

# Can the internet be made safe?

An introduction to cyber security

30 October 2018

# Presentation outline

- The internet: Not built for security
- Common types of attacks
- Case studies
  - Cyber attacks
  - Internet of Things
  - Influence operations and the information environment
- The search for solutions
- Questions

# The internet: Not built for security

- 1960s-70s: ARPANET used by academic researchers to exchange files and messages, access other computers in the network
- Closed community of trusted colleagues
- 1970s-80s: TCP/IP developed to connect ARPANET with other networks around the world; launched in 1983
  - Problem: anyone with access to the network could monitor transmissions
  - Encryption would offer privacy and security, but required more computing power than feasible at the time
- Trend continued with other protocols: openness > security

# Types of cyber attacks

- Malware: malicious software
  - Virus
  - Worm
  - Ransomware
  - Spyware
- Man in the Middle
- Denial of Service (DoS)/Distributed Denial of Service (DDoS)
- Zero-day exploits

# Motives for cyber attacks

- Accessing a system
  - Reconnaissance for future activities
- Espionage or theft
- Disruption
- Destruction

---

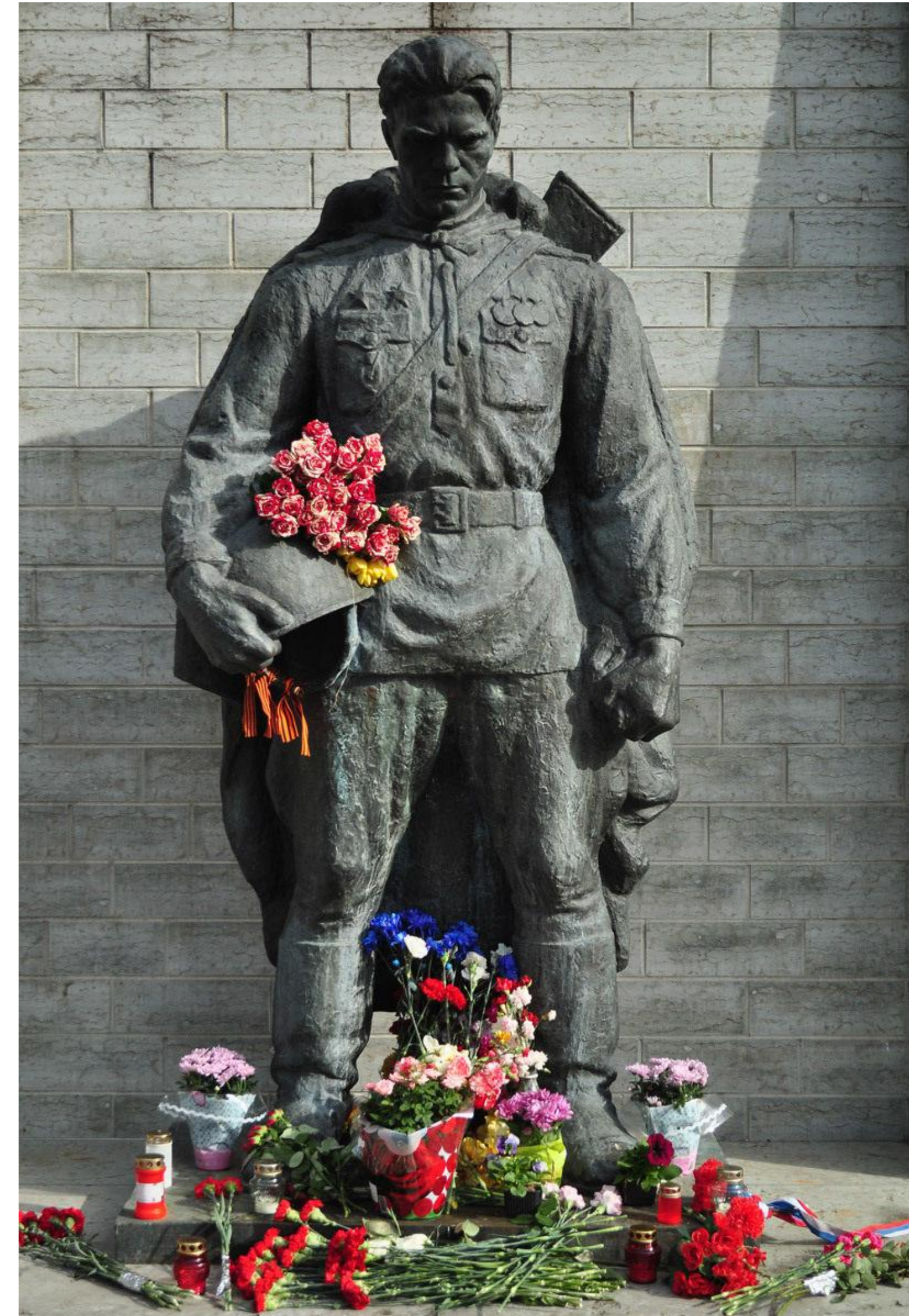
Centre for International  
Governance Innovation

