THE
NATIONAL LAW REVIEW

Attorney General's Cyber-Digital Task Force Assesses Cyber Threats and Response Efforts in New Report

Drinker Biddle
Article By
Peter Baldwin
Drinker Biddle & Reath LLP
DBR on Data

- Communications, Media & Internet
- Criminal Law / Business Crimes

- All Federal

Wednesday, August 1, 2018

The Attorney General's Cyber-Digital Task Force has released its first report, which provides a detailed assessment of the cyber threats facing the United States and discusses the ways the Department of Justice (DOJ) is combatting and preparing to combat those threats.

The DOJ Cyber-Digital Task Force was established in February 2018 and was directed to answer two fundamental questions: (1) how is DOJ responding to global cyber threats, and (2) how can federal law enforcement accomplish its mission in the cyber area more effectively.

Chapter 1 of the report focuses on threats posed by malign foreign influence operations, which include "covert actions by foreign governments intended to sow division in [American] society, undermine confidence in [American] democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives." The report discusses various types of foreign influence operations that have targeted U.S. democratic and electoral processes and details DOJ's framework to counter each of them.

Chapters 2 and 3 discuss other cyber-enabled threats. Chapter 2 describes the most common types of cyber-enabled criminal schemes, including: (1) damage to computer systems (including Distributed Denial of Service (DDoS) and ransomware attacks), (2) data theft (including the theft of personal identifying information and intellectual

property), (3) fraud/carding schemes, (4) cyber-enabled crimes threatening personal privacy (including “sextortion,” “revenge porn,” and cyber-enabled harassment), and (5) cyber-enabled crimes threatening critical infrastructure. The report then details common techniques used to facilitate cyber-attacks, including social engineering, malware, botnets, and the use of other criminal infrastructure. Chapter 3 focuses on DOJ’s efforts to detect, deter, and disrupt cyber threats and reviews DOJ’s key investigative techniques and prosecution tools for combatting cyber-enabled crimes.

Chapter 4 focuses on the role of the Federal Bureau of Investigation (FBI) in responding to cyber incidents. Specifically, the report details the FBI’s efforts to build relationships with organizations and sectors that are at particular risk for cyber-enabled attacks, as well as the FBI’s efforts to foster better sharing of cyber threat information between the U.S. Government and private industry.

Chapter 5 discusses DOJ’s efforts to recruit and train their personnel on cyber matters.

Finally, Chapter 6 identifies several challenges for DOJ in its ongoing efforts to combat cyber-enabled attacks. In addition, the report lists key areas where DOJ and the Task Force intend to focus in the future, which include: enhancing effective collaboration with the private sector, addressing encryption and anonymity, addressing malign foreign influence operations, preparing for emerging and future technology, and strengthening DOJ’s tools and authorities for combatting cyber-enabled crimes.

The establishment of the Attorney General’s Task Force and the release of its first report serve to reinforce the high priority that DOJ currently is placing on combatting, investigating, and prosecuting cyber-enabled crimes. Given this priority status, it can reasonably be expected that the number of cyber-focused investigations and criminal prosecutions – involving both domestic and international criminal actors – will continue to increase in 2018 and beyond.

A copy of the Task Force report can be accessed here.