FACT SHEET: Disruptive Technology Strike Force Efforts in First Year to Prevent Sensitive Technology from Being Acquired by Authoritarian Regimes and Hostile Nation-States

One year ago, on February 16, 2023, the Departments of Justice and Commerce, alongside their partners at the Federal Bureau of Investigation and Homeland Security Investigations, launched the Disruptive Technology Strike Force to fiercely protect advanced technology from being unlawfully acquired by foreign adversaries. Together, the agencies that comprise the Strike Force have taken an all-tools approach to aggressively pursue enforcement actions against illegal procurement networks and prevent nation-state actors from illicitly acquiring our most sensitive technology.

In the twelve months since its formation, the Strike Force has successfully:

Charged 14 cases involving alleged sanctions and export control violations, smuggling conspiracies, and other offenses related to the unlawful transfer of sensitive information, goods, and military-grade technology to Russia, China, or Iran.

- ***Seven cases charged defendants with sending or attempting to send semiconductors, microelectronics, or other technologies to Russia in violation of U.S. law.***

    - In January 2024, Brooklyn- and Los Angeles-based businessman Ilya Kahn was arrested for allegedly running a years-long scheme to unlawfully export hundreds of thousands of semiconductors to a sanctioned Russian business, using networks of businesses in the China and other transshipment points to evade export controls.

    - In October 2023, Brooklyn-based Salimdzhon Nasriddinov, a dual Russian and Tajik national, and Canadian nationals Nikolay Goltsev and Kristina Puzyreva were arrested for running a scheme to source, purchase, and ship millions of dollars' worth of dual-use electronics from U.S. manufacturers to sanctioned end-users in Russia, including components used in guided missile systems and unmanned aerial vehicles (UAVs).

    - In October 2023, Brooklyn resident Nikolay Grigorev was arrested and Russian nationals Nikita Arkhipov and Artem Oloviannikov were charged with running a scheme to procure dual-use electronic components, including semiconductors, for companies affiliated with the Russian military.

- In September 2023, Russian citizen Maxim Marchenko was charged with using shell companies in Hong Kong to smuggle large quantities of microelectronics with military applications to end users in Russia.

- In August 2023, dual Russian-German citizen Arthur Petrov was arrested in Cyprus for his involvement in a scheme to procure U.S.-sourced microelectronics on behalf of a Russia-based supplier of critical electronic components for manufacturers supplying weaponry and other equipment to the Russian military.

- In May 2023, Greek national Nikolaos Bogonikolos was arrested for overseeing a years-long operation to smuggle into Russia U.S.-origin military and dual-use technology, including sensitive components used in quantum cryptography and nuclear weapons testing.

- In May 2023, Russian nationals Oleg Sergeyevich Patsulya and Vasilii Sergeyevich were arrested for conspiring to violate export control laws and commit money laundering to obtain airplane technology for Russian airlines.

These cases were brought in partnership with Task Force KleptoCapture, an interagency law enforcement effort dedicated to enforcing the sweeping sanctions, export restrictions, and economic countermeasures that the United States, along with its allies and partners, has imposed in response to Russia's unprovoked military invasion of Ukraine.

Assistant Attorney General for National Security Matthew G. Olsen and Assistant Secretary for Export Enforcement Matthew S. Axelrod of the Commerce Department, and five U.S. Attorneys from offices around the country, and officials from HSI and FBI announced the Strike Force's first five cases in May 2023.

- ***Three cases charged former employees of U.S. companies with stealing confidential and proprietary information related to sensitive technology and attempting to take such***

information to China, and one case charged a defendant with seeking to obtain technology from U.S. manufacturers on behalf of Chinese end users.

- In February 2024, California resident Chenguang Gong was arrested for transferring more than 3,600 files containing proprietary information from his employer, including files with blueprints for sophisticated missile-detection technology. According to the complaint, Gong sought funding from the People's Republic of China (PRC)-administered "Talent Programs," which recruit individuals overseas with expertise sought after by the PRC, to develop similar technology.

- In May 2023, Liming Li of California was arrested for his alleged theft of sensitive technology related to advanced manufacturing software programs from his Southern-California-based employers and using that information to market his own competing company to businesses in China.

- In May 2023, California man and former Apple employee Weibao Wang was charged in connection with a scheme to steal Apple source code and other proprietary information related to autonomous systems. Allegedly, he left Apple to work as an engineer for a U.S.-based subsidiary of a China-based company to work on the development of self-driving cars, and, following a search of his residence, Wang left the country for China.

- In December 2023, Belgian national Hans Maria De Geetere was charged and arrested in Belgium for crimes related to a years-long scheme to export accelerometers used in aerospace and military systems from the United States to end users in China.

- ***Three cases charged individuals with seeking to procure sensitive U.S. technology on behalf of the government of Iran or Iranian end users.***

  - In February 2024, Iranian national Abolfazi Bazzazi and his son Mohammad Resa Bazzazi were charged with violating U.S. sanctions by procuring for the Government of Iran and other Iranian ends users goods and technology from U.S. companies that supply the military, aerospace, and firefighting industries.

  - In January 2023, four Chinese nationals, Baoxia Liu, You Wa Yung, Yongxin Li, and Yanlai Zhong, were charged with smuggling U.S.-origin items used in the production of UAVs and ballistic missile systems through Chinese front companies to Iranian entities with ties to the Islamic Revolutionary Guard Corps and Ministry of Defense.

  - In May 2023, Chinese national Xiangjiang Qiao was charged with multiple offenses related to a scheme to use a sanctioned Chinese company to provide high-tech materials used in the production of weapons of mass destruction to Iran, in exchange for payments made through the U.S. financial system.

Secured the guilty plea of a defendant charged for her role in a multimillion-dollar scheme to send electronic components used in UAVs and guided missile systems and other weapons to sanctioned entities in Russia.

- In February 2024, Canadian national Kristina Puzyreva, one of three defendants charged in the case, pleaded guilty to money laundering conspiracy as part of a sophisticated sanctions and export control scheme involving two Brooklyn-based companies.

Issued Temporary Denial Orders against 29 entities, including airlines, freight forwarders, defense companies, and others to cut off their access to controlled U.S. items.

Contributed to numerous parties being placed on Commerce's Entity List and Treasury's Specially Designated Nationals and Blocked Persons List.

Forged international partnerships committed to preventing critical technology from being siphoned off by foreign adversaries.

- Assistant Attorney General Matthew Olsen and Assistant Secretary for Export Enforcement Matthew Axelrod traveled to Kyiv in November 2023, following prior visits by the Attorney General to Ukraine, to reaffirm the Strike Force's close partnership with the Ukrainian Prosecutor General and commitment to curbing the illegal flow of advanced technology to Russia.

- Following the Camp David Leaders' Summit with President Biden and the leaders of Japan and Korea, DOJ and Commerce took steps to establish a Disruptive Technology Protection Network with South Korea and Japan to expand collaboration on technology protection measures, including expanding information-sharing and the exchange of best practices across the three countries' enforcement agencies.

- As part of the Munich Security Conference, Assistant Attorney General Matthew Olsen and Assistant Secretary Matthew Axelrod participated in a panel discussion on safeguarding disruptive technology in a new era of economic statecraft.

- During a speech in the United Kingdom, where she announced the creation of the Strike Force in February 2023, Deputy Attorney General Lisa Monaco delivered remarks about the national security risks posed by artificial intelligence and why it is a top enforcement priority for the Strike Force.

- Assistant Attorney General Matthew Olsen delivered remarks and participated in a roundtable discussion hosted by the American Academy at the U.S. embassy in Berlin, Germany. Throughout the visit, AAG Olsen reaffirmed the Department's close partnership with foreign counterparts to stop the flow of sensitive technology to foreign adversaries.

- Assistant Secretary of Commerce for Export Enforcement Matthew Axelrod delivered remarks on international partnerships, with a focus on the Strike Force, at the Federal Office for Economic Affairs and Export Control-Bureau of Industry and Security Export Control Forum in Frankfurt, Germany.

Assistant Attorney General for National Security Matthew G. Olsen and Assistant Secretary for Export Enforcement Matthew S. Axelrod of the Commerce Department tour the Kyiv Scientific Research Institute of Forensic Expertise, which houses drones, electronic components, and other devices used by Russia and found on the battlefields in Ukraine. The two traveled to Kyiv, Ukraine from Oct. 30 – Nov. 1, 2023, to meet with counterparts about stopping the flow of sensitive technology to Russia.

Fostered partnerships with the private sector, working directly with companies involved in the manufacture, sale, and shipment of sensitive export-controlled items.

- Hosted industry outreach events in Boston, Massachusetts; Houston, Texas; and Phoenix, Arizona to educate industry on the Strike Force's work to stem the flow of sensitive technology to our adversaries, recent corporate enforcement initiatives, and tips and best practices for working with investigators on issues related to export compliance, cybersecurity, and protecting intellectual property.

- Convened roundtable discussions with compliance officials and technical experts at multiple cutting-edge tech companies, research institutions, and defense contractors.

- Toured the largest and third-largest commercial ports in the United States.

More than 200 people from across the country gathered in Phoenix for a two-day summit to mark the Strike Force's one-year anniversary. Here, AAG Olsen, Assistant Secretary Axelrod, and the leaders of eight U.S. Attorney's Offices stand with a delegation of Ukrainian officials who spoke at the summit.

Added new interagency partners to the effort and enforcement teams to the Strike Force.

- To strengthen efforts to protect defense industry technology, the Strike Force added the Defense Criminal Investigative Service as a formal Strike Force partner.

- To strategically align Strike Force presence with the location of critical technology-related industries throughout the United States, the Strike Force added enforcement teams in the Eastern District of North Carolina, the Western District of Texas, and the Southern District of Georgia.