# Case studies



# Estonia, 2007

- April 2007: Russian-Estonian riots and protests
- Widespread cyber attacks took down government websites, ATM, news media, etc.
  - 60 key websites offline at once
  - Attacks continued for weeks
- Attributed to Russia; Russia denies
- First suspected state-sponsored cyber attack





# Stuxnet, 2010

- Sophisticated computer worm that disrupted the operation of Siemens industrial control systems
- Took advantage of Microsoft zero-day vulnerabilities
- Targeted Iran nuclear facilities
- Destroyed 1,000 centrifuges
- First computer attack to damage physical infrastructure
- Widely reported to be the work of United States and Israel; neither has confirmed





# State-sponsored cyber attacks

- Attribution challenges: Plausible deniability
- Ambiguous legal/normative landscape: “below threshold”
  - UN Group of Governmental Experts on ICT Security (GGE)
  - Tallinn Manual
- Fear of escalation
- Bad actors take advantage of uncertainty

# Wannacry, 2017

- Computer worm paired with ransomware
- Affected 300,000 people in 150 countries, including hospitals in U.K.
- Caused \$1 billion worth of damage in days
- Exploited software flaw in Microsoft Windows operating systems
  - Out-of-date institutional networks more difficult to patch
  - Vulnerability discovered by NSA, leaked
- North Korea suspected



