CYBER

MICHAEL SEXTON

ISSUES

- Iran, Syria, Israel, and the UAE have demonstrated the capability and willingness to carry out destabilizing cyber attacks in the region. Hezbollah and Hamas are also developing their own offensive cyber capabilities.
- Private corporations in the U.S. and Israel have exported offensive cyber tools and surveillance technologies both in the region and around the world, including to nondemocratic and semi-democratic regimes in Saudi Arabia, Syria, Ecuador, and elsewhere.
- Entities in Iran, the UAE, Saudi Arabia, and Egypt have been identified as engaging in influence operations, including misinformation campaigns, akin to Russia's campaign to influence the 2016 presidential election in the U.S.
- Governments throughout the Middle East are increasingly justifying use of potentially invasive contact tracing technology as part of the national response to the COVID-19 pandemic, which could lead to more incursions into privacy and civil liberties for the region's citizens, activists, and journalists.

US INTERESTS

- Strengthen cybersecurity capabilities of regional allies to limit risks of cyber conflict.
- Limit and control the proliferation of offensive cyber capabilities.
- Maintain capacity to carry out offensive cyber operations when absolutely necessary.
- Combat or prevent misinformation and influence campaigns that may destabilize allies in the region or the U.S. itself.

POLICY RECOMMENDATIONS

- Maintain dialogue with allies and adversaries to communicate priorities and red lines with respect to cyber conflict to reduce the risk of escalation.
    - Support defensive cyber cooperation and information-sharing among American allies and partners, in particular the Abraham Accords countries.
- Discourage regional states from using Huawei's 5G technology.
- Regulate and closely monitor American cyber technology companies that work to export offensive cyber tools, including penetration testing tools.
- Pressure allies, most notably Israel, to similarly exercise caution when permitting private companies to export cyber tools that can be used maliciously for surveillance or cyber attacks.
- Encourage U.S. cybersecurity firms to do business abroad and export defensive technologies, in particular with U.S. allies.
- Streamline regulatory processes for exporting defensive cyber technology.
- Strategically promote American cybersecurity companies in trade missions.
- Establish and maintain high-level dialogue between the intelligence community, law enforcement, and social media companies (Facebook, Twitter, and Google) to share information on malicious foreign influence operations, bots, and misinformation campaigns both in the U.S. and abroad.
- Discourage widespread sharing of contact tracing data with law enforcement and national security agencies, while encouraging governments to keep such data under strict control of public health and related ministries, and to purge data after it becomes irrelevant.