Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

NEAR EAST SOUTH ASIA
CENTER FOR STRATEGIC STUDIES
NATIONAL DEFENSE UNIVERSITY

ARAB-ISRAELI CONFLICT:
ISRAEL/JORDAN TRUST TO ENHANCE DEFENSE AND SECURITY COOPERATION SEMINAR

CYBERSECURITY

SIMON HANDLER

Topic

- Hacking and leaking sensitive information by state and non-state actors creates damaging effects to national security. Although Artificial Intelligence (AI) can contribute to the number of cyber-threats, it can also be used to detect and mitigate them. This session will examine and will address how AI-powered cybersecurity solutions can help both countries counter these threats and contribute toward regional stability.

Today’s presentation

- Understanding hack-and-leak operations
  - *Motives, means, and consequences*
  - *Notable examples*
- Looking outside the region
- Middle East regional threats
- Characterizing the cyber domain
- A new framing for cyber strategy
- Application of the strategy

Understanding hack-and-leak operations

- Convergence of cyber and information operations
- Adversary (and sometimes even allied) use of cyber tools to gain access to secret and/or sensitive material and subsequently release it to the public.
  - *Information*
  - *Tools*
- While the term “leak” indicates some authenticity of the material, hack-and-leak operations may involve manipulation as well.
- Obfuscated attribution, false flags, and deniability

Motives, means, and consequences

- Motives
  - *Deliberate attempts to direct public moral judgment against a target*
  - *Exposure of capabilities, vulnerabilities, and uncertainty*
  - *Financial*
- Means
  - *Phishing*
  - *Spear phishing*
  - *Ransomware*
  - *Supply chain attacks*
- Consequences, pitfalls, and risks
  - *National security, economic, and social implications*
  - *Impact may be difficult to measure but may range from severe domestic and geopolitical consequences to inconsequential.*
  - *Hacking tools provide the means for adversaries to obtain and then release secret material, but threaten to draw attention to the operation itself, rather than the scandal of the leak.*

Notable examples of hack-and-leak operations

- 1929 – Tanaka Memorial (source unknown)
- 2016 – Democratic National Committee (Russian intelligence)
- 2016 – Panama Papers (John Doe)
- 2017 – EternalBlue (Shadow Brokers)
- 2020 – Sunburst/SolarWinds (not a known hack-and-leak, but potential is there)

Looking outside the region

- State actors
  - *Russia*
  - *North Korea*
  - *China*
- Non-state actors
  - *Ransomware groups*
  - *Hacktivists*
  - *Private individuals*

Regional landscape

- State actors
  - United Arab Emirates
  - *Saudi Arabia*
  - *Iran*
- Non-state actors
  - *Hamas (MoleRATS/Gaza Cybergang)*
  - *Hezbollah (Lebanese Cedar)*

Characterizing the cyber domain

- Irregular engagements
  - *Utilized by state and non-state actors*
  - *Frequent asymmetric approaches*
- Persistent low-intensity conflict
  - *Gray zone between peace and war*
- Interconnected landscape
  - *Non-combatants exposed to conflict*
- Distinguishablity problem

A new framing for cyber strategy

- Shift framing from one-off catastrophic attacks
- Instead, take lessons for cyber conflicit from irregular conflict. Counterterrorism and counterinsurgency strategies provide useful lessons.
  - *Intelligence contest*
  - *Temporality and evolution*
  - *Compete better*

Application of the strategy

- Passive measures
  - *Ruthlessly prioritize risk*
  - *Improve defensibility*
  - *Focus on adaptability*
  - *Resilience*
- Active measures
  - *Identification and information sharing*
  - *Sanctions*
  - *Law enforcement actions*
  - *Apply pressure to safe havens*

Thank you

תודה

شكرا