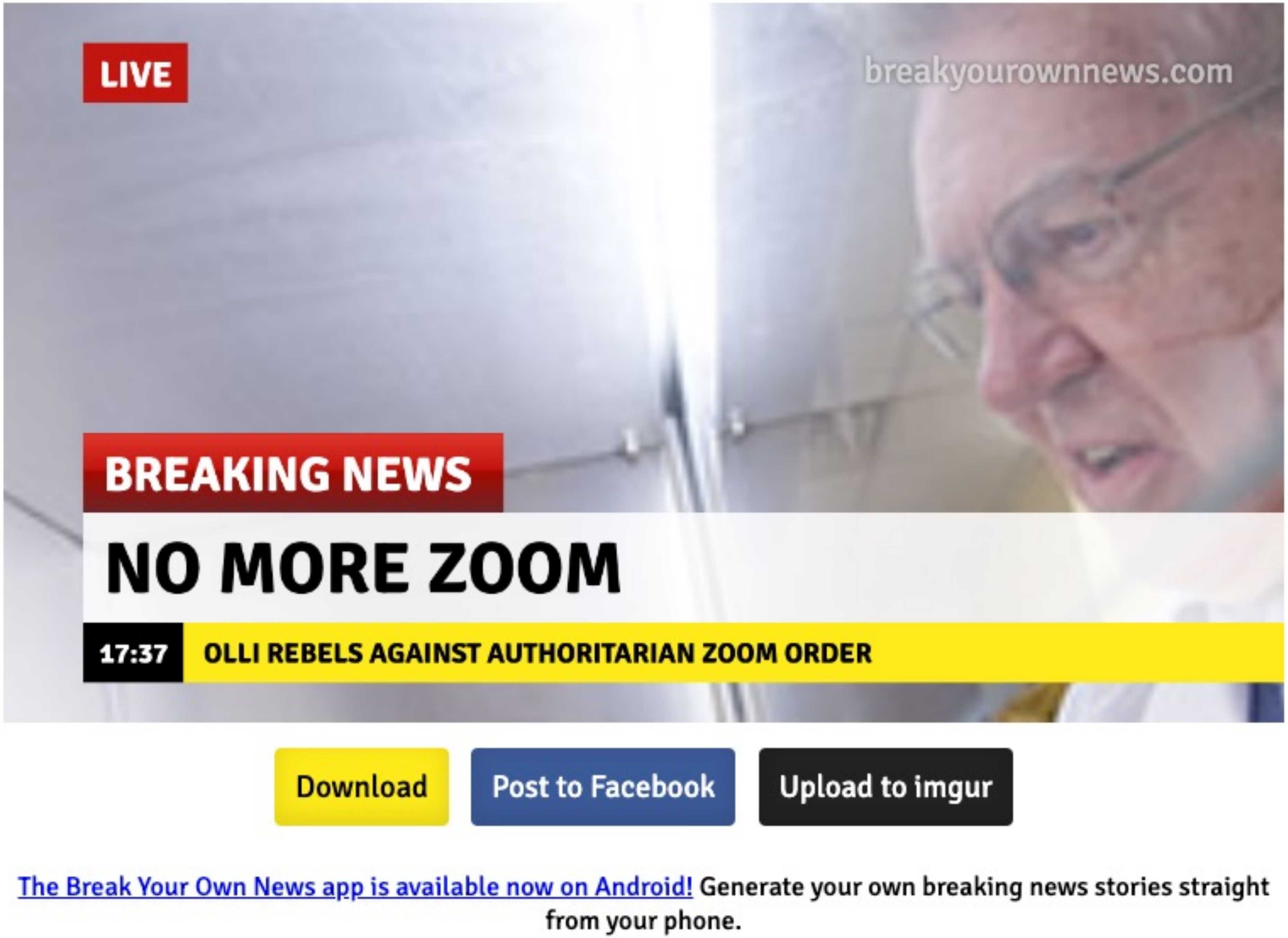
OLLI AT WORK

PLANNING THE COFFEE REVOLUTION

2022

OLDER PEOPLE KNOW WHATS WHAT

classtools.net



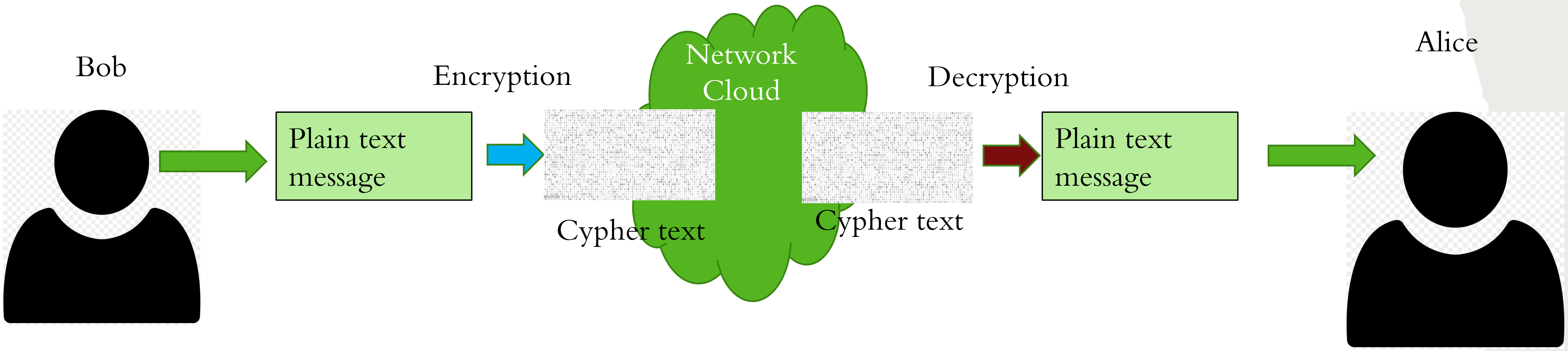
The Break Your Own News app is available now on Android! Generate your own breaking news stories straight from your phone.

2. ENCRYPTION

Auguste Kerckhoffs Principles (1883) *Journal of Military Science, Military Cryptography)*

- The system should be, if not theoretically unbreakable, unbreakable in practice.
- ***The design of a system should not require secrecy, and compromise of the system should not inconvenience the correspondents*** (Kerckhoffs's principle).
- The key should be memorable without notes and should be easily changeable.
- The cryptograms should be transmittable by telegraph.
- The apparatus or documents should be portable and operable by a single person.
- The system should be easy, neither requiring knowledge of a long list of rules nor involving mental strain.

ENCRYPTION BASICS



$\text{Decryption}_{\text{key1}} \; (\text{Encryption}_{\text{key2}} \; (\text{ plain text }) \;) = \text{plain text}$

Sometimes key1 = key 2 symmetric encryption
Sometimes key1 <> key 2 asymmetric encryption

"I'm applying for the Information Security position.
Here is a copy of my resumé, encoded, encrypted and shredded."

TRIVIAL EXAMPLE

Cleartext:	*A*	*P*	*P*	*L*	*E*	*Key*	*4*	*4*	*4*	*4*	*4*
Ciphertext:	E	T	T	P	I						

Encrypt (APPLE) $_{\text{Shift Right 4 4 4 4}}$ = ETTPI and Decrypt (ETTPI) $_{\text{Shift Left 4 4 4 4}}$ = APPLE asymmetric

Encrypt (APPLE) $_{\text{invert}}$ = ∀ЬЬΓE Decrypt (∀ЬЬΓE) $_{\text{invert}}$ = APPLE symmetric

GOOD ENCRYPTION (SHANNON) USES:

1) Confusion

Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.

The property of confusion hides the relationship between the ciphertext and the key.

2) Diffusion

Diffusion means that if we change a single bit of the plaintext, then about half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then about half of the plaintext bits should change.

"Putting your text in Pig Latin isn't the same as encrypting."

3. CYBERWAR UKRAINE RUSSIA

- ***Ukrainian authorities reported over the weekend that a piece of malware had been discovered on the networks of the Boryspil international airport in Kiev.***
- ***Global multimedia giant News Corp on Friday revealed it fell victim to a targeted cyberattack that appears to have been conducted by a "foreign government."***
- ***Shuckworm*** (aka Gamaredon, Armageddon) ***Continues Cyber-Espionage Attacks Against Ukraine***
- ***Ukraine's National Security and Defense Council (NSDC) this week published two press releases describing cyberattacks aimed at the country.***
- https://www.rnbo.gov.ua/en/Diialnist/4820.html National Security and Defence Council of Ukraine
- https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/
- https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/
- The Gamaredon Group Toolset Evolution – Unit 42, Palo Alto Networks
  Threat Brief: Ongoing Russia and Ukraine Cyber Conflict – Unit 42, Palo Alto Networks
  Technical Report on Armageddon / Gamaredon – Security Service of Ukraine
  Tale of Gamaredon Infection – CERT-EE / Estonian Information System Authority

HTTPS://UNIT42.PALOALTONETWORKS.COM/UKRAINE-CYBER-CONFLICT-CVE-2021-32648-WHISPERGATE/

- Beginning on Jan. 14, 2022, reports began emerging about a series of attacks targeting numerous Ukrainian government websites. As a result of these attacks, numerous government websites were found to be either defaced or inaccessible. As a result of this, the government of Ukraine formally accused Russia of masterminding these attacks against their websites.

- A day later, public reporting outlined a new malware family, called WhisperGate, that originally was observed on Jan. 13, 2022. This malware family disables Windows Defender Threat Protection, is destructive in nature and was discovered to have targeted multiple organizations in Ukraine. Microsoft has publicly attributed the use of this custom malware family to a threat actor they refer to as DEV-0586.

SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.

RESOURCES LECTURE 2

- https://www.vmware.com/resources/security/modern-bank-heists-2021.html
- https://www.theguardian.com/media/greenslade/2015/oct/23/news-media-websites-vulnerable-to-cyber-attacks-research
- https://www.aon.com/reputation-risk-cyber-social-media-pentland-analytics-aon/index.html
- https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media
- https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

Thank you!!