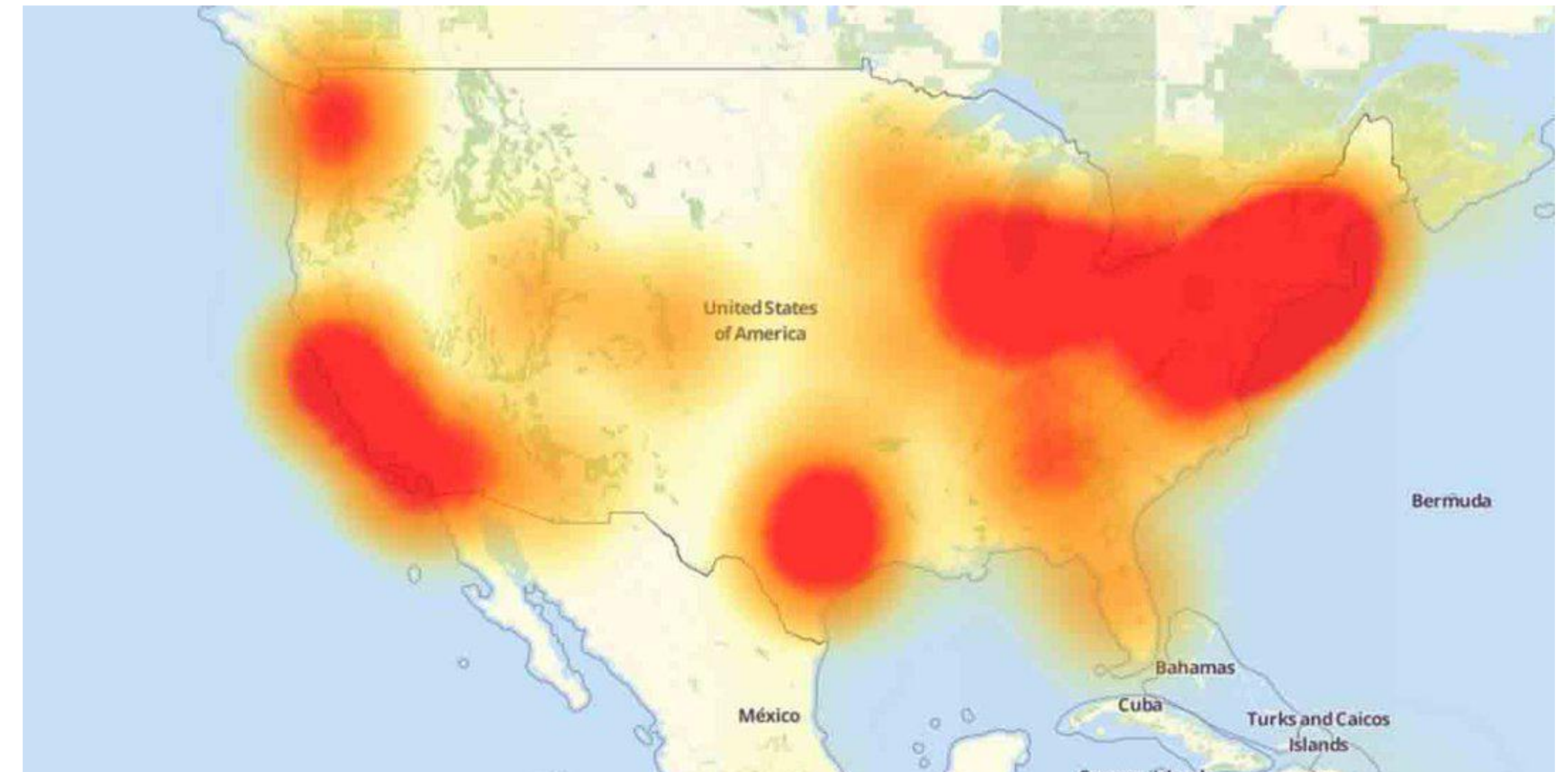
# Vulnerabilities

- If government agencies discover a security flaw, are they obligated to disclose it to the company?
  - Yes – allow companies to patch software, protect users
  - No – lose an entry point for intelligence and law enforcement
- Vulnerability Equities Procedure
- Bug bounties: Encourage public reporting



# Mirai, 2016

- Malware that created a botnet
  - Uses unsecured Internet of Things devices to launch DDoS attacks
- Targeted Dyn, a domain name system service
- Took down popular sites including Twitter, Netflix, CNN, Spotify, Reddit
- Developed by university students for gaming



# Internet of Things security

- Devices not built for security
  - Individual devices can be hacked
  - Used as entry point to networks
  - Can be harnessed to create botnets
- Supply chain issues





MAY 21, 2016 / 12.00 P.M.

# STOP ISLAMIZATION OF TEXAS



MAY 21 Stop Islamization of Texas


Public · Causes Hosted by Heart of Texas

★ Interested + Going Invite ...

🕒 Saturday, May 21 at 12 PM  
Next Week

📍 Islamic Da'wah Center 201 Travis St, Houston, TX 77002

GUESTS  
76  
interested

 **United Muslims of America** shared their event.  
Sponsored · 🌐

It's been only a month since Library of Islamic Knowledge at the center in Houston is open



**SAVE ISLAMIC KNOWLEDGE**  
May 21 at 12:00 PM, Houston TX

MAY 21 **SAVE ISLAMIC KNOWLEDGE**  
Sat 12 PM · Islamic Da'wah Center 201 Travis St,...  
42 people interested · 18 people going

