

This briefing was developed for **The Blue Book Project**, lead by the Commonwealth of Virginia, support by CNA, and funded through a FEMA regional catastrophic planning grant.

Blue Book Project Goal: Develop a coordinated operational process to support local, state, federal, and private sector priorities; support Virginia residents; and ensure continuity of government while managing consequences from a coordinated nation-state cyberattack on critical lifeline services.





# The Blue Book Project

## Russian Federation Threat Briefing



# Russian strategic goals

- Espionage
  - Using cyber attacks to infiltrate US systems to extract information
  - Identify variations in system security across US federal agencies as well as state governments
- Weakening US capabilities
  - Damaging critical infrastructure
  - Sowing division in society
- Preparing for future conflict with US
  - Using cyber attacks to test and assess potential US vulnerabilities
  - Military doctrine includes attacks on civilian infrastructure to affect adversary's will to fight
- Deterrence of US action against Russia
  - Demonstrating risks to US of engaging in hostile activities



# Russian capabilities and actors



CNA

- FSB: responsible for intelligence and counter-intelligence, incl. cyberspace
- GRU: military intelligence responsible for offensive cyber operations
  - Unit 74455: hacking and leaking cyber operations, malware
  - Unit 26165: SIGINT and cryptographic cyber operations
  - Unit 54777: psychological warfare, digital information operations
- SVR: cyber espionage operations
- Non-state actors
  - Independent and government-connected 'patriotic' hackers
  - Cyber criminals



# Malware attacks



CNA

- Colonial Pipeline
  - 2021 ransomware attack disabled digital systems, resulted in shutdown of pipeline
  - Carried out by Darkside: Russia-related cyber criminal group
  - Enabled by exposed password for VPN account: likely target of opportunity, rather than planned attack
- Thwarted potential 2022 attack on US power grid
  - Pipedream malware targets variety of industrial control systems
  - Infiltrated air-gapped control rooms of multiple electric utilities
  - Similar to successful 2015 attack on Ukraine electric grid
- NotPetya
  - 2017 GRU Unit 74455 attack stopped 1/3 of Ukrainian economy for 3 days
  - Spread globally, causing \$10 billion in economic damage, incl US health care providers



# Cyber hacking and espionage



CNA

- Turla APT: FSB cyber espionage group
  - Sophisticated group focused on long-term value targets
  - Attacked US military networks in 2008, hijacked satellite internet connections
- 2014: leak of conversation between Asst. Sec. of State and US Amb. to Ukraine
  - Intended to undermine US foreign policy vis-à-vis Ukraine
- 2016: SVR Cozybear group penetration of US voter databases at state level
- 2020: SVR Solarwinds supply chain hack
  - Allowed backdoor system access and file exfiltration
  - Affected gov't agencies includes DHS, DOJ, Treasury
- 2023: Russian hackers use backdoor to access UK MOD files
  - Publish information on access to nuclear base, prisons, other secure facilities



# Russian use of false and misleading information



CNA



## Operation Secondary Infection

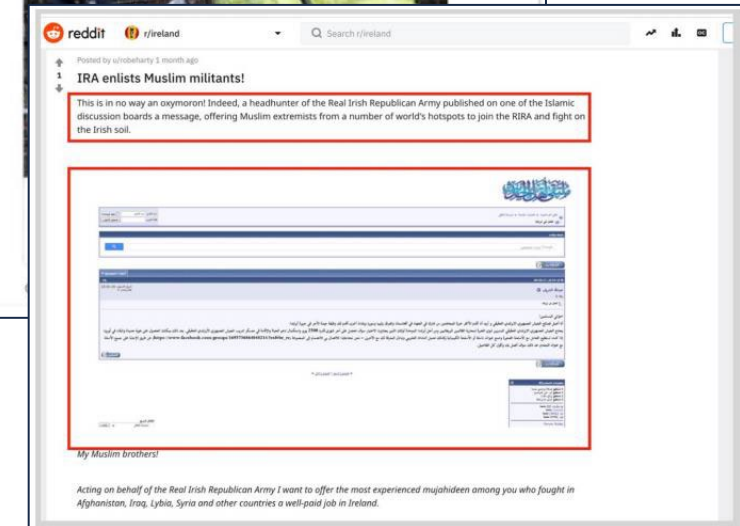
Designed to foment discord and division within countries that Russia perceives as its adversaries

- 6+ years
- 9 languages
- 30 social networks and blogging platforms
- False news stories, forged documents, and divisive content

## 2016 US Presidential Election

Designed to foment discord and division within the US

- Facebook, Twitter, Instagram, YouTube, Reddit, Pinterest, Tumblr, and Vine
- Facebook posts alone were shared over 31 million times
- Event invitations, memes, and news articles; linking across platforms; and sharing authentic and nonpolitical content



# Let's Connect



CNA

**Feel Free to email us with questions**  
**[bluebookproject@vdem.virginia.gov](mailto:bluebookproject@vdem.virginia.gov)**

**Check out the Blue Book TV Reading Corner for more information and resources**

**[Reading Corner - The Blue Book Project | VDEM](#)**

