March 3, 2023

Deputy Attorney General Announces Creation of Disruptive Technology Strike Force

On February 16, in remarks delivered at Chatham House in the United Kingdom, Deputy Attorney General Lisa Monaco announced the creation of the Disruptive Technology Strike Force, a joint initiative led by the Department of Justice (DOJ) and the Department of Commerce, to address new national security and cybersecurity threats arising from new technological capabilities.[1] These new threats include cyber attacks by rogue nation-states, often working with criminal groups; the weaponization of personal data; and the use and abuse of disruptive technologies by autocratic governments.

The DAG explained that, although nation-states are engaging in more sophisticated, brazen, and dangerous cyber attacks, effective collaboration among international law enforcement has disrupted these attacks. For example, the United States and the United Kingdom disabled the Russian military-controlled "Cyclops Blink" global botnet among other threats.[2] The DAG also cautioned that ever-advancing AI technology will enable the use of data in increasingly sophisticated ways and that foreign governments may weaponize data against perceived threats abroad, referring to China's "national security law requir[ing] any company doing business in China to make its data accessible to the government." She added: "So if a company operating in China collects your data, it is a good bet that the Chinese government is accessing it." Finally, the DAG emphasized the need to guard against autocratic governments' use of disruptive technologies for cyber theft, sanctions evasion, and exploiting foreign investment. To that end, she noted, the U.S. Committee on Foreign Investment's (CFIUS) has sharpened its focus on cybersecurity, Congress has passed the CHIPS Act, and the federal government has imposed restrictions and transfer controls on semiconductor chips and other sensitive technologies[3]. She warned that "Justice Department prosecutors will be vigorously enforcing these rules."

The DAG explained that the Disruptive Technology Strike force is the culmination of efforts to bring together top experts on national security across the federal government. Its aim is to use intelligence and data analytics to target illicit actors, enhance public-private partnerships, and identify early threat warnings. This approach of creating cross-disciplinary task forces to address growing threats is emblematic of the Biden Administration's continued "all tools" approach to national security and cybersecurity threats. For example, the DOJ and the Treasury Department's FinCEN along with French law enforcement took

---

1 *Deputy Attorney General Lisa O. Monaco Delivers Remarks on Disruptive Technologies at Chatham House*, U.S. Dep't of Justice (Feb. 16, 2023), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-disruptive-technologies-chatham.

2 *Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)*, U.S. Dep't of Justice (Apr. 6, 2022), https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation.

3 *See, e.g.*, U.S. Dep't of Commerce, Bureau of Industry and Security, *Public Information on Export Controls Imposed on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)*, https://www.bis.doc.gov/index.php/policy-guidance/advanced-computing-and-semiconductor-manufacturing-items-controls-to-prc (last updated Jan. 25, 2023).

coordinated action against the cryptocurrency exchange platform Bitzlato Ltd.,[4] and the DOJ disrupted the operations of ransomware group Hive using a multi-pronged "all tools" approach.[5]

Key Takeaways

- Companies considering the development of or investments related to technology that could broadly be construed as related to national security—particularly technologies or companies with any connection to what the DAG has referred to as "autocratic regimes"—should prepare for ever-increasing scrutiny from both the DOJ and other parts of the government.

- Companies should pay close attention not only to the ever-evolving cybersecurity threat environment but also to the changing landscape in data security standards and to disclosure regimes oriented toward facilitating public-private partnerships with law enforcement, which companies will be well served to consider where appropriate.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Yahonnes Cleary
+1-212-373-3462
ycleary@paulweiss.com

David Fein
+44-20-7367-1608
dfein@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Associates Megan L. Gao and Jordan E. Orosz contributed to this Client Memorandum.

[4] *Founder and Majority Owner of Bitzlato, a Cryptocurrency Exchange, Charged with Unlicensed Money Transmitting*, U.S. Dep't of Justice (Jan. 18, 2023), https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-bitzlato-cryptocurrency-exchange-charged-unlicensed-money.

[5] *See* Paul, Weiss Client Memorandum, *DOJ Multinational Operation to Disrupt Ransomware Organization Focuses on Aiding Ransomware Victims* (Jan. 30, 2023), https://www.paulweiss.com/media/3982995/doj_multinational_operation_to_disrupt_ransomware_organization_focuses_on_aiding_ransomware_victims.pdf.