★ Interested





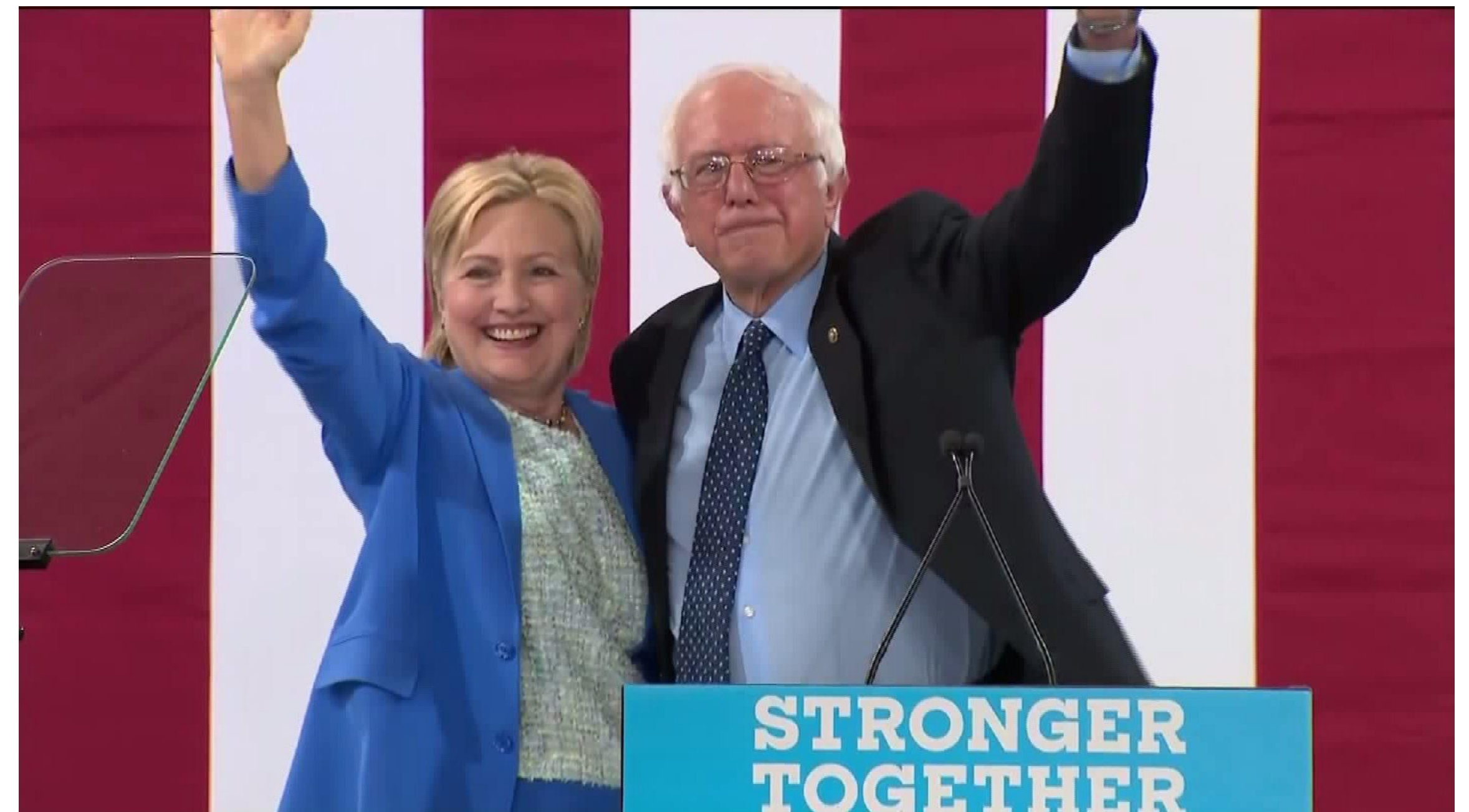


# U.S. election, 2016

- Internet Research Agency posts and ads in U.S.:
  - YouTube: 18 channels, 1,000 videos
  - Twitter: 2,752 accounts, 131,000 tweets
  - Facebook: 470 accounts, 3,000 ads, 80,000 posts
  - Social as well as political themes
- Documents hacked from DNC and John Podesta, posted on WikiLeaks at key moments of campaign

# Rationale for influence operation

- Pollute information environment
  - Spread confusion, overwhelm public dialogue
  - Cause doubt in democracy and institutions
- Hijack news agenda





# Myanmar, 2016-17

- Buddhist extremists, politicians, military leaders spread anti-Rohingya rhetoric on Facebook
- UN report:
  - *“Facebook has been a useful instrument for those seeking to spread hate, in a context where for most users Facebook is the internet. Although improved in recent months, Facebook’s response has been slow and ineffective.”*
- Facebook banned military officials in August 2018



# Freedom of speech and social media

- Platforms limit speech, but criteria not clear
  - Decisions often made by content moderators
  - Lack of appeal process
  - Accusations of differential treatment: eg. ISIS vs. extreme right
- Traditionally followed U.S. First Amendment tradition, prioritizing freedom of expression
- Protecting right to toxic speech can curtail rights of others



## India, 2018

- Two dozen deaths in mob violence and lynchings in response to rumours spread on WhatsApp
- Messages can be forwarded to groups of up to 256 people
- Encryption: Impossible to track messages
- WhatsApp has added more protections for India





# The regulation debate

- Private companies built de facto rules, created public square
- Government regulation: Which governments?
  - Sets precedent allowing repressive regimes to censor
- Strict regulation may lead to over-censorship

---

Centre for International  
Governance Innovation

# The search for solutions

# Cyber security approaches

- Focus on resilience
- Education and recruitment
- International cooperation
  - Collective action approach
- Multi-stakeholder cooperation: public, private, civil society
  - Cybersecurity Tech Accord
- Commercial security standards – eg. “nutrition label”
- Improved public outreach and education



# Information security approaches

- Improved transparency on social media platforms
  - Content moderation
  - Political advertising
- Digital media literacy
- Multistakeholder cooperation
  - Improve global outreach

---

Centre for International  
Governance Innovation

# Thank you.

67 Erb Street West,  
Waterloo, ON, Canada N2L 6C2  
Telephone +1 519 885 2444

**[smaclellan@cigionline.org](mailto:smaclellan@cigionline.org)**