(U) Russian Cyber Threats to US Critical Infrastructure

Oregon Cyber Resilience Summit Program

October 29, 2019

The overall classification of this briefing is:

UNCLASSIFIED

Cyber Mission Center

The **Cyber Mission Center** is the Department of Homeland Security's premier provider of all-source cyber threat analysis. The Mission Center delivers finished intelligence at the lowest classification level possible to enable the Department's mission of ensuring cybersecurity and resilience of federal civilian government, state, local, tribal, territorial and critical infrastructure networks.

Homeland Security

Russian Threats to US Critical Infrastructure

Context:

- Since at least March 2016, Russian Government cyber actors targeted multiple **US Government entities** and critical infrastructure sectors, including the **energy, nuclear, commercial facilities, water, aviation, critical manufacturing sectors,** as well as **industrial control system (ICS) infrastructure.**
- Russian intelligence officers were charged in July 2018 with allegedly attempting to hack into computers of **US state boards of election, US secretaries of state**, and **US companies** that supplied election-related software and other technology during the 2016 US presidential election.

Russia is aggressive: targets government networks and critical infrastructure

Russian Threats to US Critical Infrastructure

Capabilities:

- Open-source and network reconnaissance
- Phishing and spear-phishing emails
  - Primary, third party “staging” targets
  - Deployment of malware
- Watering-hole domains
  - Credential gathering
- Leveraging publicly available tools
  - Makes attribution difficult
- Persistent access to networks
  - Establishing local accounts
- Targeting network infrastructure devices
  - Infecting home and office routers and switches
    - i.e. “VPNFilter” botnet (May 2018)

Preparation → Engagement → Presence → Effect / Consequence

Russian Threats to US Critical Infrastructure

Possible Russian Intent:

- Conduct espionage, gather information and target networks
  - i.e. conduct extensive data exfiltration of sensitive files, emails, and user credentials
- Steal intellectual property
- Prepare cyber environment for future contingencies
- Conduct destructive attacks
- Divide and undermine opponents

Goals: solidify regional hegemony, support Russia's military and economic interests

Russian Government Cyber Activity Targeting US Critical Infrastructure Sectors Since 2016

Targeted sectors:

- Energy, nuclear, commercial facilities, water, aviation, critical manufacturing

Systems affected:

- Domain controllers
  - Server that responds to authentication requests (i.e. logging in)
- File servers
  - Controls access to files in a multi-user environment
- Email servers
  - Acts as a virtual post office

Multi-stage intrusion campaign:

- Staged malware in small commercial facilities' networks
- Conducted spear-phishing
- Gained remote access into energy networks `
- Conducted network reconnaissance, moved laterally, collected information on industrial control systems (ICS)

Russian campaign victims: third party "staging" targets and intended targets

Homeland Security

Russian Government Cyber Activity Targeting US Election Infrastructure in 2016

Goal:

- Steal voter data stored on computers

Targeted parties:

- State boards of election
- Secretaries of state
- Companies that supplied software, other technology related to the administration of elections

Methods of obfuscation:

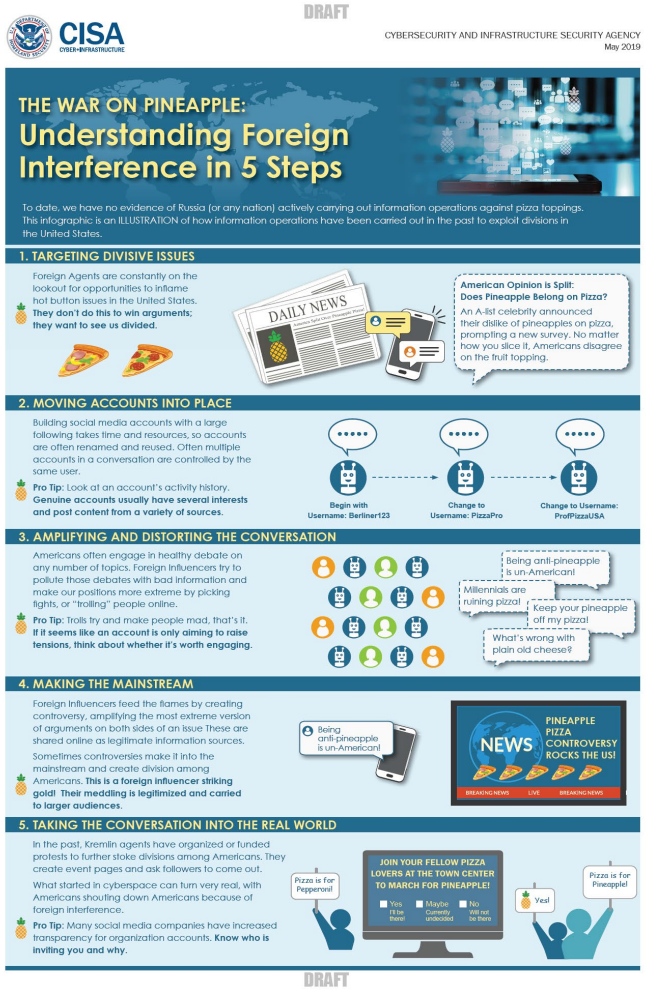
- False identities
- Global networks of computers
- Cryptocurrency to pay for accounts, servers, and domains

Russian actors sought to interfere with the 2016 US presidential election

Russian Influence Activity Targeting US Critical Infrastructure

Context:

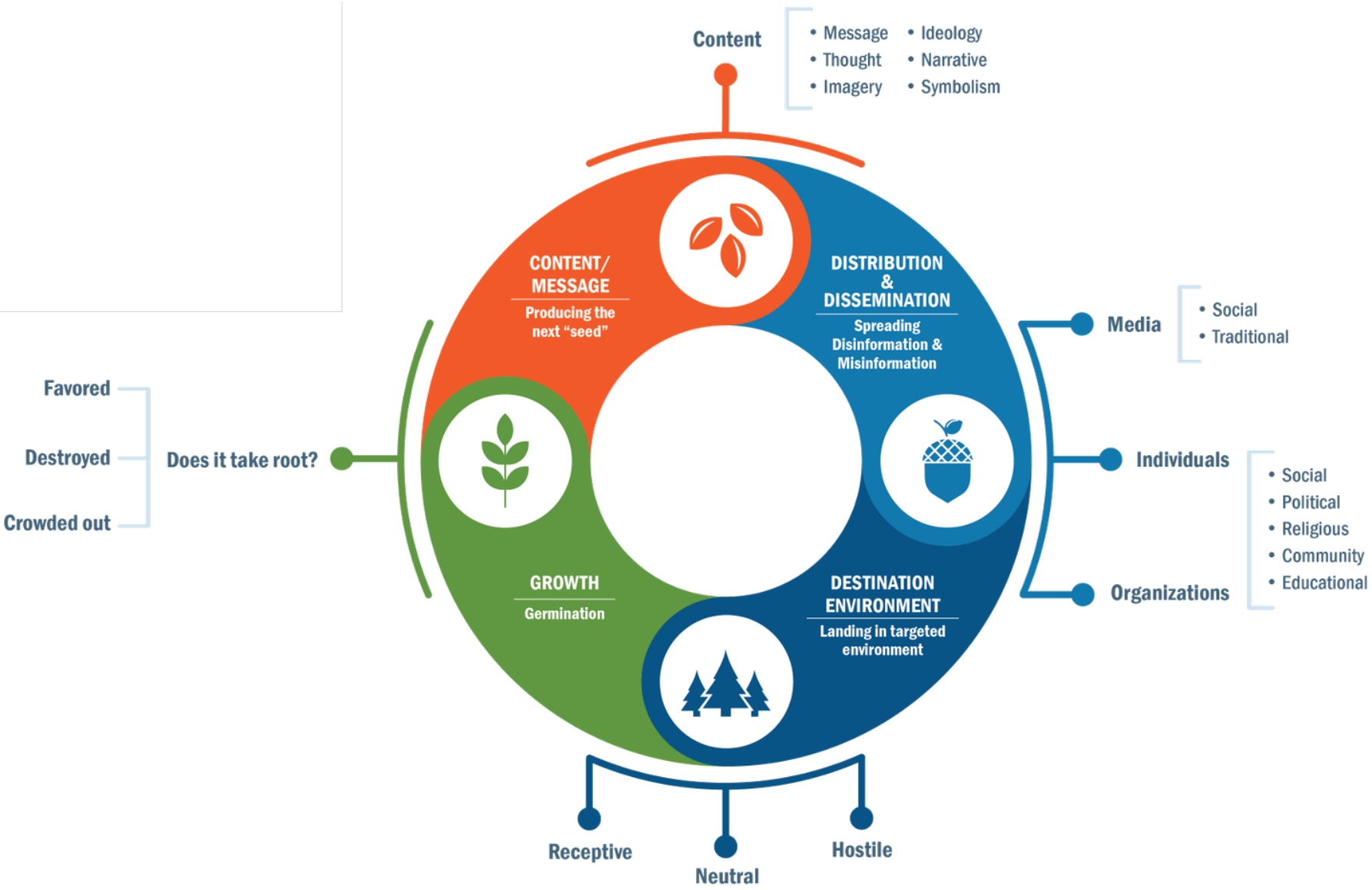
- Since at least 2015, Russian actors have used multiple platforms, including social media platforms, to target US audiences through influence activity.



Methods for distribution include: fake news websites, false personas, falsified materials, and claimed leaks

Homeland Security

How Ideas (Good or Bad) Spread & Grow… or Fade Away…



Russian Influence Case Study: 2014 Louisiana Chemical Attack

Goal:

- Disrupt US energy markets to reduce competition to Russian energy companies

Narratives:

- Dakota Access Pipeline and fracking are bad for the environment
- US Government is stealing from Native Americans
- Energy companies have record profits at the expense of the environment

Target Audiences:

- Environmentalists
- Native Americans
- Pipeline supporters

Distribution and Dissemination:

- Funded environmental groups and engaged unwitting activists
- Social media messaging and memes to stoke passions
- Petition drives
- Leveraged state-run media to push narratives

Russian Influence Case Study: 2015-2017 US Energy Markets

Goal:

- Attribute a fake attack on a US chemical facility to ISIS
- Test influence capabilities

Narratives:

- ISIS attacked a chemical facility in Louisiana

Impacted Audience:

- Local residents
- Local and national media and political commentators

Distribution and Dissemination:

- Text messages to local population
- Fake surveillance camera footage
- Doctored images of flames engulfing plant
- Fake YouTube video with ISIS claiming responsibility
- Doctored CNN webpage to show disaster made national news
- Hashtag pushed by hundreds of Twitter accounts
- Wikipedia page about the attack created
- Tweets targeting media and political commentators asking them to cover the attack

Conclusion and Questions

The overall classification of this briefing has been:

UNCLASSIFIED

When You Become a Victim…

Organization	What to Report?
DHS – Cybersecurity and Infrastructure Security Agency (CISA) | US-CERT	
Cyber Security and Infrastructure Security Agency (https://www.cisa.gov/about-cisa) (info@us-cert.gov or nccic@hq.dhs.gov) or (888) 282-0870	Suspected or confirmed cyber incidents that may impact critical infrastructure and require technical response and mitigation assistance
DHS - United States Secret Service (USSS)	
Secret Service Field Offices (http://www.secretservice.gov/field_offices.shtml) Electronic Crimes Task Forces (ECTFs) (http://www.secretservice.gov/ectf.shtml)	Cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment Information
DHS - Immigration & Customs Enforcement Homeland Security Investigations (ICE HSI)	
ICE HSI Field Offices (http://www.ice.gov/contact/inv/) ICE HSI Cyber Crimes Center (http://www.ice.gov/cyber-crimes/)	Cyber-based domestic or international cross-border crime, including child exploitation, money laundering, smuggling, and violations of intellectual property rights
Federal Bureau of Investigation (FBI)	
FBI Field Offices (http://www.fbi.gov/contact-us/field) Cyber Task Forces (http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1) Law Enforcement Online Portal (https://www.cjis.gov/CJISEAI/EAIController) or (888) 334-4536	Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity

Cyber Actor Capabilities and the Threat Environment