Cyber

The 21st century has seen the rise of entirely new challenges, in which criminal and national security threats strike from afar through computer networks with potentially devastating consequences. The FBI continues to adapt to meet these challenges. The FBI Cyber Division was created in 2002 to combat cyber-based terrorism, hostile foreign intelligence operations conducted over the Internet, and cyber crime by applying the highest level of technical capability and investigative expertise. The Cyber Division continues to evolve to meet the FBI's leading role to defend America against the rapidly growing cyber threat. It aggregates cyber-centered investigations within one division to more effectively and efficiently identify, mitigate, and disrupt cyber threats.

Intelligence-Driven Operations

- **Cyber Intelligence:** As a member of the U.S. intelligence community, the FBI leads the recently formed National Cyber Investigative Joint Task Force (NCIJTF), which brings together representatives of the intelligence community and select federal law enforcement agencies. The Cyber Intelligence Section (CybIS) leads the FBI's analysis and reporting on terrorism, foreign intelligence, and criminal matters that contain a cyber nexus. CybIS provides actionable intelligence, as well as policy, standards, and oversight support for the intelligence functions and processes of the FBI and the greater intelligence community.
- **Threat Focus Cells:** The FBI centers operational coordination and management on prioritized cyber threats through the use of Threat Focus Cells (TFCs). TFCs are diverse teams—comprised of subject matter experts from the FBI and from partner agencies—designed to adapt their focus and membership in response to a threat as it evolves. TFCs develop a comprehensive understanding of emerging cyber threats and vulnerabilities through intelligence-driven operations. They achieve their goals by focusing the attention of subject matter experts on the highest priority cyber security threats and by developing proactive operations through multi-agency collaboration.
- **Cyber Workforce Development:** In 2002, the FBI initiated a specialized training program to develop cyber investigators for the 21st century. The program recognizes the individual experience and knowledge various employees bring to the FBI and allows investigators to test out of courses involving material they have previously mastered. This permits more technically advanced new investigators to move on to more challenging courses in an individualized progression, accelerating their access to expert level training. The Cyber Workforce Development program builds the skills necessary to meet the investigative challenges posed by terrorists, hostile nation states, and criminal organizations.

Leadership and Collaboration

- **National Cyber Investigative Joint Task Force (NCIJTF):** The FBI operates the NCIJTF as a presidentially mandated and well-recognized alliance of government organizations with complementary missions to protect national cyber interests. In 2008, the NCIJTF was incorporated into Comprehensive National Cybersecurity Initiative strategy and was identified to serve as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations. The FBI leads the NCIJTF to foster each member organization's ability to identify, mitigate, and disrupt cyber threats by coordinating and integrating their counterintelligence, counterterrorism, intelligence, and law enforcement activities. The NCIJTF scope includes all domestic cyber threat activity, cyber investigations involving

government and non-government networks and intrusions, U.S. persons, private corporations, and domestic and international crime. The NCIJTF coordinates and integrates cyber threat investigations, allowing NCIJTF partners to quickly identify new threats, new motives, and new targets and effectively leverage all U.S. government authorities in pursuit of these threats.

Partnerships

- The FBI's Cyber Initiative and Resource Fusion Unit is co-located with the National Cyber Forensics and Training Alliance (NCFTA). The NCFTA develops responses to evolving threats to the nation's critical infrastructure by participating in cyber-forensic analysis, tactical response development, technology vulnerability analysis, and the development of advanced training. The NCFTA developed as an outgrowth of one of the first federal/state/local High Tech Crimes Task Forces, which recognized the significant need to attract ongoing participation from key subject matter experts within industry and academia to both enhance and sustain effectiveness.
- Established in 2000, the Internet Crime Complaint Center (IC3) is a partnership between the FBI and the National White Collar Crime Center, serving as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. IC3 was intended to serve and continues to emphasize serving the broader law enforcement community, including federal, state, and local agencies, which employ key participants in the growing number of Cyber Crime Task Forces. Since its inception, IC3 has received complaints encompassing a wide variety of cyber crime matters, including online fraud (in its many forms), intellectual property rights matters, computer intrusions (hacking), economic espionage (theft of trade secrets), child pornography, international money laundering, identity theft, and a growing list of additional criminal matters.
- InfraGard, an information sharing and analysis effort, is an FBI program that began in 1996 as a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to several FBI field offices, and in 2003, the Bureau assigned national program responsibility for InfraGard to the Cyber Division. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters. The InfraGard program has tens of thousands of members nationwide who hold regular meetings in more than 80 cities throughout the country.

International

- The FBI is a leading agency in investigating cyber crimes committed both inside and outside our national borders against U.S. persons, businesses, and critical infrastructures by cyber criminals whose physical presence and operations are often located in multiple countries. Cyber criminal groups have evolved into international enterprises with professional management business models, complex technical communications networks, and highly sophisticated cyber tools suggesting that cyber crime, as an industry, has a future of expansion and sustainable growth. The FBI's legal attaché program, which consists of more than 70 offices overseas, is on the forefront of our nation's efforts to combat transnational organized cybercrime